1.8 Allgemeine lineare Generatoren

Noch allgemeiner (und begrifflich einfacher) ist die abstrakt-algebraische Version, der **allgemeine lineare Generator**. Gegeben sind:

- ein Ring R (kommutativ und mit Einselement),
- ein R-Modul M,
- eine R-lineare Abbildung $A : M \longrightarrow M$,
- ein Startwert $x_0 \in M$.

Daraus wird eine Folge $(x_n)_{n\in\mathbb{N}}$ gebildet nach der Formel

$$x_n = Ax_{n-1} \quad \text{für } n \geq 1.$$

Beispiele

1. Für einen homogenen linearen Kongruenzgenerator ist

$$R = \mathbb{Z}/m\mathbb{Z}, \quad M = R \quad (r = 1), \quad A = (a).$$

2. Für einen inhomogenen linearen Kongruenzgenerator ist

$$R = \mathbb{Z}/m\mathbb{Z}, \quad M = R^2 \quad (r = 2), \quad A = \begin{pmatrix} 0 & 1 \\ -a & a+1 \end{pmatrix}.$$

3. Für ein lineares Schieberegister ist

$$R = \mathbb{F}_2, \quad M = \mathbb{F}_2^l \quad (r = l), \quad A = \text{die Begleitmatrix},$$

   die nur aus Nullen und Einsen besteht.

Falls M endlich ist, kann die Rekursion nur endlich viele verschiedene Werte annehmen, muss also nach einer eventuellen Vorperiode periodisch werden.

Satz 3 *Sei M ein endlicher R-Modul und $A : M \longrightarrow M$ linear. Genau dann, wenn A bijektiv ist, sind alle vom zugehörigen allgemeinen linearen Generator erzeugten Folgen rein-periodisch.*

Beweis. Sei A bijektiv und x_0 ein Startvektor. Sei t der kleinste Index, so dass x_t einen bereits vorher durchlaufenen Wert annimmt, und sei s der kleinste Index mit $x_t = x_s$. Wäre $s \geq 1$, so $x_s = Ax_{s-1}$ und $x_t = Ax_{t-1}$, also

$$x_{t-1} = A^{-1}x_t = A^{-1}x_s = x_{s-1},$$

im Widerspruch zur Minimalität von t.

Sei umgekehrt A nicht bijektiv; da M endlich ist, ist A dann auch nicht surjektiv. Man kann also $x_0 \in M - A(M)$ wählen. Dann kann niemals $x_0 = Ax_t$ sein, die Folge ist also nicht reinperiodisch. $\diamond$

Dieses Ergebnis lässt sich über die Begleitmatrix auf homogene mehrstufige Kongruenzgeneratoren, insbesondere auf lineare Schieberegister anwenden:

Korollar 1 *Ein homogener linearer Kongruenzgerator der Rekursionstiefe r erzeugt stets rein-periodische Folgen, wenn der Koeffizient a_r in $\mathbb{Z}/m\mathbb{Z}$ invertierbar ist. Ein lineares Schieberegister der Länge l erzeugt rein-periodische Folgen, wenn der Rückkopplungskoeffizient $a_l \neq 0$ ist.*

Die erste Aussage gilt auch im nicht-homogenen Fall, da die Formel

$$x_{n-r} = a_r^{-1}(x_n - a_1 x_{n-1} - \cdots - a_{r-1} x_{n-r+1} - b)$$

für die Rückwärtsberechnung der Folge sorgt.