4. Das quadratische Reziprozitätsgesetz.

Sei p eine ungerade Primzahl, sei $a \in \mathbb{Z}$ mit $(p,a)=1$. Frage: Wann gibt es $x \in \mathbb{Z}$ mit $x^2 \equiv a \mod p$? Gibt es ein derartiges x, so nennt man a einen *quadratischen Rest modulo* p. Legendre hat die folgende Notation eingeführt (das sogenannte *Legendre-Symbol*):

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1 & \text{falls } a \text{ kein quadratischer Rest modulo } p \text{ ist.} \end{cases}$$

Es wird ein Verfahren vorgestellt, wie man den Wert von $\left(\frac{a}{p}\right)$ algorithmisch berechnen kann (sofern man die Primfaktorzerlegung der auftretenden Zahlen kennt). Damit wird also die genannte Frage beantwortet — offen bleibt dabei aber, wie man ein x mit $x^2 \equiv a \mod p$ wirklich findet!

Man braucht die folgenden Eigenschaften des Legendre-Symbols (hier ist p eine ungerade Primzahl, und a, a', b sind Zahlen, die nicht durch p teilbar sind.

(K) (Kongruenz-Eigenschaft) Gilt $a \equiv a' \mod p$, so ist $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.

(M) (Starke Multiplikativität): Es ist $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

(Z) (Der Wert für $a=2$): Es ist

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

(R) (Das Reziprozitätsgesetz): Sind p, q verschiedene ungerade Primzahlen, so gilt

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

Hier ein typisches Beispiel, wie man vorgeht:

$$\begin{aligned}
&\left(\tfrac{42}{61}\right) \underset{(M)}{=} \left(\tfrac{2}{61}\right)\cdot\left(\tfrac{3}{61}\right)\cdot\left(\tfrac{7}{61}\right), \qquad \text{also braucht man} \\
&\left(\tfrac{2}{61}\right) \underset{(Z)}{=} -1 \\
&\left(\tfrac{3}{61}\right) \underset{(R)}{=} \left(\tfrac{61}{3}\right) \underset{(K)}{=} \left(\tfrac{1}{3}\right) \underset{(M)}{=} 1 \\
&\left(\tfrac{7}{61}\right) \underset{(R)}{=} \left(\tfrac{61}{7}\right) \underset{(K)}{=} \left(\tfrac{5}{7}\right) \underset{(R)}{=} \left(\tfrac{7}{5}\right) \underset{(R)}{=} \left(\tfrac{2}{5}\right) \underset{(Z)}{=} -1
\end{aligned}$$

Insgesamt erhalten wir $\left(\frac{42}{61}\right) = (-1)\cdot 1 \cdot (-1) = 1$, demnach ist 42 quadratischer Rest modulo 61.

Wir notieren hier noch einige Spezialfälle, aber auch eine zusätzliche Regel, die das Verfahren abkürzen kann:

(1) Es ist $\left(\frac{1}{p}\right) = 1$ (Dies folgt aus (M), ist aber trivial).

(Q) (Quadrate.) Es ist $\left(\frac{a^2}{p}\right) = 1$ (Dies folgt ebenfalls aus (M), ist aber auch trivial).

(-1) (Der Wert für $a = -1$.) Es ist

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

Die Regel (-1) ist ein Spezialfall des Euler-Kriteriums, das wir in 4.1 beweisen werden; aus dem Euler-Kriterium folgt direkt (M). Die Regel (K) ist offensichtlich. (R) ist das berühmte Gauß'sche Reziprozitäts-Gesetz, wir werden zwei Beweise vorführen (von Gauß selbst gibt es sieben oder acht Beweise, insgesamt gibt es mehr als hundert Beweise und Beweis-Varianten... Die Regel (Z) wird in 4.4.2 bewiesen.

Beachte: $\frac{p-1}{2}$ ist genau dann ungerade, wenn $p \equiv 3 \mod 4$ gilt. Wir können daher die Aussage (R) umformulieren:

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{falls} \quad p \equiv 3 \mod 4, \quad \textbf{und} \quad q \equiv 3 \mod 4, \\ \left(\frac{q}{p}\right) & \text{falls} \quad p \equiv 1 \mod 4, \quad \text{oder} \quad q \equiv 1 \mod 4. \end{cases}$$

Entsprechend lässt sich die Aussage (-1) folgendermaßen formulieren:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls} \quad p \equiv 1 \mod 4, \\ -1 & \text{falls} \quad p \equiv 3 \mod 4. \end{cases}$$

Hier ist die Liste der ungeraden Primzahlen $p < 100$, markiert sind jeweils die Primzahlen mit $p \equiv 3 \mod 4$.

3∗	5	7∗	11∗	13	17	19∗	23∗
29	31∗	37	41	43∗	47∗	53	59∗
61	67∗	71∗	73	79∗	83∗	89	97

Schließlich lässt sich auch die Regel (Z) umschreiben:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls} \quad p \equiv 1 \mod 8, \quad \text{oder} \quad p \equiv 7 \mod 8, \\ -1 & \text{falls} \quad p \equiv 3 \mod 8, \quad \text{oder} \quad p \equiv 5 \mod 8, \end{cases}$$

Beweis: Man rechnet modulo 16: Ist $p \equiv 1, 3, 5, 7, 9, 11, 13, 15 \mod 16$, so ist $p^2 - 1 \equiv 1, 9, 9, 1, 1, 9, 9, 1 \mod 16$.

4.1. Das Euler-Kriterium.

Sei p eine Primzahl und $(a, p) = 1$. Dann ist

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

Beweis: Dies folgt unmittelbar aus der Tatsache, dass $(\mathbb{Z}/p)^*$ eine zyklische Gruppe mit (gerader) Ordnung $p-1$ ist und die Restklasse von -1 in $(\mathbb{Z}/p)^*$ die Ordnung 2 hat.

Siehe 3.8.5. Dort wurde gezeigt: Genau dann ist a ein Quadrat in $(\mathbb{Z}/p)^*$, wenn $a^{(p-1)/2} \equiv 1 \mod p$ gilt. Für jedes Element a in $(\mathbb{Z}/p)^*$ gilt $a^{p-1} \equiv 1$ mod p, also hat das Element $a^{(p-1)/2}$ die Ordnung 1 oder 2 in $(\mathbb{Z}/p)^*$. Ist nun a kein Quadrat in $(\mathbb{Z}/p)^*$, so hat also $a^{(p-1)/2}$ die Ordnung 2 in $(\mathbb{Z}/p)^*$, Die Restklasse von $a^{(p-1)/2}$ stimmt also mit der Restklasse von -1 überein.

Folgerung: Beweis der Eigenschaft (M). Es ist

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \mod p.$$

Aus $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \mod p$ folgt aber $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$, denn p ist ungerade.

4.2. Das Gauß'sche Lemma.

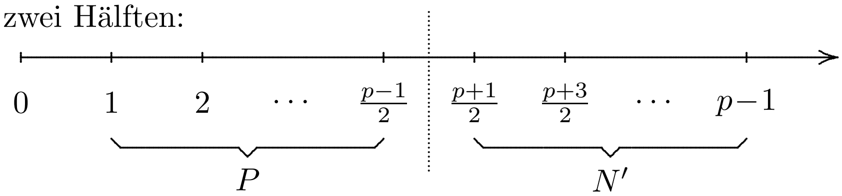
Erinnert sei an den folgenden **Beweis des kleinen Fermat:** p sei beliebige Primzahl, $(a,p) = 1$. Dann ist die Menge $\{a, 2a, 3a, \ldots, (p-1)a\}$ nichts anderes als die Menge $\{1, 2, \ldots, p-1\}$ (nur eben vielleicht umgeordnet): Die Multiplikation mit a in $\mathbb{Z}/p$ permutiert die Elemente von $(\mathbb{Z}/p)^*$. Dies liefert das linke Gleichheitszeichen:

$$\prod_{j=1}^{p-1} j = \prod_{j=1}^{p-1} ja = a^{p-1} \prod_{j=1}^{p-1} j.$$

Das Element $\prod_{j=1}^{p-1} j$ in $(\mathbb{Z}/p)^*$ ist invertierbar, also ist $1 \equiv a^{p-1} \mod p$.

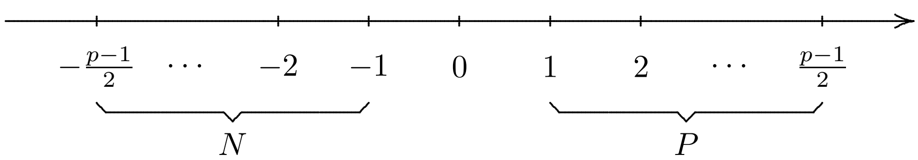
Das Gauß'sche Lemma arbeitet mit dem gleichen Trick, betrachtet aber nur das Produkt $\prod_{j=1}^{(p-1)/2} j$, falls p eine ungerade Primzahl ist.

Wir setzen wieder voraus, dass p eine ungerade Primzahl ist. Die Zahlen $1, 2, \ldots, p-1$ teilen wir in zwei Hälften:



Die punktierte Linien ist die Spiegelachse für die Multiplikation mit -1 (wir können die Zahlen in N' in der Form $-1+p, -2+p, \ldots, -\frac{p-1}{2}+p$ schreiben — dabei durchlaufen wir sie von rechts nach links).

Alternativ können wir auch die Menge N' um p nach links verschieben, also die Menge $N = \{-\frac{p-1}{2}, \ldots, -2, -1\}$ betrachten; dann sieht man noch eindringlicher, dass sich die Mengen P und N (oder N') unter der Multiplikation mit -1 entsprechen.



Beachte: die Zahlen j mit $-\frac{p-1}{2} \le j \le \frac{p-1}{2}$ sind die *betragsmäßig kleinsten Reste* mod p. Für das Gauß'sche Lemma empfiehlt es sich, die folgende Bezeichnung einzuführen: Für $x \in \mathbb{Z}$ sei $r(x)$ der betragsmäßig kleinste Rest von x modulo p: es ist also $x \equiv r(x)$ mod p und $-\frac{p-1}{2} \le r(x) \le \frac{p-1}{2}$.

Was ist die Bedeutung der Menge $P = \{1, 2, \ldots, \frac{p-1}{2}\}$? Sie liefern alle Quadratzahlen: *Die Elemente*

$$1^2,\ 2^2, \ldots, (\tfrac{p-1}{2})^2$$

in $\mathbb{Z}/p$ sind paarweise verschieden und sind gerade die Quadratzahlen in $(\mathbb{Z}/p)^*$.

Beweis: Da $\mathbb{Z}/p$ ein Körper ist, hat ein quadratisches Polynom wie etwa $f = X^2 - a$ mit $a \in \mathbb{Z}/p$ höchstens 2 Nullstellen in $\mathbb{Z}/p$. Hat f eine Nullstelle α in $\mathbb{Z}/p$, so zerfällt f in Linearfaktoren: f besitzt also zwei Nullstellen, und diese können für $p \neq 2$ und $a \neq 0$ **nicht** zusammenfallen. Wir sehen: f hat die Faktorisierung $f = X^2 - \alpha^2 = (X - \alpha)(X + \alpha)$ und $-\alpha \neq \alpha$. Ist aber $\alpha \in P$, so ist $-\alpha \in N$, ist $\alpha \in N$, so ist $-\alpha \in P$. Wir sehen also: die Quadrate der Zahlen in P sind paarweise verschieden. Und ist $\alpha \in N$, so ist $\alpha^2 = (-\alpha)^2$ und $-\alpha \in P$.

Gauß'sches Lemma. *Sei p ungerade Primzahl. Sei $(a, p) = 1$. Sei μ die Anzahl der Zahlen $j \in P$, sodass die Restklasse der Zahl ja modulo p zu N gehört. Dann ist*

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

Andere Formulierung: μ ist die Anzahl der Zahlen $1 \le j \le \frac{p-1}{2}$ mit $r(ja) < 0$.

Beweis: Wir zeigen als erstes: *Die durch $j \mapsto |r(ja)|$ definierte Abbildung $P \to P$ ist injektiv* (also bijektiv.) Seien $1 \le i, j \le \frac{p-1}{2}$. Sei $|r(ia)| = |r(ja)|$. Es ist dann entweder $r(ia) = r(ja)$ oder $r(ia) = -r(ja)$. Das letztere ist aber nicht möglich, denn dies würde bedeuten $ia \equiv r(ia) \equiv -r(ja) \equiv -ja \mod p$, also $a(i + j) \equiv 0 \mod p$ (aber $(a, p) = 1$ und $1 \le i + j \le p - 1$). Aus $r(ia) = r(ja)$ und $1 \le i, j < p$ folgt aber $ia \equiv r(ia) = r(ja) \equiv ja$, also p teilt $a(i - j)$ und demnach $p|(i - j)$. Für $1 \le i, j < p$ folgt daraus $i = j$.

Triviale Bemerkung: Ist $r(ja) < 0$, so ist $r(ja) = -|r(ja)|$, ist $r(ja) > 0$, so ist $r(ja) = |r(ja)|$. Es ist demnach

$$\prod_{j=1}^{(p-1)/2} r(ja) = (-1)^\mu \prod_{j=1}^{(p-1)/2} |r(ja)| = (-1)^\mu \prod_{j=1}^{(p-1)/2} j;$$

die letzten beiden Produkte unterschieden sich nur in der Reihenfolge der Faktoren, denn es ist $\{|r(a)|, |r(2a)|, |r(3a)|, \ldots, |r(\frac{p-1}{2}a)|\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Andererseits ist

$$\prod_{j=1}^{(p-1)/2} r(ja) \equiv \prod_{j=1}^{(p-1)/2} ja = a^{\frac{p-1}{2}} \prod_{j=1} j \mod p.$$

Wir sehen also:

$$(-1)^\mu \prod_{j=1}^{(p-1)/2} j \equiv a^{\frac{p-1}{2}} \prod_{j=1}^{p-1} j.$$

Das Element $\prod_{j=1}^{(p-1)/2} j$ in $(\mathbb{Z}/p)^*$ ist invertierbar, also ist

$$(-1)^\mu \equiv a^{\frac{p-1}{2}} \mod p.$$

Als letztes verwenden wir nun das Euler-Kriterium.

4.3. Das quadratische Reziprozitätsgesetz. Erster Beweis.

Satz (Gauß) *Seien p, q verschiedene ungerade Primzahlen. Dann gilt*

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

Beweis (nach Eisenstein, siehe Scheid).

Sei μ die Anzahl der x mit $1 \le x \le \frac{p-1}{2}$ sodass der betragsmäßig kleinste Rest von qx modulo p negativ ist.

Sei λ die Anzahl der y mit $1 \le y \le \frac{q-1}{2}$ sodass der betragsmäßig kleinste Rest von py modulo q negativ ist.

Zu zeigen ist: Es ist $\mu + \lambda$ genau dann ungerade, wenn gilt $p \equiv q \equiv 3 \mod 4$.

Wir betrachten in der reellen Ebene $\mathbb{R}^2$ die Punkte mit ganzzahligen Koeffizienten, wir nennen sie *Gitterpunkte* (unser *Gitter* ist also die abelsche Gruppe $\mathbb{Z}^2$).

Wir zählen die Gitterpunkte (x, y) mit

$$1 \le x \le \tfrac{p-1}{2}, \quad 1 \le y \le \tfrac{q-1}{2}$$

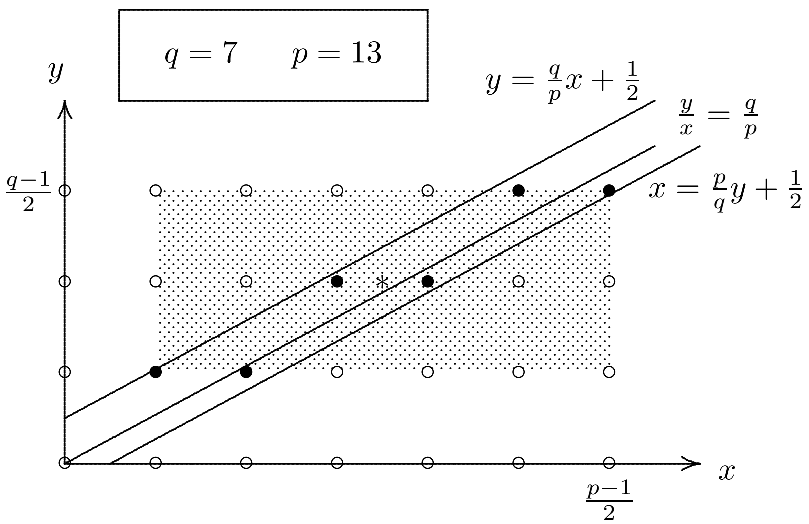
(diese Punkte bilden ein Rechteck), sodass zusätzlich gilt:

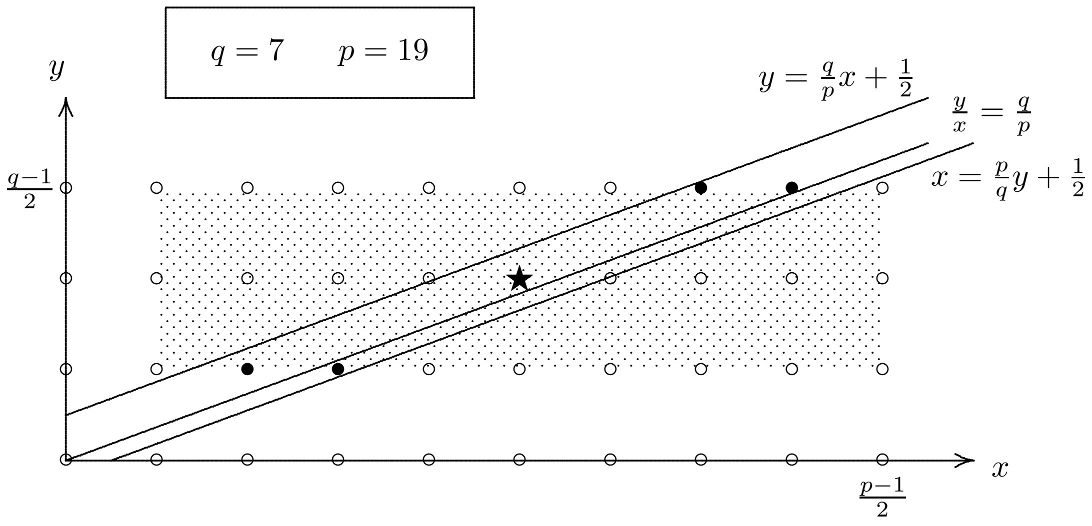
$$y < \tfrac{q}{p}x + \tfrac{1}{2}, \quad x < \tfrac{p}{q}y + \tfrac{1}{2}.$$

Wir nennen diese Menge Γ.

(Hinweis: Die beiden Geraden $y = \frac{q}{p}x + \frac{1}{2}$ und $x = \frac{p}{q}y + \frac{1}{2}$ sind parallel zur Geraden $\frac{y}{x} = \frac{q}{p}$, die letztgenannte Gerade wird im Folgenden mit g bezeichnet.)

Hier zwei Beispiele:





Wir betrachten die Punktspiegelung $(x,y) \mapsto (\frac{p+1}{2} - x, \frac{q+1}{2} - y) = (x', y')$. Dies ist eine Abbildung σ mit $\sigma^2(x,y) = (x,y)$, die den Punkt $(\frac{p+1}{4}, \frac{q+1}{4})$ (und nur diesen) fixiert (einfaches Nachrechnen!) — in den beiden Beispielen ist der Punkt als Stern $*$ markiert; im zweiten Beispiel ist dies ein Gitterpunkt, im ersten nicht!

Wir zeigen: *Die Menge der Gitterpunkte in Γ wird unter σ in sich (also auch auf sich) abgebildet.*

Beweis: Sei $(x,y) \in \Gamma$. Aus $1 \le x \le \frac{p-1}{2} = \frac{p+1}{2} - 1$ folgt $1 \le \frac{p+1}{2} - x \le \frac{p+1}{2} - 1 = \frac{p-1}{2}$ (und entsprechend für y). (Dies zeigt, dass das betrachtete Rechteck in sich abgebildet wird).

Da $(x,y) \in \Gamma$, gilt $x - \frac{1}{2} < \frac{p}{q} \cdot y$, also

$$\begin{aligned}
\tfrac{q}{p} \cdot x' + \tfrac{1}{2} &= \tfrac{q}{p} \cdot \big(\tfrac{p+1}{2} - x\big) + \tfrac{1}{2} \\
&= \tfrac{q}{p}\tfrac{p}{2} + \tfrac{q}{p}\tfrac{1}{2} - \tfrac{q}{p}x + \tfrac{1}{2} \\
&= \tfrac{q+1}{2} - \tfrac{q}{p}(x - \tfrac{1}{2}) \\
&> \tfrac{q+1}{2} - \tfrac{q}{p}\tfrac{p}{q}y \\
&= \tfrac{q+1}{2} - y = y'.
\end{aligned}$$

Entsprechend folgt aus $y - \frac{1}{2} > \frac{q}{p} \cdot x$, dass gilt $\frac{p}{q} \cdot y' + \frac{1}{2} > x'$.

Wir zeigen: Im Streifen Γ gibt es genau $\lambda + \mu$ Gitterpunkte. Genauer:

(1) Auf der durch $\frac{y}{x} = \frac{q}{p}$ definierten Geraden g liegt kein Gitterpunkt.
(2) Oberhalb dieser Geraden g liegen in Γ genau μ Gitterpunkte.
(3) Unterhalb der Geraden g liegen in Γ genau λ Gitterpunkte.

Beweis (1). Aus $qx = py$ folgt $p|x$ (da p, q verschiedene Primzahlen sind). Aber $1 \le x < p$.

Beweis (2). Sei $1 \le x \le \frac{p-1}{2}$, sodass der betragsmäßig kleinste Rest von qx modulo p negativ ist. Also gilt

$$qx = py + r \qquad \text{mit} \qquad -\tfrac{p-1}{2} \le r \le -1.$$

Wir schreiben dies um:

$$-\tfrac{p-1}{2} \le qx - py \le -1.$$

Beachte: Es folgt $1 \le y \le \frac{q-1}{2}$, denn es gilt: Wäre $y \le 0$, so wäre $qx - py \ge qx > 0$. Und es ist

$$py \le qx + \tfrac{p-1}{2} \le q\tfrac{p-1}{2} + \tfrac{p-1}{2} = (q+1)\tfrac{p-1}{2} = \tfrac{q+1}{2}(p-1),$$

also

$$y \le \tfrac{q+1}{2}\tfrac{p-1}{p} < \tfrac{q+1}{2},$$

also $y \le \frac{q-1}{2}$. Dies liefert μ Gitterpunkte im oberen Streifen. Umgekehrt ist auch zu zeigen, dass man auf diese Weise **alle** Gitterpunkte in diesem Streifen erhält.

Der Beweis von(3) ist natürlich entsprechend.

4.4. Eine Folgerung aus dem Gauß'schen Lemma.

4.4.1. *Sei p ungerade Primzahl, sei $(a,p) = 1$. Sei μ wie im Gauß'schen Lemma definiert. Dann gilt*

$$(a-1)\frac{p^2-1}{8} \equiv \mu + \sum_{j=1}^{\frac{p-1}{2}} \lfloor \tfrac{ja}{p} \rfloor.$$

Beweis: Teilen wir eine beliebige ganze Zahl a durch p mit Rest, so erhalten wir die Gleichung

$$a = p\lfloor \tfrac{a}{p} \rfloor + r'(a),$$

mit $0 \le r'(a) < p$. Dabei gilt: Ist $r'(a) \le \frac{p-1}{2}$, so ist $r(a) = r'(a)$. Ist dagegen $r(a) > \frac{p-1}{2}$, so ist $r(a) = r'(a) - p$ (denn in diesem Fall ist $-\frac{p-1}{2} \le r'(a) - p < 0$ und natürlich $r'(a) - p \equiv r'(a) \equiv a \mod p$). Ist also $r(a) > \frac{p-1}{2}$, so ist $r'(a) = r(a) + p$.

Im folgenden sind alle Summierungen über $1 \le j \le \frac{p-1}{2}$, also $\sum$ steht für $\sum_{j=1}^{\frac{p-1}{2}}$. Als erste Gleichung $(*)$ ergibt sich:

$$\begin{aligned}
a\sum j = \sum ja &= \sum \Big(p\lfloor \tfrac{ja}{p} \rfloor + r'(ja)\Big) \\
&= \sum p\lfloor \tfrac{ja}{p} \rfloor + \sum r'(ja) \\
&= \sum p\lfloor \tfrac{ja}{p} \rfloor + \sum r(ja) + p\mu \\
&\equiv \sum \lfloor \tfrac{ja}{p} \rfloor + \sum r(ja) + \mu \mod 2,
\end{aligned}$$

dabei gilt die letzte Kongruenz wegen $p \equiv 1 \mod 2$.

Wie wir im Beweis des Gauß-Lemmas gesehen haben, ist die Folge

$$|r(a)|, |r(2a)|, |r(3a)|, \dots, |r(\tfrac{p-1}{2}a)|$$

eine Permutation der Folge $1, 2, \dots, \frac{p-1}{2}$. Dies liefert das linke Gleichheitszeichen in

$$(**) \qquad \sum j = \sum |r(ja)| \equiv \sum r(ja) \mod 2,$$

das Kongruenzzeichen gilt natürlich für beliebige ganze Zahlen b: es ist $b \equiv -b \mod 2$.

Subtrahieren wir die Gleichung $(**)$ von der Gleichung $(*)$, so erhalten wir

$$(a-1)\sum j = \sum \lfloor \tfrac{ja}{p} \rfloor + \mu \mod 2.$$

Es bleibt noch zu bemerken, dass bekanntlich $\sum_{i=1}^n i = \binom{n+1}{2} = \frac{1}{2} \cdot n(n+1)$ ist. Für $n = \frac{p-1}{2}$ ist $\binom{n+1}{2} = \frac{n(n+1)}{2} = \frac{1}{2}\frac{p-1}{2}\frac{p+1}{2} = \frac{p^2-1}{8}$. Wir können also $\sum j$ durch $\frac{p^2-1}{8}$ ersetzen.

4.4.2. Erster Spezialfall: $a = 2$. Wir erhalten die Regel (Z).

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

Für $a = 2$ erhält man in 4.4.1 links $\frac{p^2-1}{8}$, und rechts erhält man μ, denn alle anderen Summanden sind $\lfloor \frac{ja}{p} \rfloor = \lfloor \frac{j2}{p} \rfloor = 0$ (wegen $2j \le 2\frac{p-1}{2} = p-1$). Das Gauß-Lemma liefert die Behauptung.

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

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

Beweis: Links gibt es in 4.4.1 den Faktor $a - 1 \equiv 0 \mod 2$, also ist die linke Seite Null, demnach ist

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

die Behauptung folgt nun aus dem Gauß'schen Lemma.

4.5. Das quadratische Reziprozitätsgesetz. Zweiter Beweis.

Wir definieren:

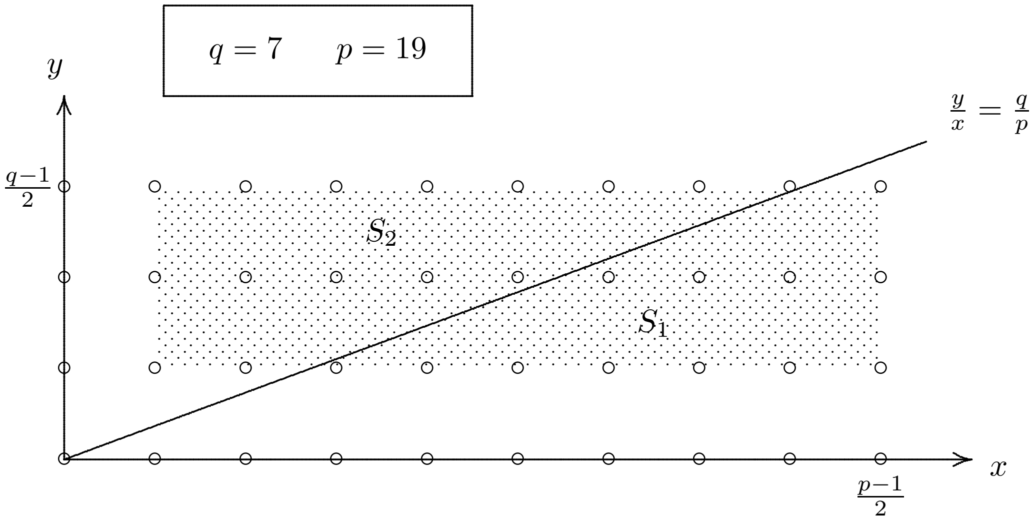
$$S = \{(x,y) \in \mathbb{Z}^2 \mid 1 \le x \le \tfrac{p-1}{2},\ 1 \le y \le \tfrac{q-1}{2}\},$$

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 $y \leq \frac{q}{p}x$ und $x \leq \frac{p-1}{2}$, dass gilt $y \leq \frac{q}{p}x \leq \frac{q}{p} \cdot \frac{p-1}{2} = \frac{q}{2} \cdot p - 1p < \frac{q}{2}$, also $y \leq \frac{q-1}{2}$.). 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 $1 \leq x \leq \frac{p-1}{2}$ (denn aus $yp = qx$ und der Tatsache, dass p, q verschiedene Primzahl sind, folgt $p|x$; für $1 \leq x \leq p-1$ 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

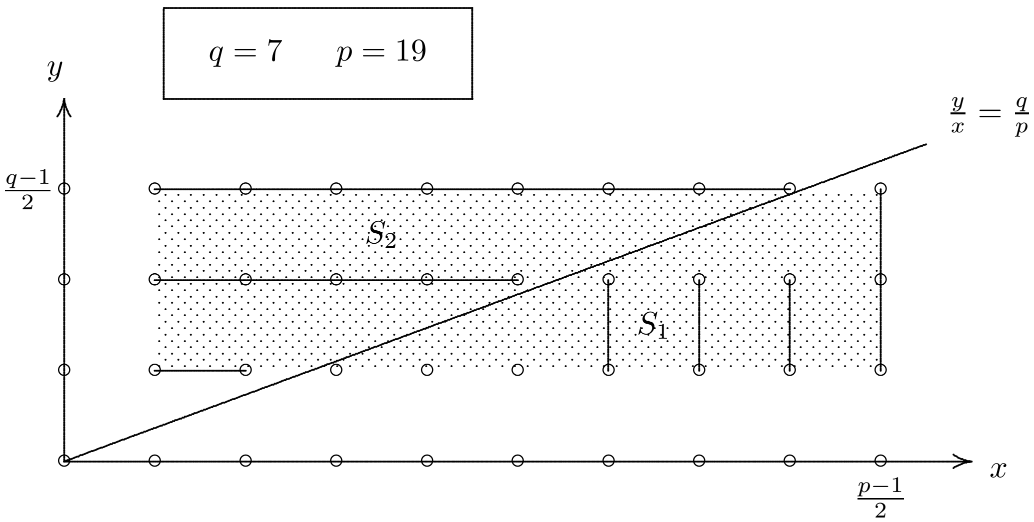
$$|S| = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Die Anzahl der Elemente in S_1 ist

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

Entsprechend gilt

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



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

Wegen 4.4.3 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.

Lemma. *Sei p eine Primzahl mit $p \equiv 3 \mod 4$. 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. Sei $x^2 \equiv 2 \mod q$. 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: $p = 11$. Es ist $11 \equiv 3 \mod 4$ und $23 = 2 \cdot 11 + 1$ ist Primzahl. Also ist 23 ein Teiler von $M_{11} = 2^{11} - 1$ (es gilt: $M_{11} = 2047 = 23 \cdot 89$).

Und $p = 23$. Es ist $23 \equiv 3 \mod 4$ und $47 = 2 \cdot 23 + 1$ ist Primzahl. Also ist 47 ein Teiler von $M_{23} = 8\,388\,607 = 47 \cdot 178\,481$.