Eine Bemerkung zur Periodenlängenbestimmung bei einem verallgemeinerten Fibonacci-Generator

Autor(en): **Eichenauer, J. / Lehn, J.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **39 (1984)**

Heft 4

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-38019

ELEMENTE DER MATHEMATIK

Revue de mathématiques élémentaires – Rivista di matematica elementare

Zeitschrift zur Pflege der Mathematik
und zur Förderung des mathematisch-physikalischen Unterrichts

El. Math. Band 39 Nr. 4 Seiten 81–112 Basel, 10. Juli 1984

Eine Bemerkung zur Periodenlängenbestimmung bei einem verallgemeinerten Fibonacci-Generator

Im Zusammenhang mit der Untersuchung mehrfach rekursiver linearer Kongruenzgeneratoren zur Erzeugung von Pseudozufallszahlen ist von Interesse, ob die erzeugten Zahlenfolgen ausreichende Periodenlängen besitzen. Für den besonders einfach gelagerten Spezialfall eines dreifach rekursiven additiven Kongruenzgenerators soll im folgenden eine Methode dargestellt werden, mit der sich schnell und auf elementare Weise überprüfen lässt, ob eine bestimmte, akzeptable Periodenlänge vorliegt.
Sei p eine Primzahl, und seien x_0, x_1, x_2 nichtnegative ganze Zahlen, die kleiner als p sind. Dann heisst die Rekursionsbeziehung

$$x_n \equiv x_{n-1} + x_{n-3} (\mathrm{mod} p), \qquad 0 \leqq x_n < p, \qquad n \geqq 3 \tag{1}$$

verallgemeinerter Fibonacci-Generator. Die durch (1) beschriebene Zahlenfolge $(x_n)_{n \geq 0}$ heisst verallgemeinerte Fibonacci-Folge, das Tripel (x_0, x_1, x_2) Startvektor der Folge und die Primzahl p Modul.
Diese Bezeichnungen erklären sich dadurch, dass die Rekursionsbeziehung

$$x_n \equiv x_{n-1} + x_{n-2} (\mathrm{mod} p), \qquad 0 \leqq x_n < p, \qquad n \geqq 2, \qquad (x_0, x_1) = (0, 1)$$

die Folge der modulo p reduzierten Fibonacci-Zahlen liefert.
Die Untersuchung des dreifach rekursiven additiven Kongruenzgenerators (1) sollte nicht dazu dienen, ihn für die Praxis zu empfehlen, da gegen seine Verwendung Vorbehalte bestehen (siehe z. B. [1], 3.2.2). Ziel war es vielmehr, elementare Untersuchungsmethoden für mehrfach rekursive lineare Kongruenzgeneratoren zu entwickeln.
Der folgende Satz entspricht Theorem 1 in [3]. Der dort angegebene Beweis lässt sich direkt übertragen.

Satz 1. *Eine verallgemeinerte Fibonacci-Folge* $(x_n)_{n \geq 0}$ *ist reinperiodisch, das heisst, es existiert ein Index* $r \geqq 1$ *mit* $(x_0, x_1, x_2) = (x_r, x_{r+1}, x_{r+2})$.

Beweis: Aus der Folge $(x_n)_{n \geq 0}$ lassen sich höchstens p^3 verschiedene Tripel der Form (x_k, x_{k+1}, x_{k+2}) bilden. Es existieren daher Indizes $t > s \geqq 0$, so dass $(x_s, x_{s+1}, x_{s+2}) = (x_t, x_{t+1}, x_{t+2})$ gilt. Durch Umindizieren erhält man aus (1)

$$x_{n-1} \equiv x_{n+2} - x_{n+1} (\mathrm{mod} p), \qquad 0 \leqq x_{n-1} < p, \qquad n \geqq 1.$$

Daraus folgt $x_{s-1} = x_{t-1}, x_{s-2} = x_{t-2}, \ldots, x_0 = x_{t-s}$. Mit $r = t - s \geqq 1$ gilt daher $(x_0, x_1, x_2) = (x_r, x_{r+1}, x_{r+2})$. □

Aufgrund dieses Satzes ist es möglich, die Periodenlänge einer verallgemeinerten Fibonacci-Folge in der folgenden Weise zu definieren. Sie hängt vom Modul p wie auch vom Startvektor (x_0, x_1, x_2) ab und ist gegeben durch

$$\lambda(p; x_0, x_1, x_2) := \min\{k \in \mathbf{N} | (x_0, x_1, x_2) = (x_k, x_{k+1}, x_{k+2})\}. \tag{2}$$

In [2] wird der dreifach rekursive additive Kongruenzgenerator

$$x_n \equiv x_{n-2} + x_{n-3} (\mathrm{mod}\, p), \qquad 0 \leqq x_n < p, \qquad n \geqq 3$$

betrachtet und mit Hinweis auf zahlentheoretische Untersuchungen mitgeteilt, dass die Periodenlänge bei diesem Generator für gewisse Primzahlen p den Wert $p^2 + p + 1$ annimmt, jedoch für keine Primzahl ein grösserer Wert erreicht wird. Bestimmt man z. B. für den Generator (1) mit dem Startvektor $(0, 0, 1)$ und für die 60 kleinsten Primzahlen p die Periodenlänge $\lambda(p; 0, 0, 1)$, so stellt man fest, dass sie ebenfalls stets kleiner oder gleich $p^2 + p + 1$ ist und für 18 der 60 Primzahlen $\lambda(p; 0, 0, 1) = p^2 + p + 1$ gilt. Da man eine grosse Periodenlänge anstrebt und der Wert $p^2 + p + 1$ für praktisch interessierende Primzahlen p bereits als befriedigend angesehen werden kann, stellt sich die Frage, ob bei einem vorgegebenen Modul p für alle Startvektoren $(x_0, x_1, x_2) \neq (0, 0, 0)$ jeweils die Periodenlänge $\lambda(p; x_0, x_1, x_2) = p^2 + p + 1$ auftritt. Wir wollen daher im folgenden eine Methode entwickeln, die dies zu überprüfen gestattet. Nach einer geringen Modifikation lässt sich diese Methode auch für die dreifach rekursiven additiven Kongruenzgeneratoren in [2] verwenden. Auf die Frage nach der Existenz von Primzahlen p, für die sich bei Generatoren der Form (1) Periodenlängen grösser als $p^2 + p + 1$ ergeben, soll hier nicht weiter eingegangen werden.
Zur Vereinfachung der Schreibweise betrachten wir die Matrix

$$A := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

und setzen $x^{(n)} := (x_n, x_{n+1}, x_{n+2})$ für alle $n \geqq 0$, so dass die Rekursionsbeziehung (1) in

$$x^{(n-1)} \cdot A \equiv x^{(n)} (\mathrm{mod}\, p), \qquad 0 \leqq x_{n+2} < p, \qquad n \geqq 1 \tag{3}$$

übergeht, wobei die Modulorechnung wie im folgenden elementweise zu verstehen ist. Die Matrix A nennen wir Generatormatrix. Insbesondere gilt dann

$$x^{(0)} \cdot A^n \equiv x^{(n)} (\mathrm{mod}\, p) \quad \text{für alle} \quad n \geqq 1. \tag{4}$$

Der folgende Satz stellt einen Zusammenhang zwischen der Periodenlänge einer verallgemeinerten Fibonacci-Folge und den Matrizen A^n her.
Im folgenden bezeichnen A stets die Generatormatrix und I die Einheitsmatrix.

Satz 2. *Es gilt*

$$\lambda(p; x_0, x_1, x_2) \geqq \min\{k \in \mathbf{N} | \det(A^k - I) \equiv 0 (\mathrm{mod}\, p)\}$$

für alle Startvektoren $(x_0, x_1, x_2) \neq (0,0,0)$. *Ausserdem existiert ein Startvektor, für den die Gleichheit gilt.*

Beweis: Aus (2) und (4) ergibt sich

$$\begin{aligned}\lambda(p; x_0, x_1, x_2) &= \min\{k \in \mathbf{N} | x^{(0)} = x^{(k)}\} \\ &= \min\{k \in \mathbf{N} | x^{(0)} \equiv x^{(0)} \cdot A^k (\mathrm{mod}\, p)\} \\ &= \min\{k \in \mathbf{N} | x^{(0)} \cdot (A^k - I) \equiv (0,0,0) (\mathrm{mod}\, p)\} \\ &\geqq \min\{k \in \mathbf{N} | \det(A^k - I) \equiv 0 (\mathrm{mod}\, p)\}\end{aligned}$$

für alle Startvektoren $(x_0, x_1, x_2) \neq (0,0,0)$. Die Ungleichung gilt, weil aus $(x_0, x_1, x_2) \cdot (A^k - I) \equiv (0,0,0) (\mathrm{mod}\, p)$ für eine Primzahl p die Kongruenz $\det(A^k - I) \equiv 0 (\mathrm{mod}\, p)$ folgt. Andererseits folgt aus $\det(A^k - I) \equiv 0 (\mathrm{mod}\, p)$, dass ein Startvektor $(x_0, x_1, x_2) \neq (0,0,0)$ mit $(x_0, x_1, x_2) \cdot (A^k - I) \equiv (0,0,0) (\mathrm{mod}\, p)$ existiert. □

Satz 3. *Ist* $k \in \mathbf{N}$ *und* $A^k \equiv I (\mathrm{mod}\, p)$, *dann ist die Periodenlänge* $\lambda(p; x_0, x_1, x_2)$ *ein Teiler von k für alle Startvektoren* $(x_0, x_1, x_2) \neq (0,0,0)$.

Beweis: Aus $A^k \equiv I (\mathrm{mod}\, p)$ folgt mit (4)

$$x^{(k)} \equiv x^{(0)} \cdot A^k \equiv x^{(0)} (\mathrm{mod}\, p).$$

Also ist $\lambda(p; x_0, x_1, x_2) \leqq k$. Für k gibt es dann eine Darstellung mit ganzen Zahlen r und s der Form $k = r \cdot \lambda(p; x_0, x_1, x_2) + s$, wobei $r \geqq 1$ und $0 \leqq s < \lambda(p; x_0, x_1, x_2)$ gilt. Da aus dem Beweis von Satz 2 insbesondere

$$x^{(n)} \cdot A^{\lambda(p; x_0, x_1, x_2)} \equiv x^{(n)} (\mathrm{mod}\, p) \quad \text{für alle} \quad n \geqq 0$$

folgt, ergibt sich

$$x^{(0)} \equiv x^{(k)} \equiv x^{(s)} \cdot A^{r \cdot \lambda(p; x_0, x_1, x_2)} \equiv x^{(s)} (\mathrm{mod}\, p).$$

Also ist $s = 0$. □

Folgerung. *Sei k eine Primzahl mit* $A^k \equiv I (\mathrm{mod}\, p)$. *Dann ist die Periodenlänge* $\lambda(p; x_0, x_1, x_2) = k$ *für alle Startvektoren* $(x_0, x_1, x_2) \neq (0,0,0)$.

Beweis: Da k eine Primzahl ist, gilt nach Satz 3 $\lambda(p; x_0, x_1, x_2) \in \{1, k\}$ für alle Startvektoren $(x_0, x_1, x_2) \neq (0,0,0)$. Aus $\lambda(p; x_0, x_1, x_2) = 1$ ergibt sich mit (1)

$$(x_0, x_1, x_2) \equiv (x_1, x_2, x_3) \equiv (x_1, x_2, x_0 + x_2) (\mathrm{mod}\, p),$$

also $x_0 \equiv x_1 \equiv x_2 \equiv x_0 + x_2 (\mathrm{mod}\, p)$. Daraus folgt $x_0 = x_1 = x_2 = 0$. □

Satz 4. *$k \in \mathbf{N}$ sei keine Primzahl und $t_1, \ldots, t_r$ seien ihre Primteiler. Ist dann $A^k \equiv I \pmod p$ und $\det(A^{(k/t_i)} - I) \not\equiv 0 \pmod p$ für alle $i \in \{1, \ldots, r\}$, so ist die Periodenlänge $\lambda(p; x_0, x_1, x_2) = k$ für alle Startvektoren $(x_0, x_1, x_2) \neq (0,0,0)$.*

Beweis: Wegen Satz 3 genügt es zu zeigen, dass für jeden Startvektor $(x_0, x_1, x_2) \neq (0,0,0)$ und alle $i \in \{1, \ldots, r\}$ die Periodenlänge $\lambda(p; x_0, x_1, x_2)$ kein Teiler von k/t_i ist. Wir nehmen an, dass $\lambda(p; x_0, x_1, x_2) \cdot s = k/t_i$ für $s \in \mathbf{N}$, $i \in \{1, \ldots, r\}$ und $(x_0, x_1, x_2) \neq (0,0,0)$ gilt. Nach dem Beweis von Satz 2 ist dann

$$x^{(0)} \cdot A^{(k/t_i)} \equiv x^{(0)} \cdot A^{\lambda(p; x_0, x_1, x_2) \cdot s} \equiv x^{(0)} \pmod p,$$

woraus man $x^{(0)} \cdot (A^{(k/t_i)} - I) \equiv (0,0,0) \pmod p$ erhält. Dies steht im Widerspruch zur Voraussetzung $\det(A^{(k/t_i)} - I) \not\equiv 0 \pmod p$. □

Dieser Satz und die Folgerung aus Satz 3 bilden die Grundlage für einen Algorithmus, mit dem für eine vorgegebene Primzahl p überprüft werden kann, ob der verallgemeinerte Fibonacci-Generator (1) mit Modul p für alle Startvektoren $(x_0, x_1, x_2) \neq (0,0,0)$ die Periodenlänge $p^2 + p + 1$ besitzt.

Algorithmus. *Seien A die Generatormatrix, I die Einheitsmatrix und p eine Primzahl. Setze $k := p^2 + p + 1$.*

1. Bestimme eine Matrix $B \equiv A^k \pmod p$ und teste, ob $B \equiv I \pmod p$ gilt; falls ja $\rightarrow$2; falls nein $\rightarrow$6.
2. Teste, ob k eine Primzahl ist; falls ja $\rightarrow$7; falls nein $\rightarrow$3.
3. Bestimme die Primteiler $t_1, \ldots, t_r$ von k und setze $i \leftarrow 1$.
4. Bestimme eine Matrix $B_i \equiv A^{(k/t_i)} \pmod p$ und teste, ob $\det(B_i - I) \equiv 0 \pmod p$ gilt; falls ja $\rightarrow$6; falls nein $\rightarrow$5.
5. Setze $i \leftarrow i + 1$ und teste, ob $i > r$ gilt; falls ja $\rightarrow$7; falls nein $\rightarrow$4.
6. Es existiert ein Startvektor $(x_0, x_1, x_2) \neq (0,0,0)$ mit $\lambda(p; x_0, x_1, x_2) \neq k$. Ende.
7. Es gilt $\lambda(p; x_0, x_1, x_2) = k$ für alle Startvektoren $(x_0, x_1, x_2) \neq (0,0,0)$. Ende.

Die grössten Zahlen, die im Rechner exakt dargestellt werden müssen, treten in den Schritten 1 und 4 auf und lassen sich durch $3p^2$ nach oben abschätzen. Schritt 3 ist für grosse Primzahlen p unter Umständen mit sehr grossem Rechenaufwand verbunden. Dagegen ist Schritt 2 auch für sehr grosse Primzahlen mit geeigneten Algorithmen sehr schnell durchzuführen. Hinweise auf solche Algorithmen findet man in [1], vol. II, ch. 4.

J. Eichenauer und J. Lehn
Technische Hochschule Darmstadt

LITERATURVERZEICHNIS

1 D.E. Knuth: The Art of Computer Programming, Vol. 2. Addison-Wesley, Reading, 2nd ed., 1981.
2 J.C.P. Miller und M.J. Prentice: Additive congruential pseudo-random number generators. Computer J. *11*, 341–346 (1968).
3 D.D. Wall: Fibonacci series modulo *m*. Am. Math. Monthly *67*, 525–532 (1960).

 0013-6018/84/040081-04$1.50 + 0.20/0