7.3.3. Zweiter Spezialfall: a ungerade. *Sei $p > 2$ Primzahl, sei $(a, 2p) = 1$. Dann gilt:*

$$\left(\frac{a}{p}\right) = (-1)^\nu \qquad \text{mit} \qquad \nu = \sum_{j=1}^{(p-1)/2} \lfloor \tfrac{ja}{p} \rfloor.$$

Beweis: Links gibt es in 7.3.1 den Faktor $a - 1 \equiv 0 \mod 2$, also ist die linke Seite Null, demnach ist

$$\mu \equiv \sum_{j=1}^{(p-1)/2} \lfloor \tfrac{ja}{p} \rfloor \mod 2.$$

Wenn wir also die rechte Seite mit ν bezeichnen, so erhalten wir aus dem Gauß'schen Lemma

$$\left(\frac{a}{p}\right) = (-1)^\mu = (-1)^\nu.$$

7.4. Das quadratische Reziprozitätsgesetz.

Wir definieren:

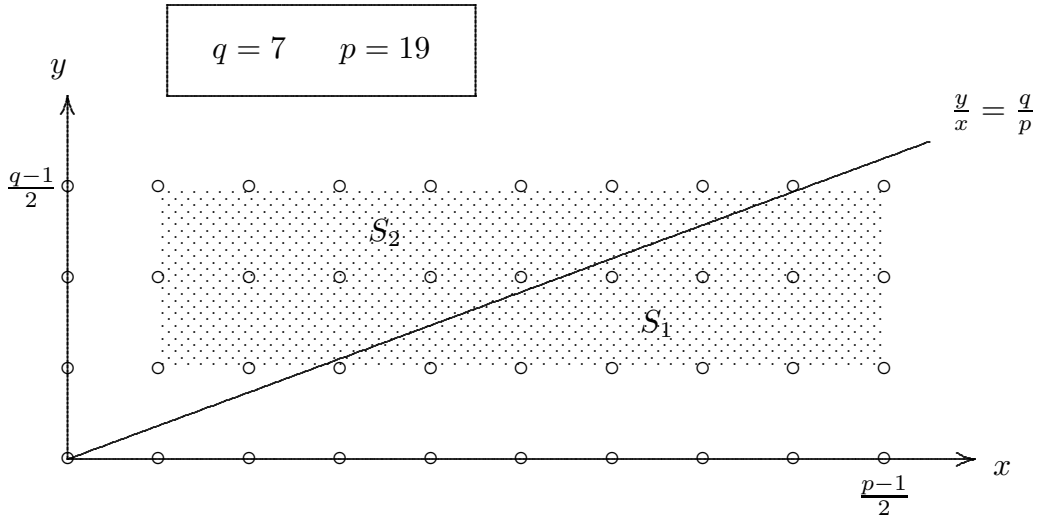
$$S = \{[x, y] \in \mathbb{Z}^2 \mid 1 \le x \le \tfrac{p-1}{2},\ 1 \le y \le \tfrac{q-1}{2}\},$$

und

$$S_1 = \{[x, y] \in \mathbb{Z}^2 \mid 1 \le x \le \tfrac{p-1}{2},\ 1 \le y \le \tfrac{q}{p}x\},$$
$$S_2 = \{[x, y] \in \mathbb{Z}^2 \mid 1 \le y \le \tfrac{q-1}{2},\ 1 \le x \le \tfrac{p}{q}y\}.$$

Beachte, dass S_1, S_2 in S enthalten sind (denn zum Beispiel folgt aus $y \le \frac{q}{p}x$ und $x \le \frac{p-1}{2}$, dass gilt $y \le \frac{q}{p}x \le \frac{q}{p} \cdot \frac{p-1}{2} = \frac{q}{2} \cdot \frac{p-1}{p} < \frac{q}{2}$, also $y \le \frac{q-1}{2}$.). Umgekehrt ist natürlich S in $S_1 \cup S_2$ enthalten — und $S_1 \cup S_2$ ist eine disjunkte Vereinigung: auf der Geraden $\frac{y}{x} = \frac{q}{p}$ gibt es keinen Gitterpunkt $[x, y]$ mit $1 \le x \le \frac{p-1}{2}$ (denn aus $yp = qx$ und der Tatsache, dass p, q verschiedene Primzahl sind, folgt $p|x$; für $1 \le x \le p - 1$ ist dies aber nicht möglich). Wir sehen also:

$$S = S_1 \cup S_2 \qquad \text{und dies ist eine disjunkte Vereinigung.}$$



Wir zählen nun die Gitterpunkte in S, S_1, S_2 ab. Offensichtlich ist

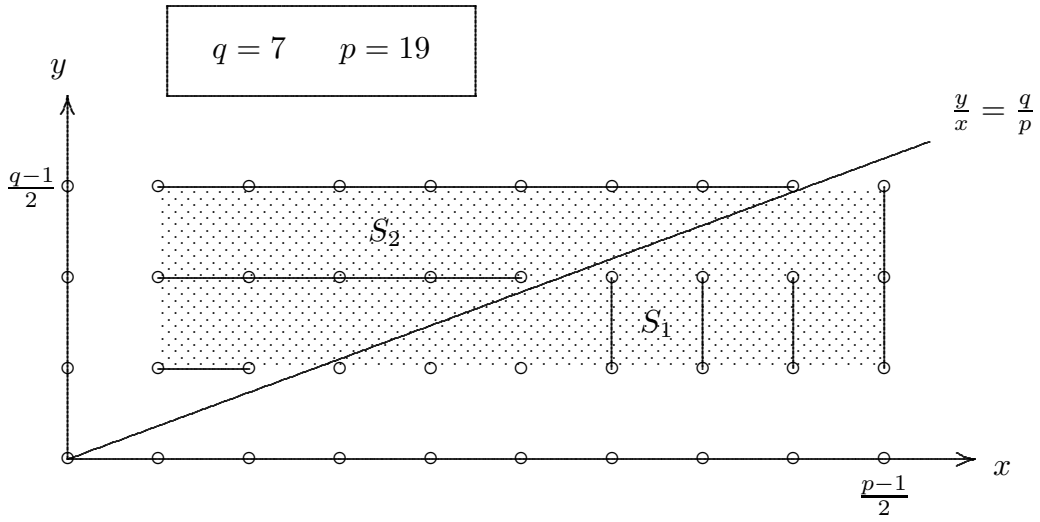
$$|S| = \tfrac{p-1}{2} \cdot \tfrac{q-1}{2}.$$

Die Anzahl der Elemente in S_1 ist

$$|S_1| = \sum\nolimits_{x=1}^{(p-1)/2} \lfloor \tfrac{q}{p} \cdot x \rfloor.$$

Entsprechend gilt

$$|S_2| = \sum\nolimits_{y=1}^{(q-1)/2} \lfloor \tfrac{p}{q} \cdot y \rfloor.$$



(die einzelnen Summanden von $|S_1|$ entsprechen den vertikalen Strecken; die Summanden von $|S_2|$ den horizontalen Strecken).

Wegen 4.3.3 gilt für ungerade Primzahlen $p \neq q$

$$\left(\tfrac{q}{p}\right) = (-1)^{\mu} \qquad \text{mit} \qquad \mu = \sum\nolimits_{x=1}^{(p-1)/2} \lfloor \tfrac{q}{p} \cdot x \rfloor = |S_1|$$
$$\left(\tfrac{p}{q}\right) = (-1)^{\lambda} \qquad \text{mit} \qquad \lambda = \sum\nolimits_{y=1}^{(q-1)/2} \lfloor \tfrac{p}{q} \cdot y \rfloor = |S_2|$$

und daher

$$\left(\tfrac{p}{q}\right)\left(\tfrac{q}{p}\right) = (-1)^{|S_1|+|S_2|} = (-1)^{|S|} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Eine Anwendung: Einige Teiler Mersenne'scher Zahlen.

Erinnerung: Ist $M_n = 2^n - 1$ eine Primzahl, so nennt man dies eine Mersenne'sche Primzahl, siehe 2.11. Wir haben gesehen: Ist M_n eine Primzahl, so ist $n = p$ selbst eine Primzahl.

Satz. *Sei $p \equiv 3 \mod 4$. Ist $q = 2p + 1$ eine Primzahl, so ist q ein Teiler der Mersenne'schen Zahl M_p.*

Beweis: Sei $q = 2p + 1$ eine Primzahl. Wegen $p \equiv 3 \mod 4$, ist $q \equiv 7 \mod 8$, also ist 2 quadratischer Rest modulo q (dies ist gerade die Regel (Z)). Wähle als $x \in \mathbb{N}$ mit $x^2 \equiv 2 \mod q$. Es ist

$$2^p \equiv (x^2)^p = x^{2p} = x^{q-1} \equiv 1 \mod q$$

(dabei haben wir am Ende den kleinen Fermat verwandt). Dies besagt: q ist ein Teiler von $2^p - 1 = M_p$.

Beispiele: Betrachte die ersten dreizehn Primzahlen $p \equiv 3 \mod 4$ und bilde $q = 2p + 1$, und bilde $q = 2p + 1$: Wir markieren mit J, falls q eine Primzahl ist.

p	3	7	11	19	23	31	43	47	59	67	71	79	83
$q = 2p + 1$	7	15	23	39	47	63	87	95	119	135	143	159	167
Primzahl	J	N	J	N	J	N	N	N	N	N	N	N	J

Insgesamt sehen wir also:

$$7|M_3, \quad 11|M_{23}, \quad 47|M_{23}, \quad 167|M_{83}.$$

Nun ist $M_3 = 7$, daher ist die erste Teilbarkeitsbeziehung ohne Interesse, die weiteren besagen aber, dass die Mersenne'schen Zahlen M_{11}, M_{23} und M_{83} **keine** Primzahlen sind.

Es ist

$$\begin{aligned} M_{11} &= 2047 = 23 \cdot 89 \\ M_{23} &= 8\,388\,607 = 47 \cdot 178\,481 \\ M_{83} &= 167 \cdot 57\,912\,614\,113\,275\,649\,087\,721 \end{aligned}$$

Aber es gibt auch Primzahlen p mit $p \equiv 3 \mod 4$, für die $2p + 1$ keine Primzahl ist, und M_p keine Primzahl ist, etwa $p = 43$

$$M_{43} = 8796093022207 = 431 \cdot 9719 \cdot 2099863,$$

und es gibt Primzahlen p mit $p \equiv 1 \mod p$, für die M_p keine Primzahl ist, wie etwa $p = 29,\ 37,\ 41$.