## 1.5 Die maximale Periode multiplikativer Generatoren

Multiplikative Generatoren $x_n = ax_{n-1} \bmod m$ können nie die Periode $m$ erreichen, da das Folgenglied 0 nie mehr verlassen wird. Was können sie bestenfalls? Dazu brauchen wir zwei zahlentheoretische Funktionen. Die erste ist die EULERsche $\varphi$-Funktion, also die Ordnung der multiplikativen Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$. Ihr Exponent, also die maximale Ordnung eines Elements in der Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$, ist die CARMICHAEL-Funktion $\lambda(m)$. Eine ganze Zahl $a$ heißt **primitives Element** $\bmod m$, wenn $a \bmod m$ in $\mathbf{Z}/m\mathbb{Z}$ invertierbar ist und seine Ordnung gleich $\lambda(m)$ ist.

**Hauptsatz 2 (CARMICHAEL 1910)** *Die maximale Periode eines multiplikativen Generators mit erzeugender Funktion $s(x) = ax \bmod m$ ist $\lambda(m)$. Sie wird insbesondere dann erreicht, wenn gilt:*

(i) *$a$ ist primitiv $\bmod m$.*

(ii) *$x_0$ ist teilerfremd zu $m$.*

Zusatz 1. *Notwendig für das Erreichen der Periode $\lambda(m)$ ist* (i) *zusammen mit*

(ii') *Ist $d$ der größte gemeinsame Teiler von $m$ und $x_0$, so ist $\lambda(m) = \lambda(\frac{m}{d})$.*

Zusatz 2. *Wird die maximale Periode $\lambda(m)$ erreicht, so ist sie gleich der effektiven Periode.*

*Beweis.* Es ist $x_n = a^n x_0 \bmod m$. Ist $k$ die Ordnung von $a$, so $x_k = x_0$, also die Periode $\leq k \leq \lambda(m)$. Sei nun $a$ primitiv $\bmod m$, also $1, a, \ldots, a^{\lambda(m)-1} \bmod m$ verschieden. Da $x_0$ zu $m$ teilerfremd ist, folgt, dass die Periode $\lambda(m)$ ist.

Sei umgekehrt die Periode $= \lambda(m)$. Dann sind die Zahlen $x_0, ax_0, \ldots, a^{\lambda(m)-1}x_0 \bmod m$ verschieden, also hat $a$ mindestens die Ordnung $\lambda(m)$, ist also primitiv. Sei $\bar{m} = \frac{m}{d}$ und $\bar{x}_0 = \frac{x_0}{d}$; dann ist $\bar{x}_0$ zu $\bar{m}$ teilerfremd und $\lambda(m)$ ist der kleinste Index $k$ mit $a^k \bar{x}_0 \equiv \bar{x}_0 \pmod{\bar{m}}$. Also ist $\lambda(m) =$ Ordnung von $a \bmod \bar{m} \leq \lambda(\bar{m})$. Die umgekehrte Ungleichung $\lambda(\bar{m}) \leq \lambda(m)$ ist trivial. $\diamond$

**Korollar 1** *Ist $m = p$ eine Primzahl, so wird die maximale Periode $\lambda(p) = p - 1$ genau dann erreicht, wenn gilt:*

(i) *$a$ ist primitiv $\bmod p$.*

(ii) *$x_0 \neq 0$.*

Für Primzahlmoduln ist die Situation bei den multiplikativen Generatoren also sehr gut: Die Periode ist nur um 1 kleiner als überhaupt mit einstufiger Rekursion möglich, die effektive Periode ist genau so groß, und jeder Startwert außer 0 ist geeignet. Zum Beweis des Korollars (und um

die Lücke im obigen Beispiel zu schließen) ist aber noch zu zeigen, dass die multiplikative Gruppe $\bmod p$ tatsächlich zyklisch ist. Das folgt direkt aus einem Standard-Ergebnis der Algebra:

**Satz 1** *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 6 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 6** *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 $m = \max\{\operatorname{Ord} a \mid a \in G\}$ 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 $n | m$. $\diamond$