Kapitel 5: Die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ und Primitivwurzeln modulo n

In diesem Kapitel bestimmen wir die multiplikative Struktur der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ von $\mathbb{Z}/n\mathbb{Z}$ für eine beliebige positive Zahl $n \in \mathbb{Z}_{>0}$.

16 Die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$

Wir wollen zunächst den Primzahlfall behandeln. Dazu benötigen wir:

Bemerkung 5.1

Sei G eine endliche Gruppe der Ordnung $n \in \mathbb{Z}_{>0}$.

(a) Hat G für jeden Teiler $d \mid n$ höchstens $\varphi(d)$ Elemente der Ordnung d, so ist G zyklisch.

(b) Ist umgekehrt G zyklisch, so existieren für alle $d \mid n$ genau $\varphi(d)$ Elemente der Ordnung d in G.

Beweis: Setze $\psi(d) :=$ Anzahl der Elemente der Ordnung d in G.

(a) Nach Definition ist eine Gruppe $(G, \cdot)$ genau dann zyklisch, wenn ein $g \in G$ existiert mit

$$G = \{g^k \mid k \in \mathbb{Z}_{>0}\}\,.$$

Nach Voraussetzung gilt $\psi(d) \leq \varphi(d)$ für alle $d \mid n$. Nach Lagrange ist die Ordnung jedes $g \in G$ ein Teiler von n. Daher gilt

$$n = |G| = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n$$

nach Satz 2.17(f), also ist $\sum_{d|n} \psi(d) = \sum_{d|n} \varphi(d)$. Da $\psi(d) \leq \varphi(d)$ für jedes d gilt, folgt sogar $\psi(d) = \varphi(d)$ für alle d. Also ist $\psi(n) = \varphi(n) > 0$ und somit enthält G ein Element g der Ordnung n. Daher folgt, dass $G = \{g, \ldots, g^n\}$ zyklisch ist.

(b) Sei $G = \{g^k \mid k \in \mathbb{Z}_{>0}\}$ für ein $g \in G$. Dann ist die Ordnung von g^k gleich n genau dann, wenn $\operatorname{ggt}(k, n) = 1$. Nach Definition der φ-Funktion gilt $\psi(n) = \varphi(n)$. Für jedes $d \mid n$ ist $g^{kd} = (g^d)^k$ ein Element der Ordnung $\frac{n}{d}$. Also erzeugt g^{kd} eine zyklische Gruppe der Ordnung $\frac{n}{d}$. Somit ist

$$\psi(\frac{n}{d}) \geq \varphi(\frac{n}{d})$$

für alle $d \mid n$ und

$$n = |G| = \sum_{d|n} \psi(d) \geq \sum_{d|n} \varphi(d) = n\,.$$

Daraus folgt, dass $\psi(d) = \varphi(d)$ für alle $d \mid n$ gilt. ∎

Bemerkung 5.2

Eine endliche Untergruppe $(G, \cdot)$ der multiplikativen Gruppe $(K^\times, \cdot)$ eines Körpers $(K, +, \cdot)$ ist zyklisch.

Beweis: Setze $|G| := n \in \mathbb{Z}_{>0}$. Ist $g \in G$ ein Element der Ordnung d, so gilt $g^d = 1$, und somit ist g eine Nullstelle des Polynoms $X^d - 1$. Da K ein Körper ist, hat $X^d - 1$ höchstens d Nullstellen. Also gibt es höchstens d Elemente der Ordnung d in G, nämlich $\{g, \dots, g^d\}$.
Dabei gilt: g^k hat Ordnung d genau dann, wenn $\mathrm{ggt}(d, k) = 1$. Also gibt es genau $\varphi(d)$ Elemente der Ordnung d. Aus Bemerkung 5.1 folgt nun, dass G zyklisch ist. ■

Satz 5.3

Sei $p \in \mathbb{P}$ eine Primzahl. Dann ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch.

Beweis: Der Ring $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper (AGS). Aus Bemerkung 5.2 folgt, dass $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch ist. ■

Anmerkung 5.4

Für einen Teilkörper $K \leq \mathbb{C}$ gilt: ist $g \in K^\times$ von endlicher Ordnung $n \in \mathbb{Z}_{>0}$, also $g^n = 1$, so gilt $g = e^{\frac{2\pi i k}{n}}$ für ein $k \in \mathbb{Z}$ (g ist eine **Einheitswurzel**). Nach Bemerkung 5.2 ist dann

$$\langle g \rangle = \{e^{\frac{2\pi i j}{n}} \mid 1 \leq j \leq n\}$$

die einzige endliche Untergruppe von $\mathbb{C}^\times$ der Ordnung n.

Definition 5.5 (*Primitivwurzel modulo n*)

Eine positive ganze Zahl $a \in \mathbb{Z}_{>0}$ heißt **Primitivwurzel modulo** $n \in \mathbb{Z}_{>0}$, wenn

$$(\mathbb{Z}/n\mathbb{Z})^\times = \langle [a] \rangle = \{[a], \dots, [a]^{\varphi(n)}\},$$

d.h. die Ordnung von $[a]$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ ist $\varphi(n)$.

Satz 5.3 besagt demnach: Es existieren Primitivwurzeln modulo p, falls p eine Primzahl ist. Aber wie findet man solche Zahlen?

Beispiel 13

Durch Probieren:
Sei $p = 7$. Dann kann 1 keine (nie) Primitivwurzel sein.
Für $[2]$ gilt: $[2]^2 = [4]$, $[2]^3 = [1]$, also ist 2 keine Primitivwurzel modulo 7, da $\varphi(7) = 6$.
Aber $[3]$ ist eine Primitivwurzel, denn

$$\{[3]^1, \dots, [3]^6\} = \{[3]^6, [3]^2, [3]^1, [3]^4, [3]^5, [3]^3\} = \{[1], [2], [3], [4], [5], [6]\} = (\mathbb{Z}/7\mathbb{Z})^\times.$$

17 Die Gruppe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$

Als nächsten Schritt untersuchen wir die Restklassengruppe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ für 2-Potenzen 2^α. In diesem Abschnitt ist stets $\alpha \in \mathbb{Z}_{\geq 1}$. Für kleine α beobachten wir folgendes:

Beispiel 14

$(\mathbb{Z}/2\mathbb{Z})^\times = \{[1]\}$ und $(\mathbb{Z}/4\mathbb{Z})^\times = \{[1],[3]\}$ sind zyklisch, aber $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1],[3],[5],[7]\}$ mit $[3]^2 = [1]$, $[5]^2 = [1]$, $[7]^2 = [1]$. Also haben $[3],[5],[7]$ (höchstens) Ordnung 2, und $(\mathbb{Z}/8\mathbb{Z})^\times$ ist **nicht** zyklisch.

Bemerkung 5.6

Seien $a \in \mathbb{Z}_{>0}$ ungerade und $\alpha \geq 3$. Dann ist

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

Beweis: Per Induktion nach α.
Für $\alpha = 3$ behaupten wir, dass $a^2 \equiv 1 \pmod 8$ für alle ungeraden a ist. Dies gilt nach obigem Beispiel.
Sei die Behauptung nun für $\alpha - 1$ bewiesen. Dann ist demnach

$$a^{2^{\alpha-3}} \equiv 1 \pmod{2^{\alpha-1}},$$

d.h., es existiert ein $t \in \mathbb{Z}_{>0}$ mit

$$a^{2^{\alpha-3}} = 1 + 2^{\alpha-1}t.$$

Quadrieren liefert

$$a^{2^{\alpha-2}} = (1 + 2^{\alpha-1}t)^2 = 1 + 2^\alpha t + 2^{2\alpha-2}t^2 \equiv 1 \pmod{2^\alpha}.$$

■

Anmerkung 5.7

Da gerade $a \in \mathbb{Z}$ nicht invertierbar in $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ sind, besagt Bemerkung 5.6, dass alle $a \in (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ für $\alpha \geq 3$ höchstens Ordnung $2^{\alpha-2}$ haben. Aber

$$\left|(\mathbb{Z}/2^\alpha\mathbb{Z})^\times\right| = \varphi(2^\alpha) = 2^{\alpha-1},$$

also ist $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ nicht zyklisch für $\alpha \geq 3$. Es gibt also **keine** Primitivwurzel modulo 2^α für $\alpha \geq 3$.

Bemerkung 5.8

Für $\alpha \geq 3$ hat 5 die Ordnung $2^{\alpha-2}$ in $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.

Beweis: Übung. (Blatt 6) ■

Satz 5.9

Für $\alpha \geq 3$ ist

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \langle -[1]\rangle \times \langle [5]\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}\,.$$

Beweis: Wegen $5^\alpha \equiv 1 \pmod 4$ für $\alpha \in \mathbb{Z}_{>0}$ ist $-[1] \notin \langle[5]\rangle$. Nach Bemerkung 5.8 hat $[5]$ die Ordnung $2^{\alpha-2}$. Also erzeugen $-[1],[5]$ zusammen $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. Aus $\langle -[1]\rangle = \{[1],-[1]\}$ folgt $\langle -[1]\rangle \cap \langle[5]\rangle = \{[1]\}$, und somit ist $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \langle -[1]\rangle \times \langle[5]\rangle$ das direkte Produkt von $\langle -[1]\rangle$ und $\langle[5]\rangle$. ■

18 Die Gruppe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$

Unser Ziel ist nun zu zeigen, dass $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ für ungerade Primzahlen p zyklisch ist. In diesem Abschnitt ist stets $\alpha \in \mathbb{Z}_{\geq 1}$.

Lemma 5.10

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl und sei $g \in \mathbb{Z}_{>0}$ eine Primitivwurzel modulo p^α. Dann entweder

(i) g ist Primitivwurzel modulo $p^{\alpha+1}$, oder

(ii) $g^{\varphi(p^\alpha)} \equiv 1 \pmod{p^{\alpha+1}}$.

Beweis: Sei m die Ordnung von g modulo $p^{\alpha+1}$. Es gilt

$$m \mid \left|(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\times\right| \text{ also } m \mid \varphi(p^{\alpha+1}).$$

Andererseits ist $g^m \equiv 1 \pmod{p^{\alpha+1}}$, also ist $g^m \equiv 1 \pmod{p^\alpha}$ und somit $\varphi(p^\alpha) \mid m$, also

$$(p-1)p^{\alpha-1} = \varphi(p^\alpha) \mid m \mid \varphi(p^{\alpha+1}) = (p-1)p^\alpha.$$

Demnach gibt es nur zwei Möglichkeiten:

(i) $m = \varphi(p^{\alpha+1})$, dann ist g Primitivwurzel in $(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\times$, also modulo $p^{\alpha+1}$.

(ii) $m = \varphi(p^\alpha)$, dann ist $g^{\varphi(p^\alpha)} \equiv 1 \pmod{p^{\alpha+1}}$.

■

Satz 5.11

Sei $g \in \mathbb{Z}_{>0}$ eine Primitivwurzel modulo p mit $g^{p-1} = 1 + m\,p$ für ein $m \in \mathbb{Z}$ mit $p \nmid m$. Dann ist g eine Primitivwurzel modulo p^α für alle $\alpha \geq 1$.

Beweis: Wir zeigen, dass $g^{\varphi(p^\alpha)} = 1 + m_\alpha p^\alpha$ für $p \nmid m_\alpha$ für alle $\alpha \in \mathbb{Z}_{>0}$ ist. Dann gilt $g^{\varphi(p^\alpha)} \not\equiv 1 \pmod{p^{\alpha+1}}$ und die Aussage folgt aus Lemma 5.10.

Per Induktion nach α. Für $\alpha = 1$ ist $g^{\varphi(p)} = g^{p-1} = 1 + m_1 p$ nach Voraussetzung. Sei die Behauptung jetzt für α gezeigt. Potenzieren mit p liefert nach Induktionsvoraussetzung

$$\begin{aligned} g^{\varphi(p^{\alpha+1})} = g^{p\varphi(p^\alpha)} = (1 + m_\alpha\, p^\alpha)^p &= 1 + \binom{p}{1} m_\alpha p^\alpha + \binom{p}{2} m_\alpha^2 p^{2\alpha} + \dots \\ &\equiv 1 + m_\alpha p^{\alpha+1} \pmod{p^{\alpha+2}}. \end{aligned}$$

Daher gilt

$$g^{\varphi(p^{\alpha+1})} = 1 + m_\alpha p^{\alpha+1} + k p^{\alpha+2} = 1 + \underbrace{(m_\alpha + kp)}_{m_{\alpha+1}} p^{\alpha+1}.$$

■

Anmerkung 5.12

Um Primitivwurzeln g modulo p^α zu finden, reicht es also eine Primitivwurzel modulo p zu bestimmen, welche die Voraussetzung aus Satz 5.11 erfüllt.

Beispiel 15

$\underline{p = 3:}$ $g = 2$ ist eine Primitivwurzel modulo 3 und $2^{3-1} = 2^2 = 4 = 1 + 1 \cdot 3$. Somit folgt aus Satz 5.11, dass 2 eine Primitivwurzel modulo aller 3^α ist.

$\underline{p = 5:}$ $g = 2$ ist eine Primitivwurzel modulo 5 und $2^{5-1} = 16 = 1 + 3 \cdot 5$. Nach Satz 5.11 ist 2 eine Primitivwurzel modulo aller 5^α.

$p = 5$: $g = 7$ ist eine Primitivwurzel modulo 5, aber $7^4 = 49^2 \equiv (-1)^2 \equiv 1 \pmod{25}$. Daher tritt Fall (b) von Lemma 5.10 ein und die Voraussetzung von Satz 5.11 ist nicht erfüllt. Tatsächlich hat 7 nur Ordnung $4 < \varphi(25) = 20$ modulo 25 und ist damit keine Primitivwurzel modulo 25.

Lemma 5.13

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Dann existiert eine Primitivwurzel g modulo p mit

$$g^{p-1} = 1 + mp \text{ für ein } m \in \mathbb{Z} \text{ mit } p \nmid m.$$

Beweis: Sei g eine Primitivwurzel modulo p (Satz 5.3). Gilt $g^{p-1} = 1 + mp$ mit $p \nmid m$, so sind wir fertig. Sonst gilt $g^{p-1} = 1 + mp$ mit $p \mid m$. Mit g ist auch $g' := g + p \equiv g \pmod{p}$ eine Primitivwurzel modulo p. Aber alle Terme in der binomischen Entwicklung von $(g')^{p-1} = (g+p)^{p-1}$ ab dem dritten Grad sind durch p^2 teilbar, es gibt also ein $t \in \mathbb{Z}$ mit

$$\begin{aligned}(g')^{p-1} = (g+p)^{p-1} &= g^{p-1} + \binom{p-1}{1} g^{p-2}p + tp^2 \\ &= 1 + mp + (p-1)pg^{p-2} + tp^2 = 1 + m'p,\end{aligned}$$

wobei

$$m' = m + (p-1)g^{p-2} + tp.$$

Aber g ist Primitivwurzel modulo p, also $p \nmid g$ und somit $p \nmid g^{p-2}$ und daher $p \nmid m'$, d.h. g' hat die geforderte Eigenschaft. ∎

Satz 5.14

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Dann sind $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ und $(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$ zyklisch für alle $\alpha \geq 1$.

Beweis: Wegen Lemma 5.13 existiert eine Primitivwurzel g modulo p^α. Somit ist $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ nach Definition 5.5 zyklisch. Ist g gerade, so ist auch $g + p^\alpha$ eine Primitivwurzel modulo p^α und ungerade, hat demnach Ordnung $\varphi(p^\alpha)$ modulo p^α. Aber

$$\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha).$$

Also erzeugt g auch $(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$. ∎

19 Die Struktur von $(\mathbb{Z}/n\mathbb{Z})^\times$

Im Kapitel 2, §6 haben wir schon gesehen, dass für $m, n \in \mathbb{Z}_{>0}$ mit $\operatorname{ggt}(m,n) = 1$ der Chinesische Restsatz einen Ring-Isomorphismus

$$\begin{array}{rccc}\Phi: & \mathbb{Z}/(mn)\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & [a]_{mn} & \mapsto & ([a]_m, [a]_n)\end{array}$$

liefert, so dass die Einschränkung von Φ auf die Einheiten $(\mathbb{Z}/(mn)\mathbb{Z})^\times$ die Existenz eines Gruppen-Isomorphimus

$$\begin{array}{rccc}\Phi: & (\mathbb{Z}/(mn)\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \\ & [a]_{mn} & \mapsto & ([a]_m, [a]_n)\end{array}$$

liefert.

Satz 5.15

Sei $n = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von $n \in \mathbb{Z}_{>0}$, mit ungeraden Primzahlen p_i. Dann gilt

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times.$$

Beweis: Per induktion über r, wobei der Induktionsschritt durch das obige Argument gegeben wird. ■

Bevor wir die Frage beantworten können, wann $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch ist, benötigen wir folgendes einfaches gruppentheoretisches Lemma:

Lemma 5.16

Seien G, H zyklische Gruppen. Dann gilt:

$$G \times H \text{ ist zyklisch genau dann, wenn } \operatorname{ggt}(|G|, |H|) = 1.$$

Beweis: Aufgabe, Blatt 7. ■

Folgerung 5.17

Sei $n \in \mathbb{Z}_{\geq 2}$. Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist genau dann zyklisch, wenn

$$n \in \{2, 4, p^\alpha, 2p^\alpha\},$$

wobei $p \in \mathbb{P} \setminus \{2\}$ und $\alpha \in \mathbb{Z}_{\geq 1}$.

Beweis: Verwende Lemma 5.16 induktiv zusammen mit Satz 5.3, Satz 5.9 und Satz 5.14. ■