1.3 Lineare Kongruenzgeneratoren

Die erste wichtige Klasse von elementaren – „klassischen“ – Zufallsgeneratoren sind diejenigen einstufig rekurrenten, die lineare Kongruenzen verwenden. Sie haben zunächst den Vorteil, dass sie sehr schnell sind. Sie erzeugen aber auch lange Perioden, und ihre Zufallsqualitäten lassen sich wegen ihrer einfachen Bauart leicht theoretisch absichern.

Die Zufallserzeugung mit linearen Kongruenzen geht so:

$$x_n = s(x_{n-1}) \text{ mit}$$

$$s : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad s(x) = ax + b \bmod m.$$

Die Folge hängt also von vier ganzzahligen Parametern ab; diese sind

- der **Modul** m mit $m \geq 2$,
- der **Multiplikator** $a \in [0 \ldots m-1]$,
- das **Inkrement** $b \in [0 \ldots m-1]$,
- der **Startwert** $x_0 \in [0 \ldots m-1]$.

Ein solcher Zufallsgenerator heißt **linearer Kongruenzgenerator**, wobei man im Fall $b = 0$ auch von einem **multiplikativen Generator**, im Falle $b \neq 0$ von einem **gemischten Kongruenzgenerator** spricht. Ein solcher Generator ist sehr einfach zu programmieren, selbst in Assembler, und ist sehr schnell. Gut ist er, *wenn die Parameter* m, a, b *geeignet gewählt sind.* Der Startwert ist dagegen völlig problemlos frei wählbar. Auch das ist wichtig, um bei Bedarf die erzeugten Zufallszahlen genügend variieren zu können.

Bei der Anwendung für die Bitstrom-Verschlüsselung wird der Startwert x_0 oder aber der ganze Parametersatz (m, a, b, x_0) als effektiver Schlüssel betrachtet, d. h., geheim gehalten.

Bemerkungen

1. Da nur endlich viele Werte x_n möglich sind, ist die Folge periodisch mit einer Periodenlänge $\leq m$; dabei kann auch am Anfang eine Vorperiode auftreten.

2. Die Wahl von $a = 0$ ist offensichtlich unsinnig. Aber auch $a = 1$ erzeugt eine Folge, nämlich $x_0, x_0 + b, x_0 + 2b, x_0 + 3b, \ldots$, die nicht brauchbar ist, weil sie auch mod$m$ immer wieder lange regelmäßige Stücke enthält.

3. Für $m = 13$, $a = 6$, $b = 0$, $x_0 = 1$ wird die Folge

$$6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1$$

der Periodenlänge 12 erzeugt, die der Vorstellung einer zufälligen Permutation der Zahlen 1 bis 12 schon recht nahe kommt (trotz des sehr kleinen Moduls).

4. Nimmt man statt dessen den Multiplikator 7, so entsteht die deutlich weniger sympathische Folge

$$7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1.$$

5. Ist a zu m teilerfremd, so ist die Folge rein-periodisch (d. h., es gibt keine Vorperiode). Es ist nämlich $a \bmod m$ invertierbar, also $ac \equiv 1 \pmod{m}$ für ein c. Daher ist stets $x_{n-1} = cx_n - cb \bmod m$. Ist nun $x_{\mu+\lambda} = x_\mu$ mit $\mu \geq 1$, so auch $x_{\mu+\lambda-1} = x_{\mu-1}$ usw., schließlich $x_\lambda = x_0$.

6. Durch Induktion beweist man sofort

$$x_k = a^k x_0 + (1 + a + \cdots + a^{k-1}) \cdot b \bmod m$$

für alle k – ein krasser Hinweis darauf, wie wenig zufällig die Folge in Wirklichkeit ist: Sogar der direkte Zugriff auf ein beliebiges Folgenglied ist möglich, denn der Koeffizient von b ist $(a^k - 1)/(a - 1)$, wobei die Division mod m vorzunehmen ist.

7. Sei $m = 2^e$ und a gerade. Dann ist

$$x_k = (1 + a + \cdots + a^{e-1}) \cdot b \bmod m$$

für alle $k \geq e$, die Periode also 1. Allgemein verkürzen gemeinsame Teiler von a und m die Periode und sind daher zu vermeiden.

8. Sei d ein Teiler des Moduls m. Die Folge $y_n = x_n \bmod d$ ist dann die entsprechende Kongruenzfolge zum Modul d, also $y_n = ay_{n-1} + b \bmod d$. Die Folge (x_n) hat $\bmod d$ also eine Periode $\leq d$, die eventuell sehr kurz ist.

9. Besonders drastisch ist dieser Effekt im Fall einer Zweierpotenz, $m = 2^e$, zu sehen: Das niedrigste Bit von x_n hat dann bestenfalls die Periode 2, ist also abwechselnd 0 und 1, wenn es nicht überhaupt konstant ist. Die k niedrigsten Bits zusammen haben höchstens die Periode 2^k.

10. Ein Modul m mit vielen Teilern, insbesondere eine Zweierpotenz, ist also gegenüber einem Primzahlmodul bei der Zufallserzeugung gehandikapt. Die Qualität ist aber oft doch noch ausreichend, wenn man die erzeugten Zahlen durch m dividiert, also als Zufallszahlen im reellen Intervall $[0, 1[$ ansieht, und am rechten Ende großzügig rundet. Für kryptographische Anwendungen sind solche Moduln aber sicher nicht geeignet.

11. Im Beispiel $m = 2^{32}$, $a = 4095 = 2^{12} - 1$, $b = 12794$ sind die Parameter nicht geeignet gewählt: Aus $x_0 = 253$ ergibt sich $x_1 = 1048829$ und $x_2 = 253 = x_0$.

    Beliebte Moduln sind

    - $m = 2^{32}$, weil er den 32-Bit-Bereich ausschöpft und außerdem sehr effizient handhabbar ist,
    - $m = 2^{31} - 1$, weil dies oft die maximale darstellbare Ganzzahl ist und weil man damit fast so effizient rechnen kann wie mit einer Zweierpotenz. Ein weiterer Vorteil: Diese Zahl ist eine Primzahl (von MERSENNE 1644 behauptet, von EULER 1772 bewiesen), und das hat gute Auswirkungen auf die Qualität der erzeugten Zufallsfolge. Allgemeiner sind FERMAT-Primzahlen $2^k + 1$ und MERSENNE-Primzahlen $2^k - 1$ ähnlich gut geeignet; die nächste solche Zahl ist $2^{61} - 1$.

Die ersten 100 Glieder einer Folge, die mit dem Modul $m = 2^{31} - 1 = 2147483647$, dem Multiplikator $a = 397204094$, dem Inkrement $b = 0$ und dem Startwert $x_0 = 58854338$ erzeugt wurde, zeigt Tabelle 1. In Abbildung 1 ist diese Information visuell umgesetzt. Man sieht daran schon eine deutliche Regellosigkeit der Folge. Es wird aber auch klar, dass ein solcher visueller Eindruck wohl kaum ausreicht, um die Qualität einer Zufallsfolge zu beurteilen.

Abbildung 1: Eine lineare Kongruenzfolge. Waagerechte Achse: Zähler von 0 bis 100, senkrechte Achse: Größe des Folgenglieds von 0 bis $2^{31} - 1$.

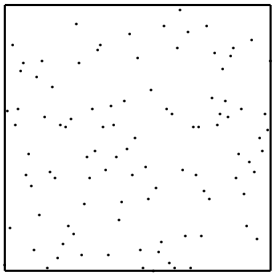

Tabelle 1: 100 Glieder einer linearen Kongruenzfolge

1292048469	319941267	173739233	1992841820
345565651	2011011872	31344917	592918912
1827933824	1691830787	857231706	1416540893
1184833417	145217588	589958351	1776690121
1330128247	558009026	1479515830	1197548384
1627901332	929586843	19840670	1268974074
1682548197	760357405	666131673	1642023821
787305132	1314353697	167412640	1377012759
963849348	971229179	247170576	1250747100
703109068	1791051358	1978610456	1746992541
177131972	1844679385	1328403386	1811091691
1586500120	1175539757	74957396	753264023
468643347	821920620	1269873360	963348259
1698955999	139484430	30476960	1327705603
1266305157	1337811914	1808105128	640050202
37935526	1185470453	2111728842	380228478
808553600	934194915	824017077	881361640
1492263703	414709486	298916786	1883338449
771128019	558671080	1935988732	798347213
120356246	1378842534	37149011	272238278
1190345324	1006355270	1161592162	1079789655
220609946	1918105148	791775291	979447727
1160648370	779600833	1170336930	1271974642
375813045	1089009771	280197098	1144249742
1236647368	1729816359	650188387	1714906064