8 Zufallszahlen

(8.1) Wenn man mit dem in §7 beschriebenen Primzahltest von Rabin eine natürliche Zahl m darauf testen will, ob sie eine Primzahl ist, so ist mehrere Male eine Zahl aus der Menge $\mathcal{M}_m = \{1, 2, \cdots, m-1\}$ zufällig zu wählen. Die Abschätzung der Fehlerwahrscheinlichkeit beim Primzahltest von Rabin in (7.5)(2) beruht darauf, daß diese Wahl wirklich zufällig geschieht. Wohl jeder hat eine Vorstellung, was dies bedeutet, etwa daß jede der $m-1$ Zahlen aus $\mathcal{M}_m$ mit derselben Wahrscheinlichkeit ausgewählt wird oder daß eine gewählte Zahl nicht von eventuell vorher ausgewählten Zahlen abhängig ist. Es ist aber zunächst nicht klar, wie man in einem Rechner das zufällige Auswählen von Elementen aus einer Menge $\mathcal{M}$ von Zahlen, etwa aus dem Intervall $[0, 1[$, realisieren soll. Dies geschieht folgendermaßen: Man findet einen Algorithmus, der der Reihe nach die Terme einer Folge $(u_i)_{i\geq 0}$ von Zahlen aus $\mathcal{M}$ ausgibt, und diese Folge testet man mittels statistischer Tests darauf, ob sie Eigenschaften besitzt, die man mit der Vorstellung einer Folge von zufällig aus $\mathcal{M}$ ausgewählten Zahlen verbindet. Eine solche Folge wird im folgenden eine Folge von Zufallszahlen aus der Menge $\mathcal{M}$ heißen. Über die Schwierigkeit, Zufallszahlen begrifflich sauber zu fassen, kann man in Knuth [55], Abschnitt 3.5, und in Lagarias [59] nachlesen.

(8.2) Bezeichnung: Es sei $m \in \mathbb{N}$, und es seien a, b, $x^* \in \mathbb{Z}$. Die Folge $(x_i)_{i\geq 0}$ in $\{0, 1, \ldots, m-1\}$ mit

$$x_0 := x^* \bmod m \quad \text{und} \quad x_i := (ax_{i-1} + b) \bmod m \quad \text{für jedes } i \in \mathbb{N}$$

heißt die durch (m, a, b, x^*) definierte L-Folge.

(8.3) Bemerkung: Es seien $m \in \mathbb{N}$ und a, b, $x^* \in \mathbb{Z}$, und es sei $(x_i)_{i\geq 0}$ die durch (m, a, b, x^*) definierte L-Folge.
(1) Da die Menge $\{0, 1, \ldots, m-1\}$ endlich ist, ist die Folge $(x_i)_{i\geq 0}$ – eventuell erst nach einer Vorperiode – periodisch. Es gibt also ein $k \in \mathbb{N}_0$ und ein $l \in \mathbb{N}$ mit: $x_0, x_1, \ldots, x_{k-1}, x_k, x_{k+1}, \ldots, x_{k+l-1}$ sind paarweise verschieden, und für jedes $j \in \mathbb{N}_0$ ist $x_{k+j} = x_{k+(j \bmod l)}$. $(x_0, x_1, \ldots, x_{k-1})$ heißt die Vorperiode, $(x_k, x_{k+1}, \ldots, x_{k+l-1})$ die Periode und l die Periodenlänge der Folge $(x_i)_{i\geq 0}$.
(2) Es seien $i, j \in \mathbb{N}$ mit $j > i \geq k$ und mit $x_i = x_j$. Dann ist $j - i$ durch die Periodenlänge l teilbar, denn es gilt $r := (j-i) \bmod l \in \{0, 1, \ldots, l-1\}$ und $x_i = x_j = x_{i+(j-i)} = x_{i+r}$, und da $x_i, x_{i+1}, \ldots, x_{i+(l-1)}$ paarweise verschieden sind, folgt $r = 0$.
(3) Durch Induktion folgt sogleich: Für jedes $i \in \mathbb{N}$ ist

$$x_i = \left(a^i x^* + b(1 + a + a^2 + \cdots + a^{i-1})\right) \bmod m =$$

$$= \begin{cases} (a^i x^* + ib) \bmod m, & \text{falls } a \equiv 1 \pmod m \text{ gilt,} \\ \left(a^i x^* + b\dfrac{a^i - 1}{a - 1}\right) \bmod m, & \text{falls } a \not\equiv 1 \pmod m \text{ gilt.} \end{cases}$$

(4) Gilt $\mathrm{ggT}(a, m) = 1$, so besitzt die Folge $(x_i)_{i\geq 0}$ keine Vorperiode, und für ihre Periodenlänge l gilt $l = \min(\{i \in \mathbb{N} \mid x_i = x_0\})$.
Beweis: Es gelte $\mathrm{ggT}(a, m) = 1$, und es seien $i, j \in \mathbb{N}$ mit $i < j$ und mit $x_i = x_j$. Es gilt

$$\begin{aligned} & a^i\left((a^{j-i} - 1)x^* + b(1 + a + a^2 + \cdots + a^{j-i-1})\right) = \\ & = \left(a^j x^* + b(1 + a + \cdots + a^{j-1})\right) - \left(a^i x^* + b(1 + a + \cdots + a^{i-1})\right) \equiv \\ & \equiv x_j - x_i = 0 \pmod m, \end{aligned}$$

wegen $\mathrm{ggT}(a, m) = 1$ folgt daraus

$$(a^{j-i} - 1)x^* + b(1 + a + a^2 + \cdots + a^{j-i-1}) \equiv 0 \pmod m,$$

also

$$x_0 = x^* \bmod m = \left(a^{j-i}x^* + b(1 + a + a^2 + \cdots + a^{j-i-1})\right) \bmod m = x_{j-i}.$$

Also gehört x_0 zur Periode der Folge $(x_i)_{i\geq 0}$. Daher besitzt diese Folge keine Vorperiode, und ihre Periodenlänge ist die kleinste natürliche Zahl i, für die $x_i = x_0$ ist.

(8.4) Bemerkung: D. H. Lehmer hat in [62] das folgende Verfahren zur Erzeugung von Zufallszahlen im Intervall $[0, 1[$ vorgeschlagen: Man wähle Zahlen $m \in \mathbb{N}$ und a, b, x^* in $\mathbb{Z}$, berechne die Terme der durch (m, a, b, x^*) definierte L-Folge $(x_i)_{i\geq 0}$ und setze $u_i := x_i/m$ für jedes $i \in \mathbb{N}_0$. Dann ist $(u_i)_{i\geq 0}$ eine Folge im Intervall $[0, 1[$, die man statistischen Tests unterzieht und, falls deren Ergebnisse es erlauben, als Folge von Zufallszahlen verwenden kann.

Der Vorteil dieses Verfahrens besteht darin, daß man sehr schnell viele Terme einer L-Folge berechnen kann. Ein offensichtlicher Nachteil besteht darin, daß L-Folgen und daher auch die aus ihnen gewonnenen Folgen in $[0, 1[$ periodisch sind. Es kommt daher darauf an, Bedingungen für die Zahlen m, a, b und x^* zu finden, die sicherstellen, daß die durch (m, a, b, x^*) definierte L-Folge eine möglichst lange Periode und wenn möglich sogar eine Periode der Länge m besitzt. Von solchen Bedingungen wird in den nächsten Abschnitten die Rede sein. G. Marsaglia hat in [66] Sätze über die "Feinstruktur" von L-Folgen bewiesen und gezeigt, wie man mit deren Hilfe L-Folgen finden kann, die zur Herstellung von Zufallszahlen geeignet sind. Auf [66] stützen sich die folgende beiden Hilfssätze.

(8.5) Hilfssatz: *Es seien $m \in \mathbb{N}$ und a, b, $x^* \in \mathbb{Z}$, es sei $(x_i)_{i\geq 0}$ die durch (m, a, b, x^*) definierte L-Folge, und es sei $(y_i)_{i\geq 0}$ die durch $(m, a, 1, 0)$ definierte L-Folge; es sei $v := ((a-1)x^* + b) \bmod m$.*
(1) *Für jedes $i \in \mathbb{N}_0$ ist $x_i = (vy_i + x^*) \bmod m$.*
(2) *Es gelte $\mathrm{ggT}(a, m) = 1$, und es sei $s := \mathrm{ggT}(v, m)$. Die Folge $(x_i)_{i\geq 0}$ hat dieselbe Periodenlänge wie die durch $(m/s, a, 1, 0)$ definierte L-Folge.*

Beweis: (1) folgt durch Induktion nach i, und (2) folgt so: Nach (8.3)(4) besitzt die Folge $(x_i)_{i\geq 0}$ keine Vorperiode, und ihre Periodenlänge l ist die kleinste natürliche Zahl i mit $x_i = x_0$. Für $i \in \mathbb{N}$ gilt: Nach (1) ist $x_i = x_0$, genau wenn $vy_i + x^* \equiv x^* \pmod m$ gilt, also genau wenn $vy_i \equiv 0 \pmod m$ ist, und vy_i ist durch m teilbar, genau wenn $(v/s)y_i$ durch m/s teilbar ist, also wegen $\mathrm{ggT}(v/s, m/s) = 1$ genau wenn y_i durch m/s teilbar ist. Also ist l die kleinste natürliche Zahl i, für die y_i durch m/s teilbar ist. Die durch $(m/s, a, 1, 0)$ definierte L-Folge ist $(y_i \bmod (m/s))_{i\geq 0}$, und wegen $\mathrm{ggT}(a, m/s) = 1$ hat nach (8.3)(4) diese Folge keine Vorperiode, und ihre Periodenlänge ist wegen $y_0 = 0$

$$\begin{aligned}\min\bigl(\{i \in \mathbb{N} \mid y_i \bmod (m/s) = y_0 \bmod (m/s)\}\bigr) \;&= \\ = \min\bigl(\{i \in \mathbb{N} \mid y_i \equiv 0 \pmod{(m/s)}\}\bigr) \;&= l.\end{aligned}$$

(8.6) Hilfssatz: *Es sei m eine natürliche Zahl, es sei a eine ganze Zahl mit $\mathrm{ggT}(a, m) = 1$, es sei d die Ordnung von $[a]_m$ in der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$, und es seien*

$$c := (1 + a + a^2 + \cdots + a^{d-1}) \bmod m \quad \text{und} \quad t := \frac{m}{\mathrm{ggT}(c, m)}.$$

Die durch $(m, a, 1, 0)$ definierte L-Folge $(y_i)_{i\geq 0}$ hat die Periodenlänge dt, und für jedes $i \in \{0, 1, \ldots, d-1\}$ und jedes $j \in \{0, 1, \ldots, t-1\}$ gilt

$$y_{i+jd} = (y_i + jc) \bmod m,$$

d.h. die Periode von $(y_i)_{i\geq 0}$ besteht der Reihe nach aus den dt Zahlen

$$\begin{array}{cccc} 0, & y_1, & \ldots & y_{d-1}, \\ c, & (y_1 + c) \bmod m, & \ldots & (y_{d-1} + c) \bmod m, \\ (2c) \bmod m, & (y_1 + 2c) \bmod m, & \ldots & (y_{d-1} + 2c) \bmod m, \\ \vdots & \vdots & & \vdots \\ ((t-1)c) \bmod m, & (y_1 + (t-1)c) \bmod m, & \ldots & (y_{d-1} + (t-1)c) \bmod m. \end{array}$$

Beweis: Wegen $\mathrm{ggT}(a, m) = 1$ hat die Folge $(y_i)_{i\geq 0}$ keine Vorperiode, und für ihre Periodenlänge l gilt $l = \min(\{i \in \mathbb{N} \mid y_i = 0\})$. Es gilt

$$a^l - 1 = (a-1)(1 + a + a^2 + \cdots + a^{l-1}) \equiv (a-1)y_l = 0 \pmod m,$$

also $[a]_m^l = [1]_m$, und daher ist l durch die Ordnung $d = \mathrm{ord}([a]_m)$ von $[a]_m$ in der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ teilbar (vgl. (3.5)(3)). Insbesondere ist somit $d \leq l$, und daher sind $y_0 = 0, y_1, \ldots, y_{d-1}$ paarweise verschieden. Für jedes $i \in \mathbb{N}_0$ gilt wegen $a^d \equiv 1 \pmod m$

$$(*) \quad y_{i+d} \equiv \sum_{j=0}^{i+d-1} a^j \equiv a^d \cdot \sum_{j=0}^{i-1} a^j + c = a^d y_i + c \equiv y_i + c \pmod m.$$

Hieraus folgt insbesondere: Es ist

$$0 = y_0 = y_l = y_{(l/d)\cdot d} \equiv y_0 + \frac{l}{d}c = \frac{l}{d}c \pmod m,$$

und für jedes $k \in \{1, 2, \ldots, l/d - 1\}$ gilt $kd < l$, also $kc \equiv y_{kd} \not\equiv 0 \pmod m$. Daher ist l/d die kleinste natürliche Zahl k mit $m \mid kc$, und diese ist, wie man sogleich sieht, gerade $m/\,\mathrm{ggT}(c, m)$. Also ist $l = dm/\,\mathrm{ggT}(c, m) = dt$. Außerdem folgt aus $(*)$, daß die Periode von $(y_i)_{i\geq 0}$ die angegebene Gestalt besitzt.

(8.7) Hilfssatz: *Es seien m_1 und m_2 teilerfremde natürliche Zahlen, es seien a, b, $x^* \in \mathbb{Z}$, und es sei $m := m_1 m_2$; es seien l_1 die Periodenlänge der durch (m_1, a, b, x^*) definierten L-Folge und l_2 die Periodenlänge der durch (m_2, a, b, x^*) definierten L-Folge. Dann gilt für die Länge der durch (m, a, b, x^*) definierten L-Folge $(x_i)_{i\geq 0}$: Es ist $l = \mathrm{kgV}(l_1, l_2)$.*

Beweis: Die durch (m_1, a, b, x^*) definierte L-Folge ist $(x_i \bmod m_1)_{i\geq 0}$, und die durch (m_2, a, b, x^*) definierte L-Folge ist $(x_i \bmod m_2)_{i\geq 0}$. Es sei $i \in \mathbb{N}$ größer als die Längen der Vorperioden der Folgen $(x_i)_{i\geq 0}$, $(x_i \bmod m_1)_{i\geq 0}$ und $(x_i \bmod m_2)_{i\geq 0}$. Wegen $x_i = x_{i+l}$ gilt $x_i \bmod m_1 = x_{i+l} \bmod m_1$ und $x_i \bmod m_2 = x_{i+l} \bmod m_2$, und nach (8.3)(2) ist daher l durch l_1 und durch l_2 teilbar. Also ist l durch $l' := \mathrm{kgV}(l_1, l_2)$ teilbar. Wegen $l_1 \mid l'$ und $l_2 \mid l'$ gilt andererseits $x_{i+l'} \bmod m_1 = x_i \bmod m_1$ und $x_{i+l'} \bmod m_2 = x_i \bmod m_2$, und daher ist $x_{i+l'} - x_i$ durch $\mathrm{kgV}(m_1, m_2) = m_1 m_2 = m$ teilbar. Also ist $x_{i+l'} = x_i$, und nach (8.3)(2) folgt $l \mid l'$. Damit ist gezeigt: Es ist $l = l' = \mathrm{kgV}(l_1, l_2)$.

(8.8) Bemerkung: (1) Es sei p eine Primzahl, es sei $\beta \in \mathbb{N}$, es sei $z \in \mathbb{Z}$, und es gelte $p^\beta > 2$, d.h. es gelte $\beta > 1$, falls $p = 2$ ist. Dann sind

$$x := \sum_{j=2}^{p} \binom{p}{j} z^{j-1} p^{(j-1)\beta-2} = \binom{p}{2} z\, p^{\beta-2} + \sum_{j=3}^{p} \binom{p}{j} z^{j-1} p^{(j-1)\beta-2} =$$

$$= z \cdot \frac{(p-1)p^{\beta-1}}{2} + \sum_{j=3}^{p} \binom{p}{j} z^{j-1} p^{(j-1)\beta-2}$$

und $z_1 := (1+px)z$ ganze Zahlen, und es gilt

$$(1+zp^\beta)^p = \sum_{j=0}^{p} \binom{p}{j} z^j p^{j\beta} = 1 + \binom{p}{1} zp^\beta + \sum_{j=2}^{p} \binom{p}{j} z^j p^{j\beta} =$$
$$= 1 + (1+px)zp^{\beta+1} = 1 + z_1 p^{\beta+1}.$$

Wenn z nicht durch p teilbar ist, ist auch z_1 nicht durch p teilbar.
(2) Es sei p eine Primzahl, es seien $\beta, \gamma \in \mathbb{N}$, es sei $z \in \mathbb{Z}$, und es gelte $p^\beta > 2$. Durch Induktion nach γ folgt mittels (1): Es ist

$$(1+zp^\beta)^{p^\gamma} = 1 + z_\gamma p^{\beta+\gamma}$$

mit einer ganzen Zahl z_γ, die nicht durch p teilbar ist, falls z nicht durch p teilbar ist.

(8.9) Satz: *Es sei $m \in \mathbb{N}$, es seien a, b, $x^* \in \mathbb{Z}$, und es gelte:*
(a) *b und m sind teilerfremd.*
(b) *Für jeden Primteiler p von m gilt $a \equiv 1 \pmod{p}$.*
(c) *Ist m durch 4 teilbar, so gilt $a \equiv 1 \pmod{4}$.*
Dann hat die Periode der durch (m, a, b, x^*) definierten L-Folge $(x_i)_{i\geq 0}$ die Länge m.

Beweis: (1) Es sei p ein Primteiler von m, und es sei $\alpha := v_p(m)$ der Exponent von p in der Primzerlegung von m. Es sei $d := \operatorname{ord}([a]_{p^\alpha})$, und es seien $c := (1 + a + a^2 + \cdots + a^{d-1}) \bmod p^\alpha$ und $t := p^\alpha / \operatorname{ggT}(c, p^\alpha)$. Nach (8.6) hat die durch $(p^\alpha, a, 1, 0)$ definierte L-Folge die Periodenlänge dt.
(a) Es gelte $a \equiv 1 \pmod{p^\alpha}$, also $[a]_{p^\alpha} = [1]_{p^\alpha}$. Dann ist $d = 1$ und daher $c = 1$, und es folgt $t = p^\alpha / \operatorname{ggT}(1, p^\alpha) = p^\alpha$. Also ist $dt = p^\alpha$. (Dies erledigt insbesondere den Fall $p = 2$ und $v_2(m) = \alpha = 1$).
(b) Es gelte $a \not\equiv 1 \pmod{p^\alpha}$. Dann gilt $1 \leq \beta := v_p(a-1) < \alpha$, und es ist $p^\beta > 2$, denn es gilt $\alpha > 1$, also ist m im Fall $p = 2$ durch 4 teilbar, und nach Voraussetzung ist daher $\beta \geq 2$. Es gilt $a = 1 + zp^\beta$ mit einem $z \in \mathbb{Z} \setminus p\mathbb{Z}$, und nach (8.8)(2) gibt es ein $z_0 \in \mathbb{Z} \setminus p\mathbb{Z}$ mit

$$a^{p^{\alpha-\beta}} = (1+zp^\beta)^{p^{\alpha-\beta}} = 1 + z_0 p^\alpha \equiv 1 \pmod{p^\alpha},$$

also ist $d = \operatorname{ord}([a]_{p^\alpha})$ ein Teiler von $p^{\alpha-\beta}$. Ebenfalls nach (8.8)(2) gibt es ein $z_1 \in \mathbb{Z} \setminus p\mathbb{Z}$ mit

$$a^{p^{\alpha-\beta-1}} = (1+zp^\beta)^{p^{\alpha-\beta-1}} = 1 + z_1 p^{\alpha-1} \not\equiv 1 \pmod{p^\alpha}.$$

Damit ist gezeigt, daß $d = p^{\alpha-\beta}$ ist. Es gilt

$$zp^\beta c \equiv (a-1)(1 + a + a^2 + \cdots + a^{d-1}) = a^d - 1 =$$
$$\equiv (1+zp^\beta)^d - 1 = (1+zp^\beta)^{p^{\alpha-\beta}} - 1 = z_0 p^\alpha \equiv 0 \pmod{p^\alpha},$$

und weil z und z_0 nicht durch p teilbar sind, folgt $v_p(c) = \alpha - \beta$. Also ist $t = p^\alpha / \operatorname{ggT}(c, p^\alpha) = p^\alpha / p^{\alpha-\beta} = p^\beta$. Damit ist gezeigt, daß auch in diesem zweiten Fall $dt = p^\alpha$ gilt.
(2) Es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m. Nach (1) besitzt für jedes $j \in \{1, 2, \ldots, r\}$ die durch $(p_j^{\alpha_j}, a, 1, 0)$ definierte L-Folge die Periodenlänge $p_j^{\alpha_j}$. Nach (8.7) hat daher die durch $(m, a, 1, 0)$ definierte L-Folge die Periodenlänge $\operatorname{kgV}(p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}) = m$.
(3) Die durch (m, a, b, x^*) definierte L-Folge $(x_i)_{i\geq 0}$ hat nach (8.5)(2) dieselbe Periodenlänge wie die durch

$$\Big(\frac{m}{\operatorname{ggT}\big((a-1)x^* + b, m\big)}, a, 1, 0\Big)$$

definierte L-Folge. Aus den Voraussetzungen (a) und (b) folgt, daß

$$\operatorname{ggT}\big((a-1)x^* + b, m\big) \;=\; 1$$

ist. Somit ist die Periodenlänge von $(x_i)_{i\geq 0}$ gleich der Periodenlänge der durch $(m, a, 1, 0)$ definierten L-Folge, also nach (2) gleich m.

(8.10) Bemerkung: Man kann beweisen, daß die in (8.9) angegebenen Bedingungen (a), (b) und (c) die L-Folgen mit maximaler Periodenlänge charakterisieren; man vergleiche dazu Kiyek-Schwarz [54], Kap. XI, § 7, oder Knuth [55], Abschnitt 3.2.1.2. In der Praxis begegnet man auch L-Folgen, die der folgende Satz behandelt; darin ist $\lambda : \mathbb{N} \to \mathbb{N}$ die Carmichael-Funktion (vgl. dazu Abschnitt (5.21)).

(8.11) Satz: *Es sei $m \in \mathbb{N}$, es seien a, $x^* \in \mathbb{Z}$, und es gelte:*
(a) *x^* und m sind teilerfremd.*
(b) *Für jeden ungeraden Primteiler p von m ist a eine Primitivwurzel modulo $p^{v_p(m)}$.*
(c) *Ist m gerade, so gilt*

$$\begin{cases} a \equiv 1 \pmod 2, & \text{falls } v_2(m) = 1 \text{ ist,} \\ a \equiv 3 \pmod 4, & \text{falls } v_2(m) = 2 \text{ ist,} \\ a \equiv 3 \text{ oder } 5 \text{ oder } 7 \pmod 8, & \text{falls } v_2(m) = 3 \text{ ist,} \\ a \equiv 3 \text{ oder } 5 \pmod 8, & \text{falls } v_2(m) \geq 4 \text{ ist.} \end{cases}$$

Dann besitzt die durch $(m, a, 0, x^*)$ definierte L-Folge (x_i) keine Vorperiode, und ihre Periode hat die Länge $\lambda(m)$.

Beweis: Wegen (b) und (c) ist $\operatorname{ggT}(a, m) = 1$, und daher hat $(x_i)_{i\geq 0}$ keine Vorperiode.

(1) Es sei p ein Primteiler von m, und es sei $\alpha := v_p(m)$. Ist p ungerade, so ist a nach (b) eine Primitivwurzel modulo p^α, und dies bedeutet, daß

$$\operatorname{ord}([a]_{p^\alpha}) = \varphi(p^\alpha) = p^{\alpha-1}(p-1) = \lambda(p^\alpha)$$

ist. Es gilt

$$\begin{aligned} \operatorname{ord}([1]_2) &= 1 = \lambda(2), \quad \operatorname{ord}([3]_4) = 2 = \lambda(4), \\ \operatorname{ord}([3]_8) &= \operatorname{ord}([5]_8) = \operatorname{ord}([7]_8) = 4 = \lambda(8) \end{aligned}$$

und für jedes $\beta \in \mathbb{N}$ mit $\beta \geq 4$

$$\operatorname{ord}([3]_{2^\beta}) = \operatorname{ord}([5]_{2^\beta}) = 2^{\beta-2} = \lambda(2^\beta)$$

(vgl. (5.20)). Also gilt wegen der Voraussetzung (c) auch im Fall $p = 2$: Es ist $\operatorname{ord}([a]_{p^\alpha}) = \lambda(p^\alpha)$.

Wegen $p \nmid a$ hat die durch $(p^\alpha, a, 0, x^*)$ definierte L-Folge $(x_i \bmod p^\alpha)_{i\geq 0}$ keine Vorperiode, und ihre Periode hat die Länge

$$\begin{aligned} l_p &= \min(\{i \in \mathbb{N} \mid x_i \bmod p^\alpha = x_0 \bmod p^\alpha\}) = \\ &= \min(\{i \in \mathbb{N} \mid x_i \equiv x_0 \pmod{p^\alpha}\}). \end{aligned}$$

Für $i \in \mathbb{N}$ gilt $x_i = (a^i x^*) \bmod m$, und daher gilt: Es ist $x_i \equiv x_0 \pmod{p^\alpha}$, genau wenn $a^i x^* \equiv x^* \pmod{p^\alpha}$ ist, also genau wenn $a^i \equiv 1 \pmod{p^\alpha}$ ist (wegen $p \nmid x^*$), also nach (4.23) genau wenn i durch $\operatorname{ord}([a]_{p^\alpha})$ teilbar ist. Also ist $l_p = \operatorname{ord}([a]_{p^\alpha}) = \lambda(p^\alpha)$.

(2) Es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m. Nach (1) hat für jedes $j \in \{1, 2, \ldots, r\}$ die durch $(p_j^{\alpha_j}, a, 0, x^*)$ definierte L-Folge die Periodenlänge $\lambda(p_j^{\alpha_j})$. Nach (8.7) gilt daher für die Periodenlänge l von $(x_i)_{i\geq 0}$: Es ist

$$l = \operatorname{kgV}(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_r^{\alpha_r})) \overset{(5.22)}{=} \lambda(m).$$

(8.12) Beispiele: (1) Die erste von D. H. Lehmer in [62] zur Erzeugung von Zufallszahlen vorgeschlagene L-Folge war die durch $(10^8 + 1, 23, 0, 47\,594\,118)$ definierte L-Folge $(x_i)_{i\geq 0}$. $10^8 + 1$ ist das Produkt der Primzahlen 17 und 5 882 353, und 23 ist eine Primitivwurzel modulo 17 und modulo 5 882 353. Nach (8.11) hat daher die Folge $(x_i)_{i\geq 0}$ keine Vorperiode, und die Länge ihrer Periode ist

$$\lambda(10^8 + 1) = \operatorname{kgV}(\lambda(17), \lambda(5\,882\,353)) = \operatorname{kgV}(16, 5\,882\,352) = 5\,882\,352.$$

Statistische Tests zeigen, daß diese Folge zur Erzeugung von Zufallszahlen gemäß (8.4) geeignet ist; die im folgenden Abschnitt erwähnten theoretischen Tests ergeben allerdings, daß sie nur mäßig brauchbar ist, da ihr Multiplikator 23 zu klein ist.
(2) Es sei $\beta \in \mathbb{N}$ mit $2 \leq \beta < 35$, es seien b, $x^* \in \mathbb{Z}$, und dabei sei b ungerade. Die durch $(2^{35}, 2^\beta + 1, b, x^*)$ definierte L-Folge hat nach (8.9) eine Periode der Länge 2^{35}. L-Folgen, bei denen der Modul m eine Potenz von 2 ist, wurden 1960 von A. Rotenberg in [94] zur Erzeugung von Zufallszahlen vorgeschlagen und getestet.
(3) Das "Standard Apple Numeric Environment (SANE)" der Macintosh-Rechner der Firma Apple stellt zur Erzeugung von Zufallszahlen die L-Folge bereit, die durch $(2^{31} - 1, 7^5, 0, x^*)$ definiert ist, wobei x^* eine nicht durch $2^{31} - 1$ teilbare ganze Zahl ist. Da $2^{31} - 1$ eine Primzahl und 7^5 eine Primitivwurzel modulo $2^{31} - 1$ ist, besitzt diese Folge nach (8.11) eine Periode der Länge $2^{31} - 2$. (Diese Periode besteht aus den natürlichen Zahlen $\leq 2^{31} - 2$, da 0 darin nicht vorkommen kann).
(4) Die NAG-Bibliothek, eine umfangreiche Sammlung von Routinen zur Numerischen Mathematik, verwendet zur Erzeugung von Zufallszahlen die durch $(2^{59},\ 13^{13},\ 0,\ (2^{32}+1) \cdot 123456789)$ erzeugte L-Folge (Routine G05CAF). Wegen $13^{13} \bmod 8 = 5$ besitzt diese Folge nach (8.11) keine Vorperiode, und ihre Periode hat die Länge 2^{57}.

(8.13) MuPAD: MuPAD benützt zur Herstellung von Zufallszahlen die durch

$$(999\,999\,999\,989,\ 427\,419\,669\,081,\ 0,\ 1)$$

definierte L-Folge $(x_i)_{i\geq 0}$. $m := 999\,999\,999\,989$ ist die größte Primzahl, die kleiner als 10^{12} ist. Da $427\,419\,669\,081$ eine Primitivwurzel modulo m ist, besitzt nach (8.11) die Folge $(x_i)_{i\geq 0}$ keine Vorperiode, und ihre Periode hat die Länge $m-1$. Die Terme dieser Folge werden von der MuPAD-Funktion `random` berechnet: Jeder Aufruf `random()` liefert einen Term der Folge $(x_i)_{i\geq 1}$. Man kann innerhalb einer MuPAD-Sitzung jederzeit einen neuen Startwert für diese Folge erklären, und zwar durch eine Anweisung `SEED := s`, wobei s eine von Null verschiedene ganze Zahl ist. (Zu Beginn einer MuPAD-Sitzung hat `SEED` stets den Wert 1).

Mit Hilfe der MuPAD-Funktion `random` kann man für jedes $q \in \mathbb{N}$ Zufallszahlen aus der Menge $\{0, 1, \ldots, q-1\}$ erzeugen. Ist q eine natürliche Zahl, so definiert `X := random(0..q-1)` oder kürzer `X := random(q)` eine MuPAD-Funktion X, für die gilt: Jeder Aufruf `X()` liefert einen Term einer Folge $(y_i)_{i\geq 1}$ aus Elementen der Menge $\{0, 1, \ldots, q-1\}$. Ist $q \leq m$, so ist dabei $y_i = x_i \bmod q$; ist $q > m$, so ist mit

$$k := \max(\{j \in \mathbb{N} \mid m^j < q\})$$

für jedes $i \in \mathbb{N}$

$$y_i = \Big(x_{i+(i-1)k} \cdot 10^{12k} + x_{i+(i-1)k+1} \cdot 10^{12(k-1)} + \\ + \cdots + x_{i+ik-1} \cdot 10^{12} + x_{i+ik}\Big) \bmod q.$$

(8.14) Es seien $m \in \mathbb{N}$ und $a, b, x^* \in \mathbb{Z}$, und es sei $(x_i)_{i\geq 0}$ die durch (m, a, b, x^*) definierte L-Folge. Wenn man die Terme der Folge $(x_i/m)_{i\geq 0}$ als Zufallszahlen im Intervall $[\,0, 1\,[$ verwenden will, so muß man zuerst sicherstellen, daß die Folge $(x_i)_{i\geq 0}$ eine möglichst lange Periode besitzt. Dies ist eine Aufgabe der Zahlentheorie, und diese Aufgabe wurde in den vorangehenden Abschnitten erledigt. Dann muß man, wie schon erwähnt, die Folge $(x_i/m)_{i\geq 0}$ einer Reihe statistischer Tests unterziehen; von solchen Tests ist in Kiyek-Schwarz [54], Kap. XI, § 7, und ausführlicher in Knuth [55], Abschnitt 3.3, die Rede. Bemerkenswert ist, daß man mit weiteren, nicht statistischen Tests untersuchen kann, ob die Folge $(x_i/m)_{i\geq 0}$ als Folge von Zufallszahlen geeignet ist. Ein wichtiger solcher Test ist der sogenannte Spektraltest, der in Knuth [55], Abschnitt 3.3.4, behandelt ist (man vgl. dazu (8.15), Aufgabe 5); andere Möglichkeiten, mit deren Hilfe man untersuchen kann, ob eine L-Folge zur Erzeugung von Zufallszahlen geeignet ist, beschreibt U. Dieter in [25].

Die mit Hilfe von L-Folgen gewonnenen Zufallszahlen sind für manche Aufgaben, bei denen Zufallszahlen benötigt werden, nicht so recht geeignet, da sie doch ziemlich viele Regelmäßigkeiten besitzen (vgl. (8.6)) und außerdem, jedenfalls bei den in (8.12) und (8.13) aufgeführten Beispielen, die Periodenlänge für manche Anwendungen doch zu klein ist. Es gibt eine Reihe anderer Methoden, Zufallszahlen herzustellen; solche Methoden, von denen viele aus der Zahlentheorie stammen, findet man in Dieter [25], in Kranakis [58], Kap. 4, in Marsaglia [67] und in Niederreiter [74] beschrieben.

(8.15) Aufgaben:

Aufgabe 1: Es sei $m := 2000$, es seien a, b und x^* ganze Zahlen, und es gelte $a \equiv 1 \pmod{20}$ und $\mathrm{ggT}(b, 10) = 1$. Nach (8.9) hat die Periode der durch (m, a, b, x^*) definierte L-Folge $(x_i)_{i\geq 0}$ die Länge 2000. Man sehe sich für verschiedene Werte von a mittels der MuPAD-Funktion `plot2d` die Punktmenge

$$\{(x_i, x_{i+1}) \mid 0 \leq i \leq 1999\}$$

in der Ebene an (etwa für $a = 81$, 181, 281, 381, 1001 und 1021; auf b kommt es nicht weiter an, auf x^* überhaupt nicht).

Aufgabe 2: Die durch $(2^{31}, 2^{16}+3, 0, 1)$ definierte L-Folge $(x_i)_{i\geq 0}$ besitzt nach (8.11) keine Vorperiode, und ihre Periode hat die Länge 2^{29}. Diese Folge wurde

vor Jahren zur Herstellung von Zufallszahlen verwendet, obwohl sie, wie diese Aufgabe zeigt, dafür wenig geeignet ist.

(a) Man zeige: Für jedes $i \in \mathbb{N}_0$ gilt $9x_i - 6x_{i+1} + x_{i+2} \equiv 0 \pmod{2^{31}}$.

(b) Man beweise: Die Punkte der Menge

$$\mathcal{M} := \left\{(x_i, x_{i+1}, x_{i+2}) \mid 0 \le i \le 2^{29} - 1\right\} \subset \mathbb{R}^3$$

liegen auf 15 parallelen Ebenen. Man veranschauliche sich $\mathcal{M}$ mit Hilfe der MuPAD-Funktion `plot3d`.

Aufgabe 3: Diese Aufgabe zeigt an einem einfachen Beispiel eines Monte-Carlo-Verfahrens, wie man mit Hilfe von Zufallszahlen Näherungswerte für Flächen- und Rauminhalte und allgemeiner für bestimmte Integrale ermitteln kann.

(a) Man wähle im Quadrat

$$Q = \left\{(x, y) \in \mathbb{R}^2 \mid 0 \le x, y \le 1\right\}$$

"aufs Geradewohl" viele Punkte und zähle ab, wieviele davon im Viertelkreis

$$\left\{(x, y) \in Q \mid x^2 + y^2 \le 1\right\}$$

liegen. Man gewinne auf diese Weise eine Näherung für die Zahl π.

(b) Man wähle im Würfel

$$W = \left\{(x, y, z) \in \mathbb{R}^3 \mid 0 \le x, y, z \le 1\right\}$$

"aufs Geradewohl" viele Punkte und zähle ab, wieviele davon in der Achtelkugel

$$\left\{(x, y, z) \in W \mid x^2 + y^2 + z^2 \le 1\right\}$$

liegen. Man gewinne auf diese Weise eine Näherung für die Zahl π.

Aufgabe 4 (G. L. L. de Buffon 1777): Man zeichne in der Ebene ein rechtwinkliges Koordinatenkreuz und für jede ganze Zahl i die Parallele

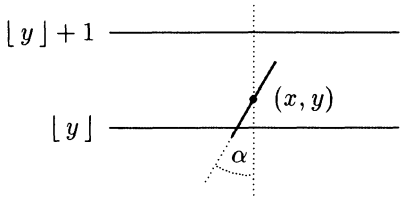
$$g_i := \left\{(x, i) \mid x \in \mathbb{R}\right\}$$

zur waagrechten Achse, werfe immer wieder "aufs Geradewohl" eine Nadel der Länge $a < 1$ auf die Ebene und zähle ab, wie oft sie bei einer größeren Anzahl von Würfen eine der Parallelen g_i, $i \in \mathbb{Z}$, trifft. Ist nach einem Wurf $(x, y) \in \mathbb{R}^2$ das Koordinatenpaar des Mittelpunkts der Nadel, so ist $d := y - \lfloor y \rfloor$ der Abstand des Mittelpunkts der Nadel von der ersten unter ihm liegenden Parallelen, und man kann als Ergebnis des Wurfs das Paar (d, α) betrachten,

wo $\alpha \in [-\pi/2, \pi/2[$ der Winkel ist, den die Richtung der Nadel mit der Richtung der senkrechten Koordinatenachse einschließt; dabei trifft die Nadel die erste unter (x, y) liegende Parallele, genau wenn $d \leq (a/2) \cdot \cos\alpha$ ist, und die erste über (x, y) liegende Parallele, genau wenn $1 - d \leq (a/2) \cdot \cos\alpha$ ist. Die Würfe lassen sich also durch Paare (d, α) repräsentieren, wobei d in $[0, 1[$ und α in $[-\pi/2, \pi/2[$ unabhängig voneinander zufällig gewählt sind. Wie man mittels einer einfachen geometrischen Überlegung zeigt, trifft die Nadel bei einem Wurf eine der Parallelen mit der Wahrscheinlichkeit $2a/\pi$.

(a) Man simuliere mittels Zufallszahlen das Buffonsche Nadelwerfen und gewinne so Schätzwerte für die Zahl π.

(b) Man lese in dem Buch [78] von J. Pfanzagl den Abschnitt 5.1, in dem das Buffonsche Nadelproblem ausführlich behandelt wird.



Aufgabe 5: Man informiere sich in Knuth [55], Abschnitt 3.3.4, über den Spektraltest und programmiere ihn in MuPAD. Man wende diesen Test auf die in (8.12), in (8.13) und in Aufgabe 2 angegebenen L-Folgen an.

9 Ein wenig Kryptologie

(9.1) Der Wunsch, eine Information so zu verschlüsseln, daß sie nur von denen gelesen und verstanden werden kann, die dazu berechtigt sind, ist wohl uralt. Wie der römische Schriftsteller Sueton schreibt, verschlüsselte schon Gaius Julius Caesar Briefe, indem er für einen jeden Buchstaben einen anderen schrieb, etwa A statt D, B statt E und so fort (vgl. [107], Divus Julius 56). Von diesen und anderen in der Antike verwendeten Methoden, militärische und politische Informationen vor den Augen Unbefugter zu verbergen, erzählt auch Aulus Gellius in [41], XVII, 9. Man sieht daran, daß die Kryptologie, also die Lehre vom Verschlüsseln und Entschlüsseln von Informationen, schon in der Antike in militärischen und in politischen Belangen wichtig war. Heute ist die Kryptologie auch im alltäglichen Leben von großer Bedeutung; kein Mensch möchte, daß seine e-mail oder die vielen Informationen, die in allerlei Datenbanken über sein Leben, seine Finanzverhältnisse, seine Krankheiten stehen, von Leuten gelesen werden, die dazu nicht berechtigt sind.

Von den vielen Methoden der Kryptologie soll hier nicht die Rede sein; vielleicht darf an Stelle von Beispielen auf einige berühmte Kriminalgeschichten hingewiesen werden: Arthur Conan Doyle in [27] und [28] und Dorothy Sayers