2.3 Lineare Kongruenzgeneratoren mit bekanntem Modul

Die Behandlung hier ist elementar ohne Benutzung der allgemeinen Theorie der vorhergehenden Abschnitte.

Die Parameter a und b des linearen Kongruenzgenerators $x_n = ax_{n-1} + b \bmod m$ seien unbekannt, bekannt hingegen sei zunächst der Modul m.

Für die Vorhersage reichen, auch wenn m nicht prim ist, 3 aufeinanderfolgende Folgenglieder x_0, x_1, x_2, wie im folgenden gezeigt wird. Aus der Relation

$$x_2 - x_1 \equiv a(x_1 - x_0) \pmod{m}$$

erhält man sofort (falls $x_1 - x_0$ zu m teilerfremd ist – das wird zunächst angenommen)

$$a = \frac{x_2 - x_1}{x_1 - x_0} \bmod m,$$

wobei die Division $\bmod m$ vorzunehmen ist (mit dem erweiterten Euklidischen Algorithmus). Das Inkrement b ergibt sich aus

$$b = x_1 - ax_0 \bmod m.$$

Damit ist das Bildungsgesetz bekannt und die Folge total vorhersagbar.

Typisch war schon in diesem einfachen Fall die Verwendung der **Differenzenfolge**

$$y_i = x_i - x_{i-1} \quad \text{für } i \geq 1.$$

Sie gehorcht dem Bildungsgesetz

$$y_{i+1} \equiv ay_i \pmod{m}.$$

Zu beachten ist, dass die y_i auch negativ sein können; sie liegen im Bereich $-m < y_i < m$. Falls m bekannt ist, könnte man sie durch $y_i \bmod m$ ersetzen, aber das spielte, wie gesehen, keine Rolle, und bei unbekanntem m – später – geht es sowieso nicht.

Hilfssatz 1 (von der Differenzenfolge) *Die Folge (x_i) sei von dem linearen Kongruenzgenerator mit Modul m, Multiplikator a und Inkrement b erzeugt. Sei (y_i) ihre Differenzenfolge, $c = \mathrm{ggT}(m, a)$ und $d = \mathrm{ggT}(m, y_1)$. Dann gilt:*

(i) *Folgende Aussagen sind äquivalent:*
  (a) *Die Folge (x_i) ist konstant.*
  (b) $y_1 = 0$.
  (c) *Für alle i ist $y_i = 0$.*

(ii) $\mathrm{ggT}(m, y_i) | \mathrm{ggT}(m, y_{i+1})$ *für alle i.*

(iii) $d | y_i$ *für alle i.*

(iv) *Ist* $\mathrm{ggT}(y_1, \ldots, y_t) = 1$ *für ein $t \geq 1$, so $d = 1$.*

(v) $c | y_i$ *für alle $i \geq 2$.*

(vi) *Ist* $\mathrm{ggT}(y_2, \ldots, y_t) = 1$ *für ein* $t \geq 2$*, so* $c = 1$*.*
(vii) $m | y_i y_{i+2} - y_{i+1}^2$ *für alle* i*.*
(viii) *Sind* $\tilde{a}, \tilde{m}$ *ganze Zahlen,* $\tilde{m} \geq 1$*, mit* $y_i \equiv \tilde{a} y_{i-1} \pmod{\tilde{m}}$ *für* $i = 2, \ldots, r$*, so gilt* $x_i = \tilde{a} x_{i-1} + \tilde{b} \bmod \tilde{m}$ *für alle* $i = 1, \ldots, r$ *mit* $\tilde{b} = x_1 - \tilde{a} x_0 \bmod \tilde{m}$*.*

Beweis. (i) Es ist nur zu bemerken, dass mit einem y_i auch alle folgenden 0 sind.

(ii) Ist e Teiler von y_i und m, so wegen $y_{i+1} = a y_i + k_i m$ auch Teiler von y_{i+1}.

(iii) ist ein Spezialfall von (ii).

(iv) gilt, weil $d | \mathrm{ggT}(y_1, \ldots, y_t)$ nach (iii).

(v) Sei $m = c\tilde{m}$ und $a = c\tilde{a}$. Dann ist $y_{i+1} = c\tilde{a} y_i + k_i c\tilde{m}$, also $c | y_{i+1}$ für $i \geq 1$.

(vi) gilt, weil $c | \mathrm{ggT}(y_2, \ldots, y_t)$ nach (v).

(vii) $y_i y_{i+2} - y_{i+1}^2 \equiv a^2 y_i - a^2 y_i \pmod{m}$.

(viii) durch Induktion: Für $i = 1$ ist die Behauptung die Definition von $\tilde{b}$. Für $i \geq 2$ folgt

$$x_i - \tilde{a} x_{i-1} - \tilde{b} \equiv x_i - \tilde{a} x_{i-1} - x_{i-1} + \tilde{a} x_{i-2} \equiv y_i - \tilde{a} y_{i-1} \equiv 0 \pmod{\tilde{m}},$$

wie behauptet. $\diamond$

Der triviale Fall der konstanten Folge braucht nicht weiter untersucht zu werden. Man erkennt an ihm aber, dass die Parameter eines linearen Kongruenzgenerators oft nicht eindeutig durch die erzeugte Folge bestimmt sind. Zum Beispiel kann man die konstante Folge mit einem beliebigen Modul m und einem beliebigen Multiplikator a erzeugen, wenn man nur das Inkrement $b = -(a-1)x_0 \bmod m$ setzt. Auch bei gegebenem m ist a dabei noch nicht eindeutig festgelegt, nicht einmal $a \bmod m$.

Im oben behandelten Fall war y_1 zu m teilerfremd und somit $a = y_2/y_1 \bmod m$. Im allgemeinen kann es allerdings passieren, dass die Division $\bmod m$ gar nicht eindeutig ist; genau dann trifft das zu, wenn m und y_1 nicht teilerfremd sind, also $d = \mathrm{ggT}(m, y_1) > 1$ ist. Die **reduzierte Differenzenfolge** $\bar{y}_i = y_i/d$ (vgl. (iii) in Hilfssatz 1) folgt dann der Rekursionsformel

$$\bar{y}_{i+1} \equiv \bar{a} \bar{y}_i \pmod{\bar{m}}$$

mit dem reduzierten Modul $\bar{m} = m/d$ und reduzierten Multiplikator $\bar{a} = a \bmod \bar{m}$, aus der sich $\bar{a} = \bar{y}_2/\bar{y}_1$ eindeutig bestimmen lässt. Setzt man $\tilde{a} = \bar{a} + k\bar{m}$ mit einer beliebigen ganzen Zahl k und $\tilde{b} = x_1 - \tilde{a} x_0 \bmod m$, so folgt nach Hilfssatz 1 (viii) auch $x_i = \tilde{a} x_{i-1} + \tilde{b} \bmod m$ für alle $i \geq 1$. Damit ist der folgende Satz gezeigt:

Satz 4 *Die Folge (x_i) sei von einem linearen Kongruenzgenerator mit bekanntem Modul m, aber unbekanntem Multiplikator a und Inkrement b erzeugt. Dann ist die gesamte Folge aus x_0, x_1 und x_2 bestimmbar. Falls die Folge (x_i) nicht konstant ist, ist der Multiplikator a genau bis auf ein Vielfaches des reduzierten Moduls $\bar{m}$ bestimmt.*

Man muss sich also auch hier unter Umständen damit begnügen, die Folge vorherzusagen, ohne letzte Gewissheit über die wirklich verwendeten Parameter erlangen zu können. Wer ein ganz einfaches Zahlenbeispiel möchte: Für $m = 24$, $a = 2k + 1$ mit $k \in [0 \dots 11]$ und $b = 12 - 2k \bmod 24$ wird aus dem Startwert $x_0 = 1$ stets die Folge $(1, 13, 1, 13, \dots)$ erzeugt.