1.8 Die CARMICHAEL-Funktion

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

Die CARMICHAEL-Funktion ist definiert als Exponent der multiplikativen Gruppe:

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

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 $\lambda(n)|\varphi(n)$. Üblich ist die Formulierung

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

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

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 $g^q = 1$, $h^q = 1$, $r|q$, $s|q$, $t|q$. $\diamond$

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

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

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

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

Bemerkungen

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

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

4. Die CARMICHAEL-Funktion ungerader Primpotenzen (Beweis als Übungsaufgabe – oder im Anhang A.3):

$$\lambda(p^e) = \varphi(p^e) = p^{e-1} \cdot (p-1) \quad \text{für } p \text{ prim} \geq 2.$$

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

Satz 8 *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 5 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 5 *Sei G eine abelsche Gruppe.*

(i) *Seien $a, b \in G$, $\operatorname{Ord} a = m$, $\operatorname{Ord} b = n$, m, n endlich und teilerfremd. Dann ist $\operatorname{Ord} ab = mn$.*

(ii) *Seien $a, b \in G$, $\operatorname{Ord} a$, $\operatorname{Ord} b$ endlich, $q = \operatorname{kgV}(\operatorname{Ord} a, \operatorname{Ord} b)$. Dann gibt es ein $c \in G$ mit $\operatorname{Ord} c = q$.*

(iii) *Sei $m = \max\{\operatorname{Ord} a \mid a \in G\} = \operatorname{Exp}(G)$ endlich. Dann gilt $\operatorname{Ord} b \mid m$ für alle $b \in G$.*

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

(ii) Sei p^e eine Primzahlpotenz mit $p^e | q$, etwa $p^e | m := \operatorname{Ord} a$. 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 $\operatorname{Ord} c_i = p_i^{e_i}$. Nach (i) hat $c = c_1 \cdots c_r$ die Ordnung q.

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