

### 1.3 Die CARMICHAEL-Funktion

Auch hier wird stets  $n \geq 2$  vorausgesetzt.

Die CARMICHAEL-Funktion ist definiert als Exponent der multiplikativen Gruppe  $\mathbb{M}_n = (\mathbb{Z}/n\mathbb{Z})^\times$ :

$$\lambda(n) := \text{Exp}(\mathbb{M}_n) = \min\{s \geq 1 \mid a^s \equiv 1 \pmod{n} \text{ für alle } a \in \mathbb{M}_n\};$$

d. h.,  $\lambda(n)$  ist das Maximum der Ordnungen der Elemente von  $\mathbb{M}_n$ .

#### Bemerkungen

1. Den Satz von EULER kann man ausdrücken durch  $\lambda(n) \mid \varphi(n)$  („Exponent teilt Gruppenordnung“). Üblich ist die Formulierung

$$a^{\varphi(n)} \equiv 1 \pmod{n} \text{ für alle } a \in \mathbb{Z} \text{ mit } \text{ggT}(a, n) = 1.$$

Beide Formen folgen unmittelbar aus der Definition.

2. Ist  $p$  prim, so  $\mathbb{M}_p$  zyklisch – siehe unten –, also

$$\lambda(p) = \varphi(p) = p - 1.$$

**Hilfssatz 1** Sei  $G$  eine Gruppe vom Exponenten  $r$ ,  $H$  eine Gruppe vom Exponenten  $s$ . Dann hat  $G \times H$  den Exponenten  $t = \text{kgV}(r, s)$ .

*Beweis.* Da  $(g, h)^t = (g^t, h^t) = (1, 1)$  für  $g \in G$ ,  $h \in H$ , ist der Exponent  $\leq t$ . Hat  $g \in G$  die Ordnung  $r$ ,  $h \in H$  die Ordnung  $s$  und  $(g, h)$  die Ordnung  $q$ , so ist  $(g^q, h^q) = (g, h)^q = (1, 1)$ , also  $g^q = 1$ ,  $h^q = 1$ ,  $r \mid q$ ,  $s \mid q$ ,  $t \mid q$ .  $\diamond$

Aus dem chinesischen Restsatz folgt unmittelbar (da  $\mathbb{M}_{mn} \cong \mathbb{M}_m \times \mathbb{M}_n$ )

**Korollar 1** Sind  $m, n \in \mathbb{N}_2$  teilerfremd, so ist

$$\lambda(mn) = \text{kgV}(\lambda(m), \lambda(n)).$$

**Korollar 2** Ist  $n = p_1^{e_1} \cdots p_r^{e_r}$  die Primzerlegung von  $n \in \mathbb{N}_2$ , so ist

$$\lambda(n) = \text{kgV}(\lambda(p_1^{e_1}), \dots, \lambda(p_r^{e_r})).$$

#### Bemerkungen

3. Die CARMICHAEL-Funktion der Zweierpotenzen (Beweis als **Übungsaufgabe** – oder im Anhang A.1):

$$\lambda(2) = 1, \quad \lambda(4) = 2, \quad \lambda(2^e) = 2^{e-2} \text{ für } e \geq 3.$$

4. Die CARMICHAEL-Funktion für Potenzen ungerader Primzahlen (Beweis als **Übungsaufgabe** – oder im Anhang A.3):

$$\lambda(p^e) = \varphi(p^e) = p^{e-1} \cdot (p - 1) \quad \text{für } p \text{ prim } \geq 3.$$

Zum Beweis der Aussage in Bemerkung 2 ist noch zu zeigen, dass die multiplikative Gruppe mod  $p$  tatsächlich zyklisch ist. Das folgt direkt aus einem Standard-Ergebnis der Algebra:

**Satz 2** Sei  $K$  ein Körper und  $G \leq K^\times$  eine endliche Untergruppe mit  $\#G = n$ . Dann ist  $G$  zyklisch und besteht genau aus den  $n$ -ten Einheitswurzeln in  $K$ .

*Beweis.* Für  $a \in G$  ist  $a^n = 1$ , also ist  $G$  enthalten in der Menge der Nullstellen des Polynoms  $T^n - 1 \in K[T]$ . Also hat  $K$  genau  $n$  Stück  $n$ -te Einheitswurzeln, und  $G$  besteht gerade aus diesen. Sei nun  $m$  der Exponent von  $G$ , insbesondere  $m \leq n$ . Der folgende Hilfssatz 2 ergibt: Alle  $a \in G$  sind schon  $m$ -te Einheitswurzeln. Also ist auch  $n \leq m$ , also  $n = m$ , und es gibt ein Element in  $G$  mit der Ordnung  $n$ .  $\diamond$

**Hilfssatz 2** Sei  $G$  eine abelsche Gruppe.

- (i) Seien  $a, b \in G$ ,  $\text{Ord } a = m$ ,  $\text{Ord } b = n$ ,  $m, n$  endlich und teilerfremd. Dann ist  $\text{Ord } ab = mn$ .
- (ii) Seien  $a, b \in G$ ,  $\text{Ord } a$ ,  $\text{Ord } b$  endlich,  $q = \text{kgV}(\text{Ord } a, \text{Ord } b)$ . Dann gibt es ein  $c \in G$  mit  $\text{Ord } c = q$ .
- (iii) Sei  $m = \max\{\text{Ord } a \mid a \in G\} = \text{Exp}(G)$  endlich. Dann gilt  $\text{Ord } b \mid m$  für alle  $b \in G$ .

*Beweis.* (i) Sei  $k := \text{Ord}(ab)$ . Da  $(ab)^{mn} = (a^m)^n \cdot (b^n)^m = 1$ , ist  $k \mid mn$ . Da  $a^{kn} = a^{kn} \cdot (b^n)^k = (ab)^{kn} = 1$ , gilt  $m \mid kn$ , also  $m \mid k$ , ebenso  $n \mid k$ , also  $mn \mid k$ .

(ii) Sei  $p^e$  eine Primzahlpotenz mit  $p^e \mid q$ , etwa  $p^e \mid m := \text{Ord } a$ . Dann hat  $a^{m/p^e}$  die Ordnung  $p^e$ . Ist nun  $q = p_1^{e_1} \cdots p_r^{e_r}$  die Primzahl-Zerlegung mit verschiedenen Primzahlen  $p_i$ , so gibt es je ein  $c_i \in G$  mit  $\text{Ord } c_i = p_i^{e_i}$ . Nach (i) hat  $c = c_1 \cdots c_r$  die Ordnung  $q$ .

(iii) Sei  $\text{Ord } b = n$ . Dann gibt es ein  $c \in G$  mit  $\text{Ord } c = \text{kgV}(m, n)$ . Also ist  $\text{kgV}(m, n) \leq m$ , also  $= m$ , also  $n \mid m$ .  $\diamond$