Lemma von Gauß

Wir teilen die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^*$ in zwei Hälften: Die <u>untere</u> Hälfte ist $U := \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{\tfrac{p-1}{2}}\}$, und die <u>obere</u> Hälfte ist $O := \{\overline{\tfrac{p+1}{2}}, \overline{\tfrac{p+3}{2}}, \ldots, \overline{p-1}\}$.

Für $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ ist Multiplikation mit $\bar{a}$ eine Bijektion

$$M_{\bar{a}} : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$$
$$\bar{x} \longmapsto \bar{a}\bar{x}$$

Sei n die Anzahl der Elemente $\bar{u} \in U$ mit $\bar{a}\bar{u} \in O$. Dann ist

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

Bem: Wir zeigen sogar eine allgemeinere Aussage: Seien $U, O \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ mit

$$U \cup O = (\mathbb{Z}/p\mathbb{Z})^*, \quad O = -U, \quad U \cap O = \emptyset.$$

Für $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ ist

$$\left(\frac{a}{p}\right) = (-1)^{\#\{\bar{u} \in U \mid \bar{a}\bar{u} \in O\}}$$

Bew: Seien

$$M_{\bar a}(U) \cap U = \{\bar s_1, \bar s_2, \dots, \bar s_k\}$$

$$M_{\bar a}(U) \cap O = \{\bar r_1, \bar r_2, \dots, \bar r_n\}$$

Beob 1) $0 \neq \bar r_i \neq \bar s_j \neq 0$

2) $n + k = \# U = \frac{p-1}{2}$

3) $O = -U$

$$\Rightarrow \quad 0 \notin U + U$$

$$\Rightarrow \quad 0 \notin M_{\bar a}(U) + M_{\bar a}(U)$$

$$\Rightarrow \quad -\bar r_i \neq \bar s_j$$

Also: $U = \{\bar s_1, \bar s_2, \bar s_3, \dots, \bar s_k, -\bar r_1, -\bar r_2, \dots, -\bar r_n\}$

$$\Rightarrow \quad (-\bar r_1)(-\bar r_2)\cdots(-\bar r_n)\, s_1 \cdots s_k = \bar 1 \cdot \bar 2 \cdot \ldots \cdot \overline{\tfrac{p-1}{2}}$$

$$\parallel$$

$$(-1)^n \, \bar a^{\,n+k} \, \bar 1 \cdot \bar 2 \cdots \overline{\tfrac{p-1}{2}} = \bar 1 \cdot \bar 2 \cdots \overline{\tfrac{p-1}{2}}$$

$$\Rightarrow \quad (-1)^n \, \bar a^{\frac{p-1}{2}} = 1$$

$$\Rightarrow \quad \left(\frac{a}{p}\right) = \bar a^{\frac{p-1}{2}} = (-1)^n$$

☑

Satz Sind p und q ungerade Primzahlen, so ist

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

5ter Beweis von Gauß

mod p \ mod q	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

A1	B1	C1
A2	B2	C2
A3	B3	C3

$m :=$ # blaue Felder in A3

$n :=$ # blaue Felder in C1

Das Lemma von Gauß impliziert

$$\boxed{\left(\frac{p}{q}\right) = (-1)^m \qquad \left(\frac{q}{p}\right) = (-1)^n}$$

$\alpha := \#$ blaue Felder in B2

$\beta := \#$ blaue Felder in B3

$\gamma := \#$ blaue Felder in C2

$\delta := \#$ blaue Felder in C3

__Beob__: Im Bereich

B2	C2
B3	C3

gibt es eine Punktsymmetrie der roten und blauen Felder (induziert durch $n \mapsto pq - n$).

__Folge__: $\alpha + \delta = \frac{p-1}{2} \frac{q-1}{2} = \beta + \gamma$

__Beob__: Im Bereich A3 - B3 - C3 hat jede Zeile $\frac{q-1}{2}$ blaue Felder. In den höheren Zeilen sind es $\frac{q+1}{2}$ blaue Felder. Der Grund ist, daß das letzte blaue Feld in der rechten unteren Ecke von B2 liegt.

Analog: Jede Spalte im Bereich C1-C2-C3 hat $\frac{p-1}{2}$ blaue Felder.

Kor: $$m+\beta+\delta = \frac{p-1}{2}\,\frac{q-1}{2} = n+\gamma+\delta$$

Also: $$\begin{aligned}\frac{p-1}{2}\,\frac{q-1}{2} &= \alpha+\delta\\ &= \beta+\gamma\\ &= m+\beta+\delta\\ &= n+\gamma+\delta\end{aligned}$$

Also ist:
$$\begin{aligned}m+n+\frac{p-1}{2}\,\frac{q-1}{2} &= m+\beta+n+\gamma\\ &= \frac{p-1}{2}\,\frac{q-1}{2}-\delta+\frac{p-1}{2}\,\frac{q-1}{2}-\delta\\ &= 2\alpha\end{aligned}$$

Wichtig ist nur, daß
$$m+n+\frac{p-1}{2}\,\frac{q-1}{2}$$
gerade ist. Damit ist
$$(-1)^{m+n+\frac{p-1}{2}\,\frac{q-1}{2}} = 1$$

$\boxtimes$

Eisensteins geometrischer Beweis

Lemma: Sei p eine ungerade Primzahl und a teilerfremd zu $2p$. Dann ist:

$$\left(\frac{a}{p}\right) = (-1)^t \quad \text{mit} \quad t = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor$$

Beweis: Der Rest, den ia modulo p läßt ist $ia - p\left\lfloor \frac{ia}{p} \right\rfloor$. Sei $\{s_1, \ldots, s_h\}$ die Menge dieser Reste $< \frac{p}{2}$ und $\{r_1, \ldots, r_n\}$ die Menge der Reste $> \frac{p}{2}$.

Wir wissen $\left(\frac{a}{p}\right) = (-1)^n$ nach dem Lemma von Gauß.

Nun ist:

$$\sum_{i=1}^{\frac{p-1}{2}} ia = p \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor + \sum_{j=1}^{n} r_n + \sum_{j=1}^{h} s_h$$

Die Menge <u>aller</u> Reste $< \frac{p}{2}$ ist

$$\{s_1, \ldots, s_h, p - r_1, \ldots, p - r_n\}$$

Also ist

$$\sum_{i=1}^{\frac{p-1}{2}} i = \sum_{j=1}^{n} p - r_j \quad + \sum_{j=1}^{k} s_k$$

$$= np + \sum_{j=1}^{k} s_k - \sum_{j=1}^{n} r_n$$

Wir subtrahieren:

$$(a-1)\sum_{i=1}^{\frac{p-1}{2}} i = p\left[-n + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \right] + \underbrace{2\sum_{j=1}^{n} r_j}_{\text{gerade}}$$

Also

$$(a-1)\,\frac{p^2-1}{8} \equiv \left(-n + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor\right) p \mod 2$$

$$\equiv -n + t \mod 2$$

Da $a-1$ gerade ist, haben n und t gleiche Parität. $\boxtimes$

Nun zum Reziprozitätsgesetz:

Sei $M := \{ (x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2} \}$

Dann ist $\# M = \frac{p-1}{2} \frac{q-1}{2}$.

Wir zerlegen M ist zwei disjunkte Teile $M = U \cup O$

$$U := \left\{ (x,y) \in M \;\middle|\; \frac{x}{y} < \frac{p}{q} \right\}$$

$$O := \left\{ (x,y) \in M \;\middle|\; \frac{x}{y} > \frac{p}{q} \right\}$$

$\ulcorner$ $\frac{x}{y} = \frac{p}{q} \Rightarrow xq = yp$ kommt für $1 \leq x < p$ und $1 \leq y < q$ nicht vor $\lrcorner$

<u>Beob</u>: $U = \left\{ (x,y) \in \mathbb{Z}\times\mathbb{Z} \;\middle|\; 1 \leq x \leq \frac{p-1}{2},\ 1 \leq y < \frac{qx}{p} \right\}$

$$\Rightarrow \# U = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor$$

$$\Rightarrow \left(\frac{q}{p}\right) = (-1)^{\# U}$$

Analog: $\left(\frac{p}{q}\right) = (-1)^{\# O}$

<u>Also</u>: $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\# U + \# O} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ $\boxtimes$

Zolotarevs Beweis

Lemma von Zolotarev

Wir betrachten wieder die Bijektion

$$\mu_{\bar{a}} : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$$

Als Permutation der endlichen Menge hat $\mu_{\bar{a}}$ ein Vorzeichen $\sigma(\bar{a}) := (-1)^{\mu_{\bar{a}}}$.

Es ist $\sigma(\bar{a}) = \left(\frac{a}{p}\right)$.

Bew: Sei $\bar{g} \in (\mathbb{Z}/p\mathbb{Z})^*$ ein primitives Element.

Dann ist $\mu_{\bar{g}}$ eine zyklische Vertauschung von $p-1$ Elementen und hat Vorzeichen $\sigma(\bar{g}) = (-1)^{p-2} = -1$.

Dann ist $\sigma(\bar{g}^k) = (-1)^k = 1$ genau dann, wenn k gerade ist. $\boxtimes$

2ter Bew: Euler's Kriterium:

$\bar{a}$ ist quadr. Rest

$$\iff \bar{a}^{\frac{p-1}{2}} = 1$$

$$\iff \operatorname{ord}(\bar{a}) \mid \frac{p-1}{2}$$

$\Leftrightarrow \quad \frac{p-1}{\mathrm{ord}(\bar{a})}$ ist gerade

<u>Bem:</u> $\mathrm{ord}(\bar{a})$ ist die Länge einer <u>Bahn</u>

$\{\bar{x}, \bar{a}\bar{x}, \bar{a}^2\bar{x}, \dots\}$

und $\frac{p-1}{\mathrm{ord}(\bar{a})}$ ist die Anzahl der Bahnen.

(*) <u>Bem:</u> $\mathrm{ord}(\bar{a}) \cdot \#\text{Bahnen} = p-1$: gerade

Also: #Bahnen ungerade $\Rightarrow$ $\mathrm{ord}(\bar{a})$ gerade

<u>Erinnerung:</u>

$$(-1)^{\mu} = (-1)^{\#\substack{\text{Anzahl der Bahnen} \\ \text{gerader Länge}}}$$

$$= \begin{cases} 1 : & \mathrm{ord}(\bar{a}) \text{ ungerade } \underline{\text{oder}} \\ & \frac{p-1}{\mathrm{ord}(a)} \text{ gerade} \\ -1 : & \mathrm{ord}(\bar{a}) \text{ gerade } \underline{\text{und}} \\ & \frac{p-1}{\mathrm{ord}(\bar{a})} \text{ ungerade} \end{cases}$$

$$\underset{(*)}{=} \left\{ \begin{array}{ll} 1 : & \frac{p-1}{\mathrm{ord}(a)} \text{ gerade} \\ -1 : & \frac{p-1}{\mathrm{ord}(a)} \text{ ungerade} \end{array} \right\} = \left(\frac{a}{p}\right)$$

$\boxtimes$

Die grundlegende Strategie ist schon sehr elegant:

Finde Permutationen

$$\sigma, \tau, \mu : X \to X$$

mit

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

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

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

$$\mu = \sigma^{-1}\tau$$

Dann folgt die Behauptung aus den Tatsachen

$$(-1)^{(\alpha\beta)} = (-1)^{\alpha}(-1)^{\beta}$$

$$(-1)^{(\alpha^{-1})} = (-1)^{\alpha}$$

Für die Menge X wählen wir das „Rechteck"

Chinesischer Restsatz

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \overset{\downarrow}{=} \mathbb{Z}/pq\mathbb{Z}$$

Wir repräsentieren das Rechteck in der Weise, die wir schon aus Gauß' 5tem Beweis kennen.

0	15	30	10	25	5	20
21	1	16	31	11	26	6
7	22	2	17	32	12	27
28	8	23	3	18	33	13
14	29	9	24	4	19	34

LU

Es gibt noch zwei weitere einfache Schemata:

LO

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

RU

0	5	10	15	20	25	30
1	6	11	16	21	26	31
2	7	12	17	22	27	32
3	8	13	18	23	28	33
4	9	14	19	24	29	34

Die Permutationen können wir definieren, indem wir die Schemata „übereinandr legen":

0 0 → 0	1 15 → 5	2 30 → 10	3 10 → 15	4 25 → 20	5 5 → 25	6 20 → 30
7 21 → 1	8 1 → 6	9 16 → 11	10 31 → 16	11 11 → 21	12 26 → 26	13 6 → 31
14 7 → 2	15 22 → 7	16 2 → 12	17 17 → 17	18 32 → 22	19 12 → 27	20 27 → 32
21 28 → 3	22 8 → 8	23 23 → 13	24 3 → 18	25 18 → 23	26 33 → 28	27 13 → 33
28 14 → 4	29 29 → 9	30 9 → 14	31 24 → 19	32 4 → 24	33 19 → 29	34 34 → 34

Die Permutationen μ, σ, τ sind:

$$\boxed{\begin{array}{l} 0 \le k \le 4 \\ 0 \le j \le 6 \end{array}}$$

$$k \cdot 7 + j = (n \bmod 5)7 + (n \bmod 7)$$

$$\begin{tikzcd}
(n \bmod 5)7 + (n \bmod 7) = k\cdot 7 + j \arrow[r, mapsto, "\mu"] & j \cdot 5 + k = (n \bmod 7)5 + (n \bmod 5) \\
n \arrow[u, mapsto, "\sigma"] \arrow[ur, mapsto, "\tau"'] &
\end{tikzcd}$$

Beob: σ erhält Spalten (Reste mod q), denn die Schemata LU und LO setzen n in die Spalte n mod q.

Genauer: Sei (j,k) das Feld $\equiv j \bmod p$ und $\equiv k \bmod q$

Dann ist $\sigma(j,k)$ das Feld $\equiv j \bmod p$ und $\equiv pk+j \bmod q$

Beob: Die Permutation

$$\pi_j : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$$
$$k \longmapsto pk+j$$

hat Vorzeichen $(-1)^{\pi_j} = \left(\frac{p}{q}\right)$, denn

$$\pi_j = \underbrace{(x \mapsto x+j)}_{\mathrm{sgn}=1} \circ \underbrace{(x \mapsto px)}_{\mathrm{sgn}=\left(\frac{p}{q}\right)}$$

$\ulcorner$ $j=0$: $x \mapsto x+j$ ist die Identität

$j \neq 0$: $x \mapsto x+j$ ist Zykel ungerader Länge $\lrcorner$

Kor: $\sigma = \prod_{j=0}^{p-1} \pi_j$ hat Vorzeichen

p ist ungerade

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

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

Nun berechnen wir das Vorzeichen $(-1)^{\mu}$.

Erinnerung: $\mu(kp+j) = jq+k$

$$\left(\underset{\text{Spalte}}{j} = 0, \dots, p-1 \qquad \underset{\text{Zeile}}{k} = 0, \dots, q-1 \right)$$

Beob: $kp + j < k'p + j' \iff k < k'$ oder $k = k'$ und $j < j'$

$$\big\downarrow \mu \qquad\qquad \big\downarrow \mu$$

$jq + k > j'q + k' \iff j > j'$ oder $j = j'$ und $k > k'$

Also kehrt μ die Ordnung genau dann um, wenn $k < k'$ und $j > j'$ ist.

<u>Beob</u>: Das sind genau $\binom{p}{2}\binom{q}{2}$ Paare

$$\{(k,j),(k',j')\} \text{ die } \mu \text{ umkehrt}$$

<u>Also</u>:
$$
\begin{aligned}
(-1)^M &= (-1)^{\binom{p}{2}\binom{q}{2}} \\
&= (-1)^{\frac{p(p-1)}{2}\frac{q(q-1)}{2}} \\
&= \left((-1)^{pq}\right)^{\frac{p-1}{2}\frac{q-1}{2}} \qquad pq \text{ ist ungerade} \\
&= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}
\end{aligned}
$$

$\boxtimes$