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? – λ ist im folgenden Satz die CARMICHAEL-Funktion und wurde genau in diesem Zusammenhang erstmals eingeführt.

Satz 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.*

Beweis. Es ist $x_n = a^n x_0 \bmod m$. Ist $k = \mathrm{Ord}_m a$ 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. $\diamond$

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 und jeder Startwert außer 0 ist geeignet.

Dieses Ergebnis wird in Abschnitt 1.9 weitgehend verallgemeinert.