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. Im Moment 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:

Hauptsatz 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 werden drei Hilfssätze vorangestellt.

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

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

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

Daher kann man im Beweis des Hauptsatzes m als Primpotenz annehmen.

Hilfssatz 2 *Sei $m = 2^e$ mit $e \geq 2$.*

(i) *Ist a ungerade, so*

$$a^{2^s} \equiv 1 \pmod{2^{s+2}} \text{ für alle } s \geq 1.$$

(ii) *Ist $a \equiv 3 \pmod 4$, so $m \mid 1 + a + \cdots + a^{m/2-1}$.*

Beweis. (i) Ist $a = 4q+1$, so $a^2 = 16q^2+8q+1$; ist $a = 4q+3$, so $a^2 = 16q^2+24q+9 \equiv 1 \pmod 8$. Die Behauptung folgt durch Induktion:

$$a^{2^{s-1}} = 1 + t2^{s+1} \Longrightarrow a^{2^s} = (a^{2^{s-1}})^2 = 1 + 2t2^{s+1} + t^2 2^{2s+2}.$$

(ii) Es ist $2m = 2^{e+1} \mid a^{m/2} - 1$ nach (i). Da in $a-1$ nur die erste Potenz von 2 aufgeht, folgt

$$m = 2^e \mid \frac{a^{m/2}-1}{a-1},$$

wie behauptet. $\diamond$

Hilfssatz 3 *Sei p eine Primzahl und e eine natürliche Zahl mit $p^e \geq 3$. Sei p^e die größte p-Potenz, die in $x-1$ aufgeht. Dann ist p^{e+1} die größte p-Potenz, die in $x^p - 1$ aufgeht.*

Beweis. Es ist $x = 1 + tp^e$ mit einer ganzen Zahl t, die kein Vielfaches von p ist. Nach der Binomialformel ist

$$x^p = 1 + \sum_{k=1}^{p} \binom{p}{k} t^k p^{ke}.$$

Da p alle Binomialkoeffizienten $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ für $k = 1, \ldots, p-1$ teilt, kann man aus der Summe sogar p^{e+1} ausklammern:

$$x^p = 1 + tp^{e+1}s$$

mit einer ganzen Zahl s. Also geht p^{e+1} in $x^p - 1$ auf. Zu zeigen ist noch, dass s kein Vielfaches von p ist. Dazu sieht man sich s genauer an:

$$\begin{aligned} s &= \sum_{k=1}^{p} \frac{1}{p}\binom{p}{k} \cdot t^{k-1} p^{e(k-1)} \\ &= 1 + \frac{1}{p}\binom{p}{2} \cdot tp^e + \cdots + \frac{1}{p} \cdot t^{p-1} p^{e(p-1)}. \end{aligned}$$

Da $p^e \geq 3$, ist $e(p-1) \geq 2$, also $s \equiv 1 \pmod p$. $\diamond$

Beweis des Hauptsatzes. Für beide Beweisrichtungen kann man 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

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

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 2 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 3 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. Ist a teilerfremd zu m, so heißt die Ordnung von $a \bmod m$ in der multiplikativen Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ die **multiplikative Ordnung von** $a \bmod m$. Es wird ein Hilfssatz benötigt:

Hilfssatz 4 *Habe $m \geq 2$ die Primzerlegung $m = p_1^{e_1} \cdots p_r^{e_r}$. Sei $a \in \mathbb{Z}$ mit $p_i | a-1$ für $i = 1, \ldots, r$, und sei s die multiplikative Ordnung von $a \bmod m$. Dann gilt $s | p_1^{e_1-1} \cdots p_r^{e_r-1}$.*

Beweis. Genau dann ist $a^s \equiv 1 \pmod{m}$, wenn $a^s \equiv 1 \pmod{p_i^{e_i}}$ für $i = 1, \ldots, r$. Also ist s das kleinste gemeinsame Vielfache der multiplikativen Ordnungen von $a \bmod p_i^{e_i}$. Es reicht daher, den Hilfssatz im Fall $r = 1$, $m = p^e$ zu beweisen. Das geht mit Induktion über den Exponenten e. Ist $e = 1$, so folgt $s = 1$ aus $a \equiv 1 \pmod{p}$. Ist $e \geq 2$ und $t | p^{e-2}$ die multiplikative Ordnung von $a \bmod p^{e-1}$, so $p^{e-1} | a^t - 1$, also $p^e | a^{tp} - 1$ nach Hilfssatz 3. Es folgt $s | tp | p^{e-1}$. $\diamond$

Eine ganze Zahl m heißt **quadratfrei**, wenn für alle $t \in \mathbb{N}$ mit $t \geq 2$ stets t^2 kein Teiler von m ist. Äquivalent dazu ist, dass in der Primzerlegung von m kein Faktor mehrfach vorkommt. Jede Primzahl selbst ist quadratfrei. 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 Hauptsatz 1 die überhaupt größtmögliche Periode erreicht und mit Korollar 1 auch einen brauchbaren Spezialfall gefunden. Eine genauere Untersuchung, die auf MARSAGLIA zurückgeht, zeigt allerdings, dass die Periode oft in kleinere Teile zerfällt, die sich nur unwesentlich voneinander unterscheiden. Und zwar tritt dieser Effekt gerade auch bei der maximalen Periodenlänge m auf. Das sieht man ganz einfach mit dem ersten Teil des folgenden Hilfssatzes; der zweite Teil wird hier nur zur späteren Verwendung angefügt.

Hilfssatz 5 *Die Folge (x_i) sei von einem linearen Kongruenzgenerator mit Modul m, Multiplikator a, Inkrement b und Startwert 0 erzeugt. Sei a teilerfremd zu m und s die multiplikative Ordnung von $a \bmod m$. Dann gilt:*

(i) $x_{qs+r} \equiv q x_s + x_r \pmod{m}$ *für alle $q, r \in \mathbb{N}$.*

(ii) *Ist die Periode gleich m, so $\mathrm{ggT}(x_s, m) = s$.*

Beweis. (i) Da $x_0 = 0$, ist $x_k \equiv (1 + \cdots + a^{k-1})b$ für alle k, und es folgt

$$x_{qs+r} \equiv (1+\cdots+a^{s-1}+1+\cdots+a^r)b \equiv q(1+\cdots+a^{s-1})b+(1+\cdots+a^r)b \equiv qx_s+x_r.$$

(ii) Nach Hilfssatz 4 ist $s | m$, und

$$\frac{m}{s} | q \iff m | qs \iff x_{qs} = 0 \iff q x_s \equiv 0 \pmod{m}$$

$$\Longleftrightarrow m|qx_s \Longleftrightarrow \frac{m}{\mathrm{ggT}(x_s,m)}|q,$$

und daraus folgt die Behauptung. $\diamond$

Bleiben wir zunächst beim Startwert $x_0 = 0$ und nehmen b als teilerfremd zu m an. Dann ist das Folgenstück $(x_{qs+r})_{0\le r\le s-1}$ identisch mit $(x_r)_{0\le r\le s-1}$ bis auf die Verschiebung mod m um den festen Wert qx_s. Die gesamte Periode der Länge λ besteht also aus λ/s Blöcken der Länge s, die sich nur unwesentlich unterscheiden. (Dabei ist s ein Teiler von λ weil

$$x_k = 0 \Longrightarrow 0 = (a-1)x_k = (a^k-1)b \Longrightarrow a^k = 1.)$$

Bei beliebigem Startwert sieht das Bild nicht besser aus – dann ist nämlich

$$\begin{aligned} x_i &= a^i x_0 + (1+\cdots+a^{i-1})b \bmod m \\ &= x_0 + (a^i-1)x_0 + (1+\cdots+a^{i-1})b \bmod m \\ &= x_0 + (1+\cdots+a^{i-1})c \bmod m \end{aligned}$$

mit $c = (a-1)x_0 + b \bmod m$. Betrachtet man die „reduzierte Folge“

$$y_i = ay_{i-1} + 1 \bmod m \quad \text{mit } y_0 = 0,$$

so ist $x_i = x_0 + cy_i \bmod m$ für alle i. Die Zerlegung in λ/s Blöcke der Länge s trifft also genau so zu. Daher nennt man s die **effektive Periode** des linearen Kongruenzgenerators. Für einen guten Generator sollte also s, die multiplikative Ordnung von a mod m, möglichst groß sein; die absolute Untergrenze für statistische Anwendungen ist 10^9.

Das schlechte Beispiel $s(x) = x + 1$ mit Periode m hat die effektive Periode 1. Damit haben wir also einen neuen Gesichtspunkt, unter dem ein sehr schlechter Generator auch sehr schlecht aussieht.

Falls $a-1$ kein Nullteiler in $\mathbb{Z}/m\mathbb{Z}$ ist, stimmt die effektive Periode mit der Periode überein, denn

$$x_s = a^s x_0 + t_s b \bmod m \text{ mit } t_s = 1+\cdots+a^{s-1} \bmod m,$$

und $(a-1)\cdot t_s = 0$, also $t_s = 0$, also $x_s = x_0$. Insbesondere scheidet für einen Primzahlmodul m nur der triviale Multiplikator $a = 1$ wegen zu kleiner effektiver Periode aus.