Wichtige Sätze und Definitionen zu
§4: Das quadratische Reziprozitätsgesetz
aus der Vorlesung:

LV-NR	150 239
Veranstaltung	Diskrete Mathematik II, 4.0 std
Dozent	Holtkamp, R.

4.1
G sei Gruppe (mit multiplikativ geschriebener Verknüpfung) und $a \in G$. Dann heißt

$$\operatorname{ord}(a) := \begin{cases} \infty & \text{falls } a^k \neq 1_G \ \forall\ k \geq 1 \\ \min\left\{k \geq 1 \mid a^k = 1_G\right\} & \text{sonst} \end{cases}$$

Ordnung *von a (in G).*
(Analog für additiv geschriebene Gruppen: $\min\{k \in \mathbb{N} \mid k \cdot a = 0\}$*)*

Beispiele
$(\mathbb{Z}/7\mathbb{Z})^*$ *multiplikative Gruppe bzgl „$\cdot$“, Elemente* $\bar{1}, \bar{2}, \bar{3}$ *und* $-\bar{1}, -\bar{2}, -\bar{3}$.
$\operatorname{ord}(\bar{1}) = 1$, $\operatorname{ord}(\bar{2}) = 3$, $\operatorname{ord}(\bar{3}) = 6$, $\operatorname{ord}(-\bar{1}) = 2$, $\operatorname{ord}(-\bar{2}) = 6$, $\operatorname{ord}(-\bar{3}) = 3$

Satz 1 (Elementordnung teilt Gruppenordnung)
Ist G endliche Gruppe ($\#G < \infty$) so gilt

$$\operatorname{ord}(a) \,\big|\, \#G \ \forall\ a \in G$$

d.h. $\#G$ ist Vielfaches von $\operatorname{ord}(a)$.
Weiterhin gilt: Wenn $\operatorname{ord}(a) = n < \infty$, so ist

$$\langle a \rangle := \left\{a^i \mid 0 \leq i < n\right\}$$

Untergruppe von G mit n Elementen.

4.2
$\langle a \rangle$ heißt die **von a erzeugte Untergruppe**. *Speziell heißt G* **zyklisch**, *wenn ein a existiert mit $\langle a \rangle = G$ (d.h. wenn ein a existiert mit* $\operatorname{ord}(a) = \#G$*).*

Satz 2 (kleiner Fermat)
$p \in \mathbb{N}$ sei Primzahl, $p \geq 2$.

$$\begin{aligned} a \in \mathbb{Z}/p\mathbb{Z} \quad \Rightarrow \quad & a^p = a \\ & a^{p-1} = 1 \quad (\text{wenn } a \neq 0,\ p > 2) \\ & a^{\frac{p-1}{2}} \in \{+1, -1\} \quad (\text{wenn } a \neq 0,\ p > 2) \end{aligned}$$

Satz 3 (Zyklizität von $(\mathbb{Z}/p\mathbb{Z})^*$)

$$p \text{ Primzahl} \quad \Longrightarrow \quad \exists\ a \in (\mathbb{Z}/p\mathbb{Z})^* \text{ mit } \operatorname{ord}(a) = p - 1$$

Insbesondere existiert für jedes solche a genau ein Isomorphismus

$$\begin{aligned}(\mathbb{Z}/(p-1)\mathbb{Z},+) &\to \left((\mathbb{Z}/p\mathbb{Z})^*,\cdot\right)\\ \bar{1} &\mapsto a\end{aligned}$$

Beispiel
Isomorphismus zwischen $(\mathbb{Z}/10\mathbb{Z},+)$ *und* $\left((\mathbb{Z}/11\mathbb{Z})^*,\cdot\right)$.

4.3

a) Für $m,n\in\mathbb{N}$, $a\in\mathbb{Z}$ *mit* $\operatorname{ggT}(a,m)=1$ *heißt* a *ein* **n-ter Potenzrest** *modulo* m, *falls die Gleichung*

$$X^n\equiv a \mod m$$

in $\mathbb{Z}$ *lösbar ist.*
Speziell heißt a **quadratischer Rest** ($\mod m$) *falls*

$$X^2\equiv a \mod m$$

lösbar ist. Andernfalls heißt a **quadratischer Nichtrest**.

b) Sei $p>2$ *Primzahl,* $a\in\mathbb{Z}$, $\operatorname{ggT}(a,p)=1$. *Dann heißt*

$$\left(\frac{a}{p}\right):=\begin{cases}1 & \text{falls } a \text{ quadratischer Rest modulo } p\\ -1 & \text{falls } a \text{ quadratischer Nichtrest modulo } p\end{cases}$$

Legendre-Symbol *(„a nach p“).*

Beispiel
2 *ist quadratischer Rest* $\mod 7$, *denn* $3^2\equiv 2 \mod 7$.
2 *ist quadratischer Nichtrest* $\mod 3$, *denn* $1^2\not\equiv 2 \mod 3$ *und* $2^2\not\equiv 2 \mod 3$.

Satz 4 (Rechenregeln Legendre-Symbol)
$p>2$ prim.

(i) Wenn $a,b\in\mathbb{Z}$, $a\equiv b \bmod p$, $\operatorname{ggT}(a,p)=1$ so ist $\operatorname{ggT}(b,p)=1$ und

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

(ii) Wenn $a,b\in\mathbb{Z}$, $\operatorname{ggT}(a,p)=1$, $\operatorname{ggT}(b,p)=1$ so ist $\operatorname{ggT}(a\cdot b,p)=1$ und

$$\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$$

(iii) Wenn $\operatorname{ggT}(a,p)=1$, $\overline{a}=\pi_p(a)$, $\operatorname{ord}(\overline{a})=p-1$ so ist

$$\left(\frac{a}{p}\right)=-1,\ \left(\frac{a^i}{p}\right)=(-1)^i \text{ für } i\geq 1$$

(iv) Wenn $\mathrm{ggT}(a,p)=1$ und $\overline{a}=\pi_p(a)$, so ist

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

Übung
Ist $p\equiv 1 \bmod 4 \quad\Longrightarrow\quad -1$ *ist Quadrat* mod$p$.
Ist $p\equiv 3 \bmod 4 \quad\Longrightarrow\quad -1$ *kein Quadrat* mod$p$.

Satz 5 (Quadratisches Reziprozitätsgesetz)
$p\neq q$ seine Primzahlen >2. Dann:

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=\begin{cases}-1 & \text{falls } p\equiv 3 \bmod 4 \text{ und } q\equiv 3 \bmod 4\\ +1 & \text{sonst}\end{cases}$$

Weiterhin:

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

$$\left(\frac{2}{p}\right)=\begin{cases}+1 & \text{falls } p\equiv \pm 1 \bmod 8\\ -1 & \text{falls } p\equiv \pm 3 \bmod 8\end{cases}$$

Beispiel (Gaußsches Lemma)
Ist $p>2$ *prim,* $a\in\mathbb{Z}$ *mit* $\mathrm{ggT}(a,p)=1$ *, so sei* $\mu_p(a)$ *die Anzahl aller* $j\in\left\{1,\ldots,\frac{p-1}{2}\right\}$*, deren Produkt mit* a *eine negative Restklasse im Repräsentantensystem* $\left\{-\frac{p-1}{2},\ldots,\frac{p-1}{2}\right\}$ *von* $\mathbb{Z}_p$ *hat. Dann ist*

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

Beispiel
Wieder folgt:

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}+1 & \textit{falls } p\equiv \pm 1 \bmod 8\\ -1 & \textit{falls } p\equiv \pm 3 \bmod 8\end{cases}$$

da $\mu_p(-1)=\#\left\{j\in 1,\ldots,\frac{p-1}{2}\mid -j<0\right\}=\frac{p-1}{2}$.

Beispiele
$\left(\frac{2}{7}\right)=1$, $\left(\frac{2}{17}\right)=1$, $\left(\frac{2}{11}\right)=-1$, $\left(\frac{2}{5}\right)=-1$,
$\left(\frac{17}{31}\right)=-1$, $\left(\frac{17}{23}\right)=-1$, $\left(\frac{-87}{103}\right)=1$,
Für p *Primzahl der Form* $6k+1$*:* $\left(\frac{-3}{p}\right)=1$.

4.4
Für $a \in \mathbb{Z}$ und ungerades $n \in \mathbb{N}_{\geq 3}$ mit $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$, p_i prim $1 \leq i \leq r$, heißt

$$\left(\frac{a}{n}\right)_J := \begin{cases} 0 & , \text{ falls } \mathrm{ggT}(a,n) > 1 \\ \left(\frac{a}{p_1}\right)^{e_1} \cdot \left(\frac{a}{p_2}\right)^{e_2} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{e_r} & , \text{ sonst} \end{cases}$$

Jacobi-Symbol.

Bemerkung 4.1
Man beachte, dass $\mathrm{ggT}(a,p_i) = 1 \ \forall \ i$, wenn $\mathrm{ggT}(a,n) = 1$. Ist $n = p_1$ prim, $\mathrm{ggT}(a,n) = 1$, so ist $\left(\frac{a}{p_1}\right)_J = \left(\frac{a}{p_1}\right)$. Das Jacobi-Symbol ist also eine Erweiterung des Legendre-Symbols und man schreibt meist auch $\left(\frac{a}{n}\right)$ für $\left(\frac{a}{n}\right)_J$.

Beispiele
$\left(\frac{15}{9}\right)_J = 0$
$\left(\frac{-1}{15}\right)_J = -1$
$\left(\frac{2}{15}\right)_J = 1$, *aber 2 ist quadratischer Nichtrest modulo 15!*
$\left(\frac{11}{91}\right)_J = -1$

Satz 6 (Rechenregeln für das Jacobi-Symbol und Reziprozitätsgesetz)
Seien $m, n \in \mathbb{N}_{\geq 3}$ ungerade. Dann

(i) $\forall \ a, b \in \mathbb{Z}$ mit $a \equiv b \bmod n$ ist

$$\left(\frac{a}{n}\right)_J = \left(\frac{b}{n}\right)_J$$

(ii) $\forall \ a, b \in \mathbb{Z}$ gilt:

$$\left(\frac{a \cdot b}{n}\right)_J = \left(\frac{a}{n}\right)_J \cdot \left(\frac{b}{n}\right)_J$$

(iii) falls $\mathrm{ggT}(m,n) = 1$ gilt:

$$\left(\frac{n}{m}\right)_J \cdot \left(\frac{m}{n}\right)_J = \begin{cases} -1 & \text{wenn } m \equiv n \equiv 3 \bmod 4 \\ +1 & \text{sonst} \end{cases}$$

(iv)

$$\left(\frac{1}{n}\right)_J = 1$$

(v)

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

(vi)

$$\left(\frac{2}{n}\right)_J = \begin{cases} 1 & n \equiv \pm 1 \bmod 8 \\ -1 & n \equiv \pm 3 \bmod 8 \end{cases}$$

Beispiel
$\mathrm{ggT}(127, 703) = 1$, $\left(\frac{127}{703}\right)_J = -\left(\frac{703}{127}\right)_J = -1$.

$\left(\frac{57}{77}\right)_J = \left(\frac{77}{57}\right)_J = \left(\frac{20}{57}\right)_J = \ldots = -1.$
$\left(\frac{57}{77}\right)_J = \left(\frac{57}{7}\right) \cdot \left(\frac{57}{11}\right) = \ldots = -1.$

Beispiel (Solovay-Strassen-Test)
Gegeben eine (große) ungerade Zahl n. Der Test stellt entweder fest, dass n keine Primzahl ist (diese Antwort ist immer korrekt) oder dass „ohne Garantie“ eine Primzahl vorliegt. Im Fall dass n keine Primzahl ist, wird die zweite Antwort mit einer Wahrscheinlichkeit $< \frac{1}{2^k}$ gegeben, k wählbar. Hierbei wählt man eine Anzahl $k > 1$ von Schritten und eine zufällige Folge $a_1, \ldots, a_k$ von Zahlen mit $1 < a_i < n - 1$ (für $a \leq 1 \leq k$). Berechnet wird in jedem Schritt:

$$g_i := \mathrm{ggT}\,(a_i, n)$$

Notwendig für Primzahl ist

$$1.) \quad g_i = 1$$

Falls OK, wird

$$b_i := a_i^{(n-1)/2} \mod n$$

berechnet in $\left\{-\frac{n-1}{2}, \ldots, \frac{n-1}{2}\right\}$ Ist

$$2.) \quad b_i = \pm 1$$

so wird auch noch $\left(\frac{a_i}{n}\right)_J$ berechnet. Falls n prim, so muss

$$3.) \quad b_i = \left(\frac{a_i}{n}\right)_J$$

gelten. Hohe Wahrscheinlichkeit für Primzahl, wenn für alle a_i nacheinader $1.) - 3.)$ OK.

Aufgabe

Es sei $E_{529} = \left\{a \in (\mathbb{Z}/529\mathbb{Z}) - \{1, 528\} \mid a^{264} = \pm 1\right\}$ und $E'_{529} = \left\{a \in E_{529} \mid a^{264} = \left(\frac{a}{529}\right)\right\}$.
Man berechne $\#E_{529}$ und $\#E'_{529}$.

Man beachte, dass $529 = 23 * 23$ ist. Es ist $E_{529} \subseteq (\mathbb{Z}/529\mathbb{Z})^*$ und $\#\left(\mathbb{Z}/529\mathbb{Z}\right)^* = 22 \cdot 23$. Wir zerlegen $(\mathbb{Z}/529\mathbb{Z})^*$ in $U \times V$ mit

$$U = \left\{a \in (\mathbb{Z}/529\mathbb{Z})^* \mid a^{22} \equiv 1 \bmod 529\right\}$$

und

$$V = \left\{a \in (\mathbb{Z}/529\mathbb{Z})^* \mid a \equiv 1 \bmod 23\right\}$$

wobei $\#U = 22$ und $\#V = 23$. Wir betrachten statt der Menge

$$\left\{a \in (\mathbb{Z}/529\mathbb{Z}) \mid a^{264} = \pm 1\right\}$$

die Menge

$$\left\{(b, c) \in U \times V \mid (b, c)^{264} = \pm (1, 1)\right\}$$

und beachten, dass die Ordnungen der Elemente von U in $\{1, 2, 11, 22\}$ liegen, während die von 1 verschiedenen Elemente von V die Ordnung 23 haben. Es ist also

$$\begin{aligned} b^{264} &= \left(b^{22}\right)^{12} \\ &= 1 \end{aligned}$$

für alle $b \in U$. Damit auch $c^{264} = 1$ gilt, ist es notwendig, dass $1 = c^{2 \cdot 264} = c^{23 \cdot 23} c^{-1} = c^{-1}$, also dass $c = 1$. Somit folgt

$$\left\{(b, c) \in U \times V \mid (b, c)^{264} = \pm (1, 1)\right\} = \{(b, c) \mid b \in U,\ c = 1\}.$$

Diese Menge hat $\#U = 22$ Elemente. Daher ist

$$\#E_{529} = 22 - 2 = 20.$$

Weiterhin gilt $\#E'_{529} = \#E_{529}$, da

$$\left(\frac{a}{529}\right) = \left(\frac{a}{23 \cdot 23}\right) = \left(\frac{a}{23}\right)^2 = 1.$$