4 Prime Restklassen und der Satz von Euler-Fermat

Einleitung

- *Eigenschaften von $\mathbb{Z}/n\mathbb{Z}$*
- *Lösung von Kongruenzen*
- *Satz von Euler-Fermat*

Definition 4.1 (Nullteiler)**.** Es sei R ein Ring. Ein Element $x \in R$ heißt ein Nullteiler, wenn es ein $y \in R, y \neq 0$ mit $xy = 0$ gibt. Der Ring R heißt nullteilerfrei, wenn $R \neq 0$ ist und 0 der einzige Nullteiler in R ist.

Anmerkung: Der Nullring ist nicht nullteilerfrei und die 0 ist kein Nullteiler, da kein $y \in R, y \neq 0$ existiert.

Beispiel 4.2.
- Nullring hat keinen Nullteiler, da kein $y \in R$, $y \neq 0$ existiert.
- Nullteiler in $\mathbb{Z}/3\mathbb{Z} : \overline{0}$, also ist $\mathbb{Z}/3\mathbb{Z}$ nullteilerfrei.
- Nullteiler in $\mathbb{Z}/4\mathbb{Z} : \overline{0}$, $\overline{2}$ ($\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$), also nicht nullteilerfrei.

Definition 4.3 (Einheit)**.** Es sei R ein Ring. Ein Element $x \in R$ heißt eine Einheit, wenn es ein $y \in R$ mit $xy = 1$ gibt. Bezeichnung: $x^{-1} := y$. Die Einheiten im Ring $\mathbb{Z}/n\mathbb{Z}$ heißen prime Restklassen modulo n. *also: wenn ein Inverses bezüglich Multiplikation existiert*

Beispiel 4.4.
- Einheiten in $\mathbb{Z}/3\mathbb{Z} : \overline{1}$, $\overline{2}$ ($\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$).
- Einheiten in $\mathbb{Z}/4\mathbb{Z} : \overline{1}, \overline{3}$: ($\overline{3} \cdot \overline{3} = \overline{9} = \overline{1}$)

Lemma 4.5. Es sei R ein Ring. Dann gilt

(a) $R^\times := \{x \in R \mid x \text{ ist eine Einheit}\}$ ist eine abelsche Gruppe bezüglich der Multiplikation, die sogenannte Einheitengruppe von R. Insbesondere gibt es für jedes $x \in R^\times$ genau ein $y \in R^\times$ mit $xy = 1$. Dieses Element bezeichnen wir mit x^{-1} und nennen es das (multiplikativ) Inverse zu x.

Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ wird als prime Restklassengruppe modulo n bezeichnet.

(b) Ist $x \in R^\times$, dann ist x kein Nullteiler.

(c) Falls R endlich ist, dann gilt auch die Umkehrung von (b): Ist $x \in R$ kein Nullteiler, dann ist x eine Einheit.

Insbesondere gilt im Fall $R = \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$, für $\overline{x} \in R$, dass $\overline{x}$ genau dann eine Einheit ist, wenn $\overline{x}$ kein Nullteiler ist.

Beweis. (a) Sind $a, b \in R^\times$, dann ist auch $ab \in R^\times$, denn dann existieren $c, d \in R$ mit $ac = 1$, $bd = 1$, damit folgt $(ab)(cd) = (ac)(bd) = 1$.

Assoziativität und Kommutativität folgen aus der Multiplikation in R.

Neutrales Element: $1 \in R^\times$ wegen $1 \cdot 1 = 1$.

Inverse: Ist $a \in R^\times$, dann existiert nach Definition ein $b \in R$ mit $ab = 1 \implies ba = 1$. Damit folgt $b \in R^\times$.

Damit ist $R^\times$ eine abelsche Gruppe bezüglich der Multiplikation.

(b) Falls $R = 0$, dann ist $0 = 1$ also eine Einheit, aber kein Nullteiler. Falls $R \neq 0$: Sei $x \in R^\times$ und $y \in R$ mit $xy = 0$. Damit folgt $y = x^{-1}xy = x^{-1} \cdot 0 = 0$, also ist x kein Nullteiler.

(c) Sei R endlich und $x \in R$ kein Nullteiler. Wir betrachten die Abbildung $\tau : R \to R, a \mapsto xa$. τ ist injektiv, denn aus $\tau(a) = \tau(b)$ folgt $xa = xb \implies x(a-b) = 0$. Da x kein Nullteiler ist, folgt damit $a - b = 0 \implies a = b$. Als injektive Selbstabbildung der endlichen Menge R ist τ auch surjektiv, damit existiert ein $y \in R$ mit $\tau(y) = 1$, was $xy = 1$ und deshalb $x \in R^\times$ impliziert.

□

Definition 4.6 (Körper)**.** Ein Ring R heißt ein Körper, wenn $R^\times = R \setminus \{0\}$ ist.

Anmerkung: Nullring $R = 0$ ist nach Definition kein Körper

Beispiel 4.7. $\mathbb{Z}/3\mathbb{Z}$ ist ein Körper, $\mathbb{Z}/4\mathbb{Z}$ ist kein Körper.

Satz 4.8. Es sei $n \in \mathbb{N}$. Dann sind äquivalent

(i) n ist eine Primzahl

(ii) $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper

(iii) $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei.

Für Primzahlen p schreiben wir auch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Beweis. (i) $\implies$ (ii): Sei n eine Primzahl, $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \neq 0$. Zz.: $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Wegen $\overline{a} \neq 0$ folgt $n \nmid a$. Da n eine Primzahl ist, erhalten wir $\mathrm{ggT}(n, a) = 1$. Aufgrund des erweiterten Euklidischen Algorithmus gibt es $u, v \in \mathbb{Z}$ mit $un + va = 1 \implies \overline{un} + \overline{va} = \overline{1} \implies \overline{v} \cdot \overline{a} = \overline{1}$. Mit $\overline{a}^{-1} := \overline{v}$ folgt $a \in R^\times$.

(ii) $\implies$ (iii): Sei $\mathbb{Z}/n\mathbb{Z}$ ein Körper. Damit ist $\mathbb{Z}/n\mathbb{Z} \neq 0$ und $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$. Wegen 4.5 (b) ist dann $\overline{0}$ der einzige Nullteiler in $\mathbb{Z}/n\mathbb{Z}$, d.h. $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei.

(iii) $\implies$ (i): Kontraposition: Sei n keine Primzahl. Falls $n = 1$, dann ist $\mathbb{Z}/n\mathbb{Z} = 0$, also nicht nullteilerfrei. Falls $n > 1$ ist, dann gibt es $a, b \in \mathbb{N}$ mit $1 < a, b < n$, so dass $n = ab$ gilt. Damit folgt $\overline{0} = \overline{n} = \overline{ab} = \overline{a}\overline{b}$ mit $\overline{a}, \overline{b} \neq 0$, also sind $\overline{a}$, $\overline{b}$ Nullteiler, insbesondere ist $\mathbb{Z}/n\mathbb{Z}$ nicht nullteilerfrei. □

Anmerkung: Letzte Woche haben wir bereits Kongruenzrelationen in $\mathbb{Z}$ kennengelernt, heute: lernen Kongruenzen zu lösen. Frage: Wann hat eine Kongruenz eine Lösung in $\mathbb{Z}$?

Lemma 4.9. Es seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Dann sind äquivalent:

(i) Die Kongruenz $ax \equiv b \pmod{n}$ besitzt eine Lösung in $\mathbb{Z}$.

(ii) $\mathrm{ggT}(a, n) \mid b$.

Beweis. (i) $\implies$ (ii): Sei $x \in \mathbb{Z}$ mit $ax \equiv b \pmod{n}$. Dann gilt $n \mid (ax - b) \implies \exists k \in \mathbb{Z}$ mit $ax - b = kn$, also mit $b = ax - kn$. Wegen $\mathrm{ggT}(a, n) \mid a$ und $\mathrm{ggT}(a, n) \mid n$ folgt $\mathrm{ggT}(a, n) \mid b$.

(ii) $\implies$ (i): Es gelte $\mathrm{ggT}(a, n) \mid b$. Aus dem erweiterten Euklidischen Algorithmus folgt die Existenz von u, $v \in \mathbb{Z}$ mit

$$ua + vn = \mathrm{ggT}(a, n).$$

Durch Multiplikation mit der nach Voraussetzung ganzen Zahl $\frac{b}{\mathrm{ggT}(a,n)}$ erhalten wir

$$ua\frac{b}{\mathrm{ggT}(a,n)} + vn\frac{b}{\mathrm{ggT}(a,n)} = b,$$

was die Kongruenz

$$a \cdot \frac{bu}{\mathrm{ggT}(a,n)} \equiv b \pmod{n}$$

und damit die Behauptung zeigt. □

Beispiel 4.10. Die Kongruenz $15x \equiv 6 \pmod{21}$ hat wegen $\mathrm{ggT}(15,21) = 3 \mid 6$ eine Lösung. Der erweiterte Euklidische Algorithmus ergibt

$$\mathrm{ggT}(15,21) = 3 = 3 \cdot 15 + (-2) \cdot 21.$$

Damit folgt *wie im Beweis durch Multiplikation mit 2*

$$6 = 6 \cdot 15 + (-4) \cdot 21 \equiv 15 \cdot 6 \pmod{21}$$

d.h. $x = 6$ ist eine Lösung der Kongruenz.

Korrolar 4.11. Es sei $a \in \mathbb{Z}, n \in \mathbb{N}$. Dann sind äquivalent

(i) Die Kongruenz $ax \equiv 1 \pmod{n}$ besitzt eine Lösung in $\mathbb{Z}$.

(ii) $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$

(iii) $\mathrm{ggT}(a,n) = 1$

Beweis. (i) $\iff$ (ii): Die Kongruenz $ax \equiv 1 \pmod{n}$ entspricht der Gleichung $\overline{a} \cdot \overline{x} = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$, welche genau dann lösbar ist, wenn $\overline{x}$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist.

(i) $\iff$ (iii): $\mathrm{ggT}(a,n) = 1 \iff \mathrm{ggT}(a,n) \mid 1$. *Anmerkung: Hinrichtung klar, Rückrichtung: $ggT(a,n) \mid 1$ heißt, 1 ist ein Vielfaches des $ggT(a,n)$, d.h. der $ggT(a,n)$ ist bereits 1.* Folgt mit $b = 1$ aus 4.9.

Hier wird klar, warum die Einheiten in $\mathbb{Z}/n\mathbb{Z}$ prime Restklassen heißen: teilerfremd wird auch als relativ prim bezeichnet. □

Frage: Wie können große Potenzen modulo n vereinfacht werden? Dazu wird Satz v. Euler-Fermat helfen, dafür brauchen wir aber noch ein paar Definitionen

Definition 4.12 (Ordnung)**.** Es sei G eine endliche Gruppe. Die Ordnung von G (Notation: $|G|$) ist definiert als die Anzahl der Elemente von G.

Definition 4.13 (Eulersche φ-Funktion)**.** Die Abbildung

$$\begin{aligned} \varphi\colon \mathbb{N} &\to \mathbb{N} \\ n &\mapsto |(\mathbb{Z}/n\mathbb{Z})^\times| = \#\{a \in \mathbb{N}_0 \mid 0 \le a < n \text{ und } \mathrm{ggT}(a,n) = 1\}. \end{aligned}$$

Anmerkung: also zählt die φ-Funktion die zu einer Zahl n teilerfremden Zahlen zwischen 0 und n.

Beispiel 4.14. (a) Es ist wie $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$, also $\varphi(4) = 2$.

(b) Sei p eine Primzahl. Dann ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper, d.h.

$$\varphi(p) = |(\mathbb{Z}/p\mathbb{Z})^\times| = \#\{\mathbb{Z}/p\mathbb{Z}\} - 1 = p - 1.$$

Lemma 4.15. Es sei p eine Primzahl und $n \in \mathbb{N}$. Dann gilt

$$\varphi(p^n) = p^{n-1}(p-1).$$

Beweis. $\exists$ genau p^{n-1} Zahlen a mit $0 \le a < p^n$ und $\mathrm{ggT}(a,n) > 1$, denn: Primfaktorzerlegung von $p^n = \underbrace{p \cdot p \cdot \ldots \cdot p}_{n-\text{mal}} \implies$ Zahlen a sind die p^{n-1} Vielfachen von p, also $0 \cdot p, 1 \cdot p, \ldots, (p^{n-1}-1) \cdot p \implies$ $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. □

Notation für Gruppen: Verknüpfung multiplikativ und neutrales Element ist 1.

Lemma 4.16. Es sei G eine endliche abelsche Gruppe und $g \in G$. Dann gilt

$$g^{|G|} = 1.$$

Beweis. Betrachte die Abbildung $\tau_g \colon G \to G, x \mapsto gx$. Diese ist injektiv, denn aus $\tau_g(x) = \tau_g(y)$ für $x, y \in G$ folgt $gx = gy$ und nach Linkskürzung $x = y$. Als injektive Selbstabbildung auf der endlichen Gruppe G, ist τ_g auch surjektiv, also bijektiv. Da G endlich folgt damit

$$\prod_{x \in G} x \overset{\tau \text{ bijektiv, } G \text{ abelsch}}{=} \prod_{x \in G} \tau_g(x) = \prod_{x \in G} gx = g^{|G|} \prod_{x \in G} x.$$

Mit Rechtskürzung folgt damit $g^{|G|} = 1$. □

Satz 4.17 (Satz von Euler-Fermat)**.** Es sei $n \in \mathbb{N}$ und $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Dann gilt

$$\overline{a}^{\varphi(n)} = \overline{1}.$$

Beweis. Nach Definition ist $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Die Behauptung folgt damit direkt aus 4.16 mit $G = (\mathbb{Z}/n\mathbb{Z})^\times$. □

Beispiel 4.18. (1) Es ist $3^{19} \equiv 10 \pmod{17}$, denn $\overline{3} \in (\mathbb{Z}/17\mathbb{Z})^\times$ und

$$3^{16} = 3^{\varphi(17)} \overset{\text{Satz v. Euler-Fermat}}{\equiv} 1 \pmod{17}.$$

Damit folgt

$$3^{19} = 3^3 \cdot 3^{16} \equiv 27 \cdot 1 \equiv 10 \pmod{17}.$$

(2) Was ist die letzte Dezimalstelle von 7^{222}? Also welche Zahl ist 7^{222} kongruent modulo 10?
Zunächst $\varphi(10) = 4$. Und $\mathrm{ggT}(7, 10) = 1$. Dann folgt

$$7^4 = 7^{\varphi(10)} \overset{\text{Satz v. Euler-Fermat}}{\equiv} 1 \pmod{10}.$$

Dann teile 222 durch 4 mit Rest. Damit

$$7^{222} = 7^{4 \cdot 55 + 2} = (7^4)^{55} \cdot 7^2 \equiv 1^{55} \cdot 7^2 \equiv 49 \equiv 9 \pmod{10}.$$

Korrolar 4.19 (Kleiner Satz von Fermat)**.** Es sei p eine Primzahl. Dann gilt

(a) Für jedes $\overline{a} \in \mathbb{F}_p^\times$ ist $\overline{a}^{p-1} = \overline{1}$.

(b) Für jedes $\overline{a} \in \mathbb{F}_p$ ist $\overline{a}^p = \overline{a}$.

Beweis. (a) Mit $\varphi(p) = p - 1$ folgt das direkt aus dem Satz von Euler-Fermat.

(b) Falls $\overline{a} \in \mathbb{F}_p^\times$: Dann ist $\overline{a}^p = \overline{a} \cdot \overline{a}^{p-1} = \overline{a} \cdot \overline{1} = \overline{a}$. Falls $\overline{a} = \overline{0}$ ist $\overline{a}^p = \overline{0}^p = \overline{0} = \overline{a}$.

□