7. Das quadratische Reziprozitätsgesetz.

7.0. Erinnerung. Sei p eine ungerade Primzahl, sei $a \in \mathbb{Z}$. In 2.11.4 wurde das *Legendre-Symbol*) $\left(\frac{a}{p}\right)$ eingeführt:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \\ -1 & \text{falls gilt} \\ 0 & \end{cases} \quad \begin{array}{l} a \text{ ist quadratischer Rest modulo } p, \\ a \text{ ist quadratischer Nichtrest modulo } p, \\ p|a. \end{array}$$

Dabei nennt man $a \in \mathbb{Z}$ einen *quadratischen Rest modulo p*, falls a nicht durch p teilbar ist und es ein $b \in \mathbb{Z}$ gibt mit $b^2 \equiv a \mod p$ (natürlich ist dann auch b nicht durch p teilbar), falls also die Restklasse $\overline{a}$ in $\mathbb{F}_p^* = (\mathbb{Z}/p)^*$ ein Quadrat ist. Man nennt $a \in \mathbb{Z}$ einen *quadratischen Nichtrest*, falls wieder a Nicht durch p teilbar ist, und es kein $b \in \mathbb{Z}$ gibt mit $b^2 \equiv a \mod p$ gibt.

Offensichtlich gilt:

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

In 2.11.4 wurde bewiesen:

Das Euler-Kriterium. *Sei p ungerade Primzahl, sei $a \in \mathbb{Z}$. Es ist:*

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

Beweis: Ist p kein Teiler von a, so steht dies in 2.11.4. Ist aber p ein Teiler von a, so sind beide Seiten gleich Null.

Als Folgerungen haben wir dort bewiesen:

(M) (Starke Multiplikativität): Es ist $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ für alle $a, b \in \mathbb{Z}$.

Wichtig ist insbesondere der Spezialfall $a = -1$, hier erhält man nicht nur eine Kongruenz, sondern wirklich Gleichheit:

(-1) (Der Wert für $a = -1$.) Es ist

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

7.1. 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 Frage beantwortet, ob es zu einer vorgegebenen Zahl a ein x mit $x^2 \equiv a \mod p$ gibt oder nicht — offen bleibt dabei aber, wie man ein derartiges x wirklich findet!

Man braucht die folgenden Eigenschaften des Lengendre-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 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ für alle $a, b \in \mathbb{Z}$.

(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

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

Man kann diese Gleichung auch folgendermaßen umschreiben:

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

Beispiel. Hier ein typisches Beispiel, wie man vorgeht: wir berechnen $\left(\frac{42}{61}\right)$.

$$\left(\tfrac{42}{61}\right) \underset{(M)}{=} \left(\tfrac{2}{61}\right)\cdot\left(\tfrac{3}{61}\right)\cdot\left(\tfrac{7}{61}\right), \qquad \text{also braucht man}$$

$$\left(\tfrac{2}{61}\right) \underset{(Z)}{=} -1$$

$$\left(\tfrac{3}{61}\right) \underset{(R)}{=} \left(\tfrac{61}{3}\right) \underset{(K)}{=} \left(\tfrac{1}{3}\right) \underset{(M)}{=} 1$$

$$\left(\tfrac{7}{61}\right) \underset{(R)}{=} \left(\tfrac{61}{7}\right) \underset{(K)}{=} \left(\tfrac{5}{7}\right) \underset{(R)}{=} \left(\tfrac{7}{5}\right) \underset{(K)}{=} \left(\tfrac{2}{5}\right) \underset{(Z)}{=} -1$$

(dabei muss man ausrechnen: $61^2 - 1 = 3720$, und $3720/8 = 465$, und natürlich auch $5^2 - 1 = 24$ und $24/8 = 3$). 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

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

(R) ist das berühmte Gauß'sche Reziprozitäts-Gesetz. Von Gauß selbst gibt es dafür sieben oder acht Beweise, insgesamt gibt es mehr als hundert Beweise und Beweis-Varianten... Wir werden das Reziprozitätsgesetz im Abschnitt 7.4 beweisen. Die Regel (Z) wird in 7.3.2 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 $p^2 - 1 \equiv 1, 9, 9, 1, 1, 9, 9, 1 \mod 16$.

Es ist $p^2 - 1 = 16t + 1$ für ein $t \in \mathbb{Z}$, genau dann, wenn $p \equiv 1, 7, 9, 15 \mod 16$ ist

7.2. Das Gauß'sche Lemma.

Erinnert sei an den folgenden **Beweis des kleinen Fermat:** p sei beliebige Primzahl, $(a, p) = 1$. Dann liefern die Mengen $\{a, 2a, 3a, \ldots, (p-1)a\}$ und $\{1, 2, \ldots, p-1\}$ jeweils genau die Restklassen modulo p (nur eben vielleicht umgeordnet): Die Multiplikation mit a in $\mathbb{Z}/p$ permutiert die Elemente von $(\mathbb{Z}/p)^*$. Dies liefert das linke Kongruenzzeichen:

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

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

Bezeichnen wir mit $r'(x)$ den Rest beim Teilen von x durch p, also die ganze Zahl $r'(x)$ mit $0 \le r'(x) < p$ und $x \equiv r'(x) \mod p$, so sieht man, dass die folgenden beiden Mengen wirklich **gleich** sind:

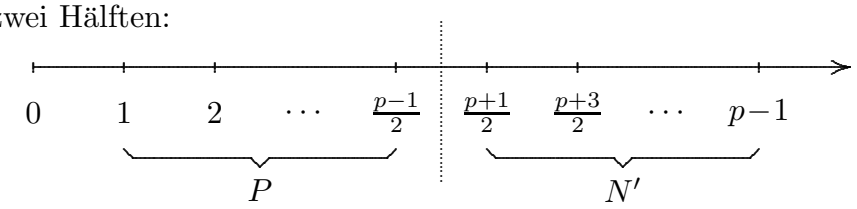
$$\{r'(a), r'(2a), r'(3a), \ldots, r'((p-1)a)\} \quad \text{und} \quad \{1, 2, \ldots, p-1\}$$

und demnach erhält man die Gleichheit

$$\prod_{j=1}^{p-1} j = \prod_{j=1}^{p-1} r'(ja)$$

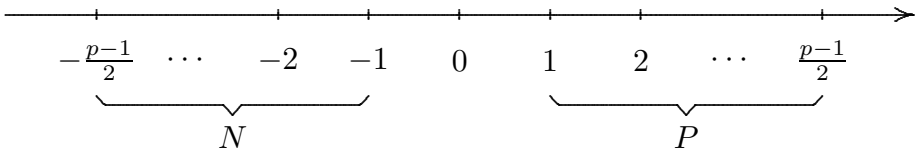
Das Gauß'sche Lemma arbeitet mit dem gleichen Trick, betrachtet aber nur das Produkt $\prod_{j=1}^{(p-1)/2} j$ (dabei ist p eine ungerade Primzahl).

Wir setzen also 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 $-\frac{p-1}{2} \le r(x) \le \frac{p-1}{2}$.

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:

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

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: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$ und erhalten $\left(\frac{a}{p}\right) \equiv (-1)^\mu \mod p$. Da die beiden Zahlen links und rechts den Betrag 1 haben, folgt aus der Kongruenz die Gleichheit.

Bemerkung. Was ist die Bedeutung der Menge $P = \{1, 2, \ldots, \frac{p-1}{2}\}$? Sie liefert alle Quadrate modulo p: *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.

7.3. Eine Folgerung aus dem Gauß'schen Lemma.

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

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

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

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

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

Wir betrachten nun $b = ja$ mit $1 \le j \le \frac{p-1}{2}$. Nach Definition von μ gibt es genau μ Zahlen j mit $1 \le j \le \frac{p-1}{2}$ und $r(ja) < 0$. Für diese Zahlen j gilt also $r'(ja) = r(ja)+p$, für die restlichen Zahlen j gilt $r'(ja) = r(ja)$.

Wir summieren nun über alle j mit $1 \le j \le \frac{p-1}{2}$, dabei schreiben wir einfach das Summenzeichen $\sum$ statt $\sum_{j=1}^{\frac{p-1}{2}}$. Als erste Gleichung $(*)$ ergibt sich:

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

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

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

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

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

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

das Kongruenzzeichen folgt natürlich aus der Tatsache, das für beliebige ganze Zahlen b gilt: es ist $|b| \equiv b \mod 2$.

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

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

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.

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

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

Für $a = 2$ erhält man in 7.3.1 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.