1.4 Die maximale Periode

Wann hat ein linearer Kongruenzgenerator zum Modul m die maximal mögliche Periode m? Für einen multiplikativen Generator ist das nicht möglich, weil man vom Folgenglied 0 nie mehr wegkommt. Für diese Frage sind also nur gemischte Kongruenzgeneratoren von Interesse. Der triviale Generator mit erzeugender Funktion $s(x) = x + 1 \bmod m$ zeigt, dass dann die Periodenlänge m möglich ist; er zeigt natürlich auch, dass die maximale Periodenlänge noch lange nicht hinreicht, um die Qualität eines Zufallsgenerators nachzuweisen. Das allgemeine Ergebnis ist leicht formuliert:

Satz 1 (Hull/Dobell **1962,** Knuth**)** *Der lineare Kongruenzgenerator mit erzeugender Funktion $s(x) = ax + b \bmod m$ hat genau dann die Periode m, wenn folgende drei Bedingungen erfüllt sind:*

(i) *b und m sind teilerfremd.*

(ii) *Jeder Primteiler p von m teilt auch $a - 1$.*

(iii) *Ist m durch 4 teilbar, so auch $a - 1$.*

Die erste Bedingung bedeutet insbesondere $b \neq 0$, so dass also wirklich ein gemischter Kongruenzgenerator vorliegt. Dem Beweis wird ein Hilfssatz vorangestellt (und es werden zwei weitere Hilfssätze aus Kapitel III, Anhang A.1 verwendet).

Hilfssatz 1 *Sei $m = m_1 m_2$ mit teilerfremden natürlichen Zahlen m_1 und m_2. Seien λ, λ_1 und λ_2 die Perioden der Kongruenzgeneratoren $x_n = s(x_{n-1}) \bmod m$ bzw. $\bmod m_1$ bzw. $\bmod m_2$ zum Startwert x_0. Dann ist λ das kleinste gemeinsame Vielfache von λ_1 und λ_2.*

Beweis. Seien $x_n^{(1)}$ und $x_n^{(2)}$ die entsprechenden Folgeglieder für m_1 bzw. m_2. Dann ist $x_n^{(i)} = x_n \bmod m_i$. Da $x_{n+\lambda} = x_n$ für alle genügend großen n, folgt sofort, dass λ ein Vielfaches von λ_1 und λ_2 ist. Umgekehrt folgt aus $m \mid t \iff m_1, m_2 \mid t$, dass

$$x_n = x_k \iff x_n^{(i)} = x_k^{(i)} \quad \text{für } k = 1 \text{ und } 2.$$

Also ist λ höchstens gleich dem kleinsten gemeinsamen Vielfachen von λ_1 und λ_2. $\diamond$

Beweis des Satzes. Für beide Beweisrichtungen kann man nach dem Hilfssatz 1 o. B. d. A. $m = p^e$ mit einer Primzahl p annehmen.

„$\Longrightarrow$“: Da jede Zahl in $[0 \ldots m-1]$ genau einmal vorkommt, darf man o. B. d. A. $x_0 = 0$ annehmen. Dann ist

$$x_n = (1 + a + \cdots + a^{n-1}) \cdot b \bmod m \quad \text{für alle } n.$$

Da x_n auch den Wert 1 annimmt, muss schon mal b zu m teilerfremd sein. Da $x_m = 0$, folgt nun $m \mid 1 + a + \cdots + a^{m-1}$, also

$$p \mid m \mid a^m - 1 = (a-1)(1 + a + \cdots + a^{m-1}).$$

Nach dem kleinen Satz von FERMAT ist $a^p \equiv a \pmod{p}$, also $a^m = a^{p^e} \equiv a^{p^{e-1}} \equiv \ldots \equiv a \pmod{p}$, also $p \mid a - 1$. Die Aussage (iii) ist der Fall $p = 2$ mit $e \geq 2$. Wegen der Aussage (ii) muss a schon mal ungerade sein. Wäre nun $a \equiv 3 \pmod{4}$, so nach Hilfssatz 1 in III.A.1 bereits $x_{m/2} = 0$. Also muss $a \equiv 1 \pmod{4}$ sein.

„$\Longleftarrow$“: Auch hier kann man wieder o. B. d. A. $x_0 = 0$ annehmen. Dann ist

$$x_n = 0 \Longleftrightarrow m \mid 1 + a + \cdots + a^{n-1}.$$

Insbesondere ist der Fall $a = 1$ trivial. Sei also o. B. d. A. $a \geq 2$. Dann ist weiter

$$x_n = 0 \Longleftrightarrow m \mid \frac{a^n - 1}{a - 1}.$$

Zu zeigen ist:

- $m \mid \frac{a^m-1}{a-1}$ – dann ist $\lambda | m$;
- m kein Teiler von $\frac{a^{m/p}-1}{a-1}$ – da m eine p-Potenz ist, folgt dann $\lambda \geq m$.

Sei p^h die maximale Potenz, die in $a-1$ aufgeht. Nach Hilfssatz 2 in III.A.1 ist dann

$$a^p \equiv 1 \pmod{p^{h+1}},\ a^p \not\equiv 1 \pmod{p^{h+2}}$$

und sukzessive

$$a^{p^k} \equiv 1 \pmod{p^{h+k}},\ a^{p^k} \not\equiv 1 \pmod{p^{h+k+1}}$$

für alle k. Insbesondere folgt $p^{h+e} \mid a^m - 1$. Da in $a-1$ höchstens p^h aufgeht, folgt $m = p^e \mid \frac{a^m-1}{a-1}$. Wäre $p^e \mid \frac{a^{m/p}-1}{a-1}$, so $p^{e+h} \mid a^{p^{e-1}} - 1$, Widerspruch. $\diamondsuit$

Dieser Satz ist vor allem für Zweierpotenz-Moduln von Interesse; für Primzahl-Moduln dagegen ergibt er kein brauchbares Ergebnis.

Korollar 1 (GREENBERGER 1961) *Ist $m = 2^e$ mit $e \geq 2$, so wird die Periode m genau dann erreicht, wenn gilt:*

(i) *b ist ungerade.*

(ii) *$a \equiv 1 \pmod{4}$.*

Korollar 2 *Ist m eine Primzahl, so wird die Periode m genau dann erreicht, wenn b zu m teilerfremd und $a = 1$ ist.*

Dieses (traurige) Ergebnis lässt sich etwas allgemeiner fassen – auch für beliebige quadratfreie Moduln m gibt es keine brauchbaren linearen Kongruenzgeneratoren der Periode m:

Korollar 3 *Ist m quadratfrei, so wird die Periode m genau dann erreicht, wenn b zu m teilerfremd und $a = 1$ ist.*

Wir haben nun mit Satz 1 die überhaupt größtmögliche Periode erreicht und mit Korollar 1 auch einen brauchbaren Spezialfall gefunden.