**Zeitschrift:** Elemente der Mathematik
**Herausgeber:** Schweizerische Mathematische Gesellschaft
**Band:** 74 (2019)
**Heft:** 3

**Artikel:** Magische Eigenschaften linearer Rekursionen
**Autor:** Strasser, Nina / Weng, Annegret
**DOI:** https://doi.org/10.5169/seals-869237

Elem. Math. 74 (2019) 104 – 113
0013-6018/19/030104-10
DOI 10.4171/EM/388



Elemente der Mathematik

# Magische Eigenschaften linearer Rekursionen

Nina Strasser und Annegret Weng

Nina Strasser studierte an der Hochschule für Technik in Stuttgart und schloss 2017 mit dem Master in Mathematik ab. Seitdem ist sie bei der Württembergischen Versicherung beschäftigt.

Annegret Weng promovierte 2001 an der Universität Duisburg-Essen über ein zahlentheoretisches Thema mit Anwendung in der Kryptographie. Nach ihrer beruflichen Praxis bei verschiedenen Versicherungsunternehmen wurde sie 2012 auf eine Professur im Studiengang Mathematik an der Hochschule für Technik berufen.

## 1 Einleitung

Wir betrachten den folgenden Zaubertrick (vgl. auch Kapitel 9 in [1] und in leichter Modifikation Kapitel 10 in [3]): Der Zauberer schreibt eine Vorhersage auf ein Blatt Papier. Dann bittet er den Zuschauer, zwei beliebige Zahlen $u$ und $v \in \{0, \ldots, 6\}$, $(u, v) \neq (0, 0)$

Wer sich mit mathematischen Zaubertricks beschäftigt, weiß, dass es Tricks gibt, die auf interessanten nicht-trivialen mathematischen Phänomenen beruhen. So lässt sich beispielsweise eine magische Eigenschaft der Fibonacci-Folge publikumswirksam einsetzen: Der Zauberer schreibt eine Vorhersage auf ein Blatt, das er einem Zuschauer zur Aufbewahrung gibt. Anschließend lässt er einen weiteren Zuschauer zwei beliebige Zahlen $u$, $v$ zwischen 0 und 6 (mindestens eine sollte von 0 verschieden sein) wählen. Mit Unterstützung des Publikums werden nun die ersten sechzehn Glieder der Folge $g_0 = u$, $g_1 = v$ und $g_n = g_{n-1} + g_{n-2} \mod 7$ ermittelt und deren Summe berechnet. Es zeigt sich, dass der Zauberer die Summe – in diesem Fall die Zahl 49 – korrekt prognostiziert hat. Die Arithmetik solcher Zaubertricks wurde von Ehrhard Behrends in einer Arbeit untersucht, die im Heft 4/2014 dieser Zeitschrift erschienen ist. Die Autorinnen der vorliegenden Arbeit beschreiben eine Verallgemeinerung, die es beispielsweise auch erlaubt, das Alter eines 50jährigen Geburtstagskindes zu forcieren. Dabei entpuppt sich der Zaubertrick als schöne Anwendung von Resultaten der linearen Algebra über endlichen Körpern.

zu wählen, die Folge

$$g_0 = u,\ g_1 = v,\ g_{n+2} = \begin{cases} g_n + g_{n+1} & \text{falls } g_n + g_{n+1} \leq 6, \\ g_n + g_{n+1} - 7 & \text{sonst,} \end{cases}$$

für $n = 0, \ldots, 13$ und die Summe $s_7 = \sum_{i=0}^{15} g_i$ zu berechnen. Obwohl der Zuschauer bei den Startwerten $u$ und $v$ freie Wahl hatte, stimmt das Ergebnis $s_7 = 49$ mit der Vorhersage des Zauberers überein.

Der Trick verwendet Eigenschaften der Primzahl $p = 7$. Für einen Mathematiker ist es natürlich zu fragen, welche Primzahlen eine ähnliche Eigenschaft aufweisen, die es erlaubt, die Summe einer Fibonacci-artigen Sequenz vorgegebener Länge vorherzusagen. Diese Frage wurde bereits von Behrends (siehe [1] oder [2]) untersucht. So funktioniert der Trick auch mit $p = 23, 43, 67, 83, \ldots$. Wenn wir die Summe über die ersten $2 \cdot p + 2$ Folgenglieder berechnen, erhalten wir für diese Primzahlen stets $s_p = p^2$ unabhängig von den Startwerten $u, v \in \{0, \ldots, p-1\}$, $(u, v) \neq (0, 0)$.

In unserem Beitrag werden wir die Ergebnisse weiter verallgemeinern. Dazu betrachten wir $(a, b)$-Fibonacci-Folgen (auch unter dem Begriff „Lucas-Folgen“ bekannt, siehe [8], Kapitel 2, Abschnitt IV). Durch diese Verallgemeinerung können wir andere Primzahlen $p$ verwenden und andere Werte für $s_p$ realisieren.

Dabei setzen wir nur bekannte Resultate über Eigenwerte und -vektoren bzw. über die Diagonalisierung von Matrizen aus der Linearen Algebra und Eigenschaften endlicher Körper voraus, wie sie in einer einführenden Vorlesung zur elementaren Zahlentheorie vermittelt werden.

## 2 Ergebnisse für $(a, b)$-Fibonacci-Folgen

Wir starten mit der Definition einer $(a, b)$-Fibonacci-Folge.

**Definition 2.1.** Es seien $a, b \in \mathbb{Z}$, $u, v \in \mathbb{N}_0$ mit $a^2 + 4b \neq 0$ und $(u, v) \neq (0, 0)$ gegeben. Die Folge definiert durch $f_0 = u$, $f_1 = v$ und

$$f_n = a \cdot f_{n-1} + b \cdot f_{n-2} \text{ für } n \geq 2$$

heißt $(a, b)$-Fibonacci-Folge.

In der Literatur sind $(a, b)$-Fibonacci-Folgen auch unter dem Begriff „Lucas-Folgen“ bekannt. P. Ribenboim behandelt Lucas-Folgen ausführlich in [8], Kapitel 2, Abschnitt IV.

Für die ursprüngliche Fibonacci-Folge gilt $a = b = 1$ und $u = 0$, $v = 1$.

Dreh- und Angelpunkt unserer weiteren Argumentation ist die folgende Matrixdarstellung.

**Lemma 2.2.** *Betrachte die Matrix* $A = \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}$ *mit* $a^2 + 4b \neq 0$.

1. *Dann gilt* $A \cdot (f_{n-2}, f_{n-1})^T = (f_{n-1}, f_n)^T$. *Folglich haben wir*

$$A^n \cdot (f_0, f_1)^T = (f_n, f_{n+1})^T.$$

2. *Das charakteristische Polynom von A is* $p_A(x) = x^2 - ax - b$. *Es hat zwei verschiedene Nullstellen in* $\mathbb{C}$, *und* $A^n$ *lässt sich in der Form*

$$A^n = S^{-1} \cdot \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \cdot S \tag{1}$$

*für eine invertierbare Matrix S mit Einträgen in* $\mathbb{C}$ *schreiben.*

*Wenn die Diskriminante* $a^2 + 4b$ *des charakteristischen Polynoms positiv ist, dann liegen* $\lambda_1, \lambda_2$ *in* $\mathbb{R}$ *und es existiert bereits eine Diagonalisierung über den reellen Zahlen.*

*Beweis.* Die erste Eigenschaft können wir einfach durch Induktion zeigen. Für die zweite Behauptung verwenden wir, dass die Diskriminante $a^2 + 4b$ des Polynoms $p_A(x)$ von 0 verschieden ist und dass sich Matrizen mit paarweise verschiedenen Eigenwerten diagonalisieren lassen. □

Im Folgenden betrachten wir nun $(a, b)$-Fibonacci-Folgen modulo einer Primzahl $p$. Es sei $g_i \in \{0, \ldots, p-1\}$ der Rest von $f_i$ bei Division mit $p$. Weiter beschränken wir uns auf Primzahlen mit der folgenden Eigenschaft:

$$p \text{ ist ungerade, } p \text{ teilt weder } a, b \text{ noch } a^2 + 4b \text{ (kurz: } 2 \nmid p,\ p \nmid a, b, a^2 + 4b).$$

Damit werden für eine vorgegebene $(a, b)$-Fibonacci-Folge nur endlich viele Primzahlen ausgeschlossen.

Auch über endlichen Körpern lässt sich eine Diagonalisierung der Matrix $\overline{A} := A \mod p$ wie in Lemma 2.2 erreichen. Dazu betrachten wir in Analogie zu $\mathbb{R}$ und $\mathbb{C}$ die endlichen Körper $\mathbb{F}_p$ und $\mathbb{F}_{p^2}$ mit $p$ bzw. $p^2$ Elementen. Wie für $\mathbb{R}$ unterscheiden wir zwei Fälle:

1. Wenn die Diskriminante $a^2 + 4b$ ein Quadrat modulo $p$ ist, dann hat das charakteristische Polynom $p_A(x) = x^2 - ax - b$ zwei Nullstellen in $\mathbb{F}_p$. Diese sind voneinander verschieden, weil wir $p \nmid a^2 + 4b$ gefordert haben.
2. Im anderen Fall ist $a^2 + 4b$ kein Quadrat modulo $p$ und das Polynom $p_A(x)$ ist über $\mathbb{F}_p$ irreduzibel. Analog zur Konstruktion der komplexen Zahlen durch Adjunktion der Nullstelle des über $\mathbb{R}$ irreduziblen Polynoms $x^2 + 1$ können wir nun den Körper $\mathbb{F}_{p^2}$ definieren, in dem jedes Polynom mit Koeffizienten über $\mathbb{F}_p$ vom Grad 2 zwei Nullstellen $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2}$ besitzt.

Die Folgenglieder einer $(a, b)$-Fibonacci-Folge nehmen modulo $p$ nur endlich viele Werte an. Somit ist die Folge stets periodisch. Im Folgenden betrachten wir die kleinste natürliche Zahl $\gamma$ mit $\overline{A}^\gamma = E$ über $\mathbb{F}_p$. Die Zahl $\gamma$ bestimmt, über wie viele Werte für den Zaubertrick summiert wird. In vielen Fällen ist sie gleich der Periodenlänge. Auf die Ausnahmen werden wir noch in Bemerkung 2.4.1 eingehen. In jedem Fall teilt die Periodenlänge die Zahl $\gamma$.

Das Resultat des nächsten Lemmas ist bereits bekannt (siehe z.B. [7], Theorem 3 oder [5], Abschnitt 3). Mit den oben beschriebenen Grundlagen zu endlichen Körpern können wir einen kurzen Beweis geben.

**Lemma 2.3.**

1. *Falls* $a^2 + 4b$ *ein Quadrat modulo* $p$ *ist, folgt* $\gamma \mid p - 1$.
2. *Es sei* $\operatorname{ord}_p(-b)$ *die Ordnung von* $-b$ *in* $\mathbb{F}_p$. *Falls* $a^2 + 4b$ *kein Quadrat modulo* $p$ *ist, ergibt sich* $\gamma \mid \operatorname{ord}_p(-b) \cdot (p+1)$.

*Beweis.* Wir betrachten die Matrix $\overline{A} := A \mod p$.
1. Falls $a^2+4b$ ein Quadrat in $\mathbb{F}_p$ ist, hat das charakteristische Polynom von $\overline{A}$ genau zwei verschiedene Nullstellen $\lambda_1, \lambda_2 \in \mathbb{F}_p$. Die Matrix $\overline{A}$ lässt sich über $\mathbb{F}_p$ in der Form

$$\overline{A} = \overline{S}^{-1} \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \cdot \overline{S} \tag{2}$$

für $\lambda_1, \lambda_2 \in \mathbb{F}_p$ und eine invertierbare Matrix $\overline{S}$ mit Koeffizienten in $\mathbb{F}_p$ schreiben. Aus dem kleinen Satz von Fermat folgt nun $\lambda_i^{p-1} \equiv 1 \mod p$ und somit ist $\overline{A}^{p-1}$ die Einheitsmatrix $E$. Da $\gamma$ die kleinste Zahl mit $\overline{A}^{\gamma} = E$ ist, folgt $\gamma \mid p - 1$.

2. Falls $x^2 - ax - b$ über $\mathbb{F}_p$ irreduzibel ist, hat das Polynom zwei Nullstellen $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2}$. In Analogie zur komplexen Konjugation gibt es bei endlichen Körpern den Frobenius-Automorphismus gegeben durch $\lambda \mapsto \lambda^p$. Die beiden Nullstellen sind zueinander konjugiert, das bedeutet, $\lambda_2 = \lambda_1^p$ (vgl. auch Abschnitt 11 in [4]). Aus der Zerlegung $x^2 - ax - b = (x - \lambda_1)(x - \lambda_1^p)$ in $\mathbb{F}_{p^2}$ folgt

$$\lambda_1^{p+1} = \lambda_1 \lambda_2 = -b \text{ in } \mathbb{F}_{p^2} \text{ bzw. } \lambda_1^{\operatorname{ord}_p(-b)(p+1)} \equiv 1 \mod p.$$

Somit ist $\overline{A}^{\operatorname{ord}_p(-b)(p+1)}$ die Einheitsmatrix. □

Offensichtlich ist für $\gamma$ nur eine Teilbarkeitsaussage möglich, da selbst für die Ordnungen von Elementen in $\mathbb{F}_p$ keine geschlossenen Formeln existieren.

**Bemerkung 2.4.**

1. Es kann Startwerte $u$ und $v$ geben, für die die $(a, b)$-Fibonacci-Folge eine Periodenlänge kleiner als $\gamma$ hat. Wenn das charakteristische Polynom bereits über $\mathbb{F}_p$ zerfällt und die Eigenwerte $\lambda_1$ und $\lambda_2$ in $\mathbb{F}_p$ unterschiedliche Ordnung haben, definieren die Einträge der zugehörigen Eigenvektoren Startwerte, die zu unterschiedlich langen Perioden führen.
   Als Beispiel betrachten wir die Folge mit $a = b = 1$ für die Primzahl $p = 11$. Ein Eigenwert ist $\lambda_1 = 4$ mit $\operatorname{ord}_p(\lambda_1) = 5$ und zugehörigem Eigenvektor $(1, 4)^T$. Die Startwerte $u = 1$ und $v = 4$ definieren eine Folge der Periodenlänge 5. Der zweite Eigenwert ist $\lambda_2 = 8$ mit $\operatorname{ord}_p(\lambda_2) = 10$ und zugehörigem Eigenvektor $(1, 8)^T$. Die Folge beginnend mit $u = 1$ und $v = 8$ hat Periodenlänge 10.
2. Falls das charakteristische Polynom jedoch über $\mathbb{F}_p$ irreduzibel ist, ist die Periodenlänge immer von $u$ und $v$ unabhängig und damit immer gleich $\gamma$: Die Konjugation $\lambda \mapsto \lambda^p$ ist wegen $(\lambda^p)^p = \lambda$ eine bijektive Abbildung (sogar ein Körperautomorphismus). Somit haben beide Eigenwerte die gleiche Ordnung in $\mathbb{F}_{p^2}$ und der oben beschriebene Fall kann hier nicht auftreten.

3. Für den Spezialfall $a = b = 1$ ist $\gamma$ immer gerade (siehe [1], Proposition 2). Dies ist für allgemeine $a, b$ nicht zwingend. Beispielsweise ergibt sich für $a = 1, b = 3$ und $p = 37$ der Wert $\gamma = 171$.

Analog zu [1] nennen wir eine Primzahl $p$ nun eine „gute Primzahl", falls $\gamma$ gerade ist und außerdem $\overline{A}^{\gamma/2} = -E$ gilt.

**Lemma 2.5.**

1. *Falls das charakteristische Polynom modulo $p$ irreduzibel und $\gamma$ gerade ist, ist $p$ eine gute Primzahl.*
2. *Falls das charakteristische Polynom modulo $p$ zerfällt und zudem $-b$ kein Quadrat modulo $p$ ist, kann $p$ keine gute Primzahl sein.*
3. *Wenn das charakteristische Polynom modulo $p$ zerfällt, $-b$ ein Quadrat modulo $p$ ist und $\gamma = p - 1$ gilt, ist $p$ eine gute Primzahl.*

*Beweis.* Wir betrachten wieder die Diagonalisierung von $\overline{A}$, d.h. die Darstellung

$$\overline{A} = \overline{S}^{-1} \cdot \overline{D} \cdot \overline{S} = \overline{S}^{-1} \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \cdot \overline{S} \tag{3}$$

mit $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2}$. Es gilt $\overline{A}^{\gamma/2} = -E$ genau dann, wenn $\overline{D}^{\gamma/2} = -E$.

Falls $\gamma$ gerade ist, haben wir stets $\lambda_i^{\gamma/2} = \pm 1$. Da $\gamma$ minimal mit der Eigenschaft $\overline{A}^{\gamma} = E$, kann nicht $\lambda_1^{\gamma/2} = \lambda_2^{\gamma/2} = 1$ gelten. Somit folgt $\lambda_i^{\gamma/2} = -1$ für mindestens ein $i$. Eine Primzahl $p$ ist genau dann eine gute Primzahl, wenn $\lambda_1 = \lambda_2 = -1$ gilt.

Falls das charakteristische Polynom modulo $p$ irreduzibel ist, haben die beiden Nullstellen $\lambda_1, \lambda_2$ die gleiche Ordnung in $\mathbb{F}_{p^2}$ (siehe auch Bemerkung 2.4.2). Daraus folgt die erste Behauptung.

Wir betrachten nun den Fall, dass das charakteristische Polynom zwei Nullstellen $\lambda_1, \lambda_2 \in \mathbb{F}_p$ hat und $\lambda_1^{\gamma/2} = \lambda_2^{\gamma/2} = -1$ gilt. Nach Lemma 2.3 gibt es ein $k \in \mathbb{N}$ mit $k \cdot \gamma = p-1$. Da $\lambda_1 \cdot \lambda_2 \equiv -b \mod p$ ist, ergibt sich $(-b)^{(p-1)/2} \equiv (-b)^{\gamma/2 \cdot k} \equiv \left((\lambda_1 \cdot \lambda_2)^{\gamma/2}\right)^k \equiv 1^k \equiv 1 \mod p$. Nach dem Euler-Kriterium ist eine Zahl $a \in \mathbb{F}_p$ genau dann ein Quadrat modulo $p$, falls $a^{\frac{p-1}{2}} \equiv 1 \mod p$ gilt (vgl. auch [6], Satz 8.5.2). Somit kann es keine gute Primzahl $p$ geben, für die das charakteristische Polynom zerfällt und $-b$ kein Quadrat modulo $p$ ist.

Sei nun $p$ eine Primzahl, für die das Polynom $x^2 - ax - b$ mindestens eine Nullstelle $\lambda_i \in \mathbb{F}_p$ der Ordnung $\gamma = p - 1$ hat und für die $(-b)^{(p-1)/2} \equiv 1 \mod p$ gilt. Ohne Beschränkung der Allgemeinheit gelte $\mathrm{ord}_p(\lambda_1) = p - 1$, also insbesondere $\lambda_1^{(p-1)/2} \equiv -1 \mod p$. Aus $1 \equiv (-b)^{(p-1)/2} \equiv \lambda_1^{(p-1)/2} \cdot \lambda_2^{(p-1)/2} \mod p$ folgt $\lambda_2^{(p-1)/2} = -1$ bzw. $\overline{A}^{(p-1)/2} = -E$. □

Der Beweis des nächsten Satzes benötigt die Werte $a$ und $b$ nicht und unterscheidet sich somit nicht vom Beweis der Proposition 3.1 in [1].

**Satz 2.6.** *Sei $p$ eine gute Primzahl und sei $\nu$ die Anzahl der Nullen in der Folge $g_0, g_1, \ldots, g_{\gamma-1}$. Dann folgt*

$$g_0 + \cdots + g_{\gamma-1} = p \cdot (\gamma/2 - \nu/2).$$

Da der Satz zum Verständnis des Zaubertricks von zentraler Bedeutung ist, skizzieren wir kurz die Beweisidee: Für eine gute Primzahl $p$ gilt $\overline{A}^{\gamma/2} = -E$. Zusammen mit der Aussage 1. in Lemma 2.2, die ebenso für endliche Körper gilt, folgt

- für $g_i, g_{\gamma/2+i} \neq 0$, dass $g_{\gamma/2+i} = p - g_i$ bzw. $g_i + g_{\gamma/2+i} = p$ und
- für $g_i = 0$ auch $g_{\gamma/2+i} = 0$, also $g_i + g_{\gamma/2+i} = 0$.

Wir können die Summe $g_0 + \cdots + g_{\gamma-1}$ dann in der Form $(g_0 + g_{\gamma/2}) + (g_1 + g_{\gamma/2+1}) + \cdots$ schreiben. Diese Summe enthält $\nu/2$ Summanden, die gleich 0 sind, und $\gamma/2 - \nu/2$ Summanden, die den Wert $p$ annehmen.

Wenn wir nun an den Zaubertrick zu Beginn denken, dann suchen wir gute Primzahlen, für die die Anzahl $\nu$ der Nullen in der Menge $\{g_0, \ldots, g_{\gamma-1}\}$ nicht von den Anfangswerten $g_0 = u$ und $g_1 = v$ abhängt. Solche Primzahlen nennen wir analog zu [1] sehr gute Primzahlen.

**Lemma 2.7.** *Sei $p$ eine sehr gute Primzahl. Dann gilt $(p+1) \cdot \nu = \gamma$. Insbesondere teilt $p+1$ die Zahl $\gamma$.*

*Beweis.* Wir definieren eine Äquivalenzrelation $\sim_R$ auf $\mathbb{F}_p \times \mathbb{F}_p \setminus \{(0,0)\}$: Es gilt $(x, y) \sim_R (x', y')$ genau dann, wenn es ein $k \in \mathbb{N}$ gibt mit $\overline{A}^k (x, y)^T = (x', y')^T$. Dies ist genau dann der Fall, wenn $x', y'$ zwei aufeinanderfolgende Folgenglieder in der $(a, b)$-Fibonacci-Folge modulo $p$ mit Anfangswerten $u = x, v = y$ sind. Die Größe einer Äquivalenzklasse entspricht gerade der jeweiligen Periodenlänge. Wir identifizieren die Nullen in einer Folge mit den Tupeln $\{0\} \times \mathbb{F}_p^* := \{0\} \times \mathbb{F}_p \setminus \{(0,0)\}$. Diese Menge hat $p-1$ Elemente.

Wir zeigen zunächst, dass für eine gute Primzahl $p$ alle Äquivalenzklassen die gleiche Ordnung haben müssen: Unterschiedliche Ordnungen sind nach Bemerkung 2.4.2 nur möglich, wenn das charakteristische Polynom über $\mathbb{F}_p$ zerfällt und somit nach Lemma 2.3 $\gamma \mid p-1$ gilt. Wegen $\gamma \cdot (p-1) \leq (p-1)^2 < p^2 - 1$ gibt es in diesem Fall mehr als $p-1$ Äquivalenzklassen und deshalb auch solche, die keine Null enthalten.

Wenn alle Äquivalenzklassen die gleiche Länge $\gamma$ haben, ist die Anzahl der Äquivalenzklassen durch $\frac{p^2-1}{\gamma}$ gegeben. Wenn nun alle Äquivalenzklassen $\nu$ Nullen enthalten, ergibt sich

$$\frac{p^2-1}{\gamma} \cdot \nu = p - 1. \qquad \square$$

Der Beweis zu Lemma 2.7 zeigt insbesondere, dass für jede sehr gute Primzahl $p$ das Polynom $x^2 - ax - b$ über $\mathbb{F}_p$ irreduzibel sein muss.

Wir betrachten jetzt die Anzahl der Nullen in einem Periodenzyklus für den speziellen Fall mit Startwerten $u = 0$ und $v = 1$. Das Ergebnis des folgenden Lemmas findet sich in einer etwas anderen Darstellung und von hier abweichendem Beweis auch in [7], Theorem 4 und [5], Abschnitt 3.

**Lemma 2.8.** *Sei $p$ eine Primzahl mit $p+1 \mid \gamma$. Wir betrachten den Spezialfall $u = 0$ und $v = 1$. Dann ist die Ordnung der Menge $\{g_k : 0 \leq k \leq \gamma - 1, g_k = 0\}$ gleich*

$$\nu = \begin{cases} \operatorname{ord}_p(-b), & \text{falls } -b \text{ kein Quadrat in } \mathbb{F}_p \text{ ist und} \\ 2 \cdot \operatorname{ord}_p(-b), & \text{falls } -b \text{ ein Quadrat in } \mathbb{F}_p \text{ ist.} \end{cases}$$

*Beweis.* Aus $\overline{A}^{p+1} = -bE$ in $\mathbb{F}_p$ folgt $g_p = 0$. Sei $m > 0$ die kleinste natürliche Zahl mit $g_m = 0$. Dann ergibt sich $\overline{A}^m \cdot (0,1)^T = (0, g_{m+1})^T$, also ist $g_{m+1} \in \mathbb{F}_p$ ein Eigenwert von $\overline{A}_m$ und es gilt $\lambda_1^m = \lambda_2^m = g_{m+1} \in \mathbb{F}_p$.

Sei $n = \operatorname{ggT}(p+1, m)$. Mit dem erweiterten Euklidischen Algorithmus können wir $n = n_1 \cdot (p+1) + n_2 \cdot m$ für geeignete $n_1, n_2 \in \mathbb{Z}$ schreiben und erhalten $\lambda_1^n \in \mathbb{F}_p$. Aus der Minimalität von $m$ folgern wir $m = \operatorname{ggT}(p+1, m)$ bzw. $m \mid p+1$.

Aus dem kleinen Satz von Fermat erhalten wir $\lambda_i^{m \cdot (p-1)} = 1$ und wegen $p+1 \mid \gamma$ muss $p+1$ die Zahl $m \cdot (p-1)$ teilen. Dies ist nur für $m = (p+1)/2$ oder $m = p+1$ möglich. Es gilt $m = (p+1)/2$ genau dann, wenn $\lambda_i^{p+1}$ ein Quadrat modulo $p$ ist. Die Menge $\{g_k : 0 \leq k \leq \gamma - 1, g_k = 0\}$ hat somit $\gamma / m = \operatorname{ord}_p(-b)$ Elemente, falls $-b$ kein Quadrat ist, und sonst $\gamma / m = 2 \cdot \operatorname{ord}_p(-b)$ Elemente. □

Damit können wir jetzt die Primzahlen $p$ für unseren Zaubertrick charakterisieren.

**Lemma 2.9.** *Eine gute Primzahl $p$, für die das charakteristische Polynom $x^2 - ax - b$ über $\mathbb{F}_p$ irreduzibel ist, ist eine sehr gute Primzahl genau dann, wenn die Periodenlänge gleich $\operatorname{ord}_p(-b) \cdot (p+1)$ ist und $-b$ kein Quadrat in $\mathbb{F}_p$ ist.*

*Beweis.* Betrachte ein Element $(0, v)^T$ in $\{0\} \times \mathbb{F}_p^*$, das nicht in der Bahn von $(0,1)^T$ unter der Operation von $\overline{A}$ enthalten ist. Wir nehmen an, dass

$$\overline{A}^m \cdot (0, v)^T = (0, v')^T.$$

Dann folgt

$$\overline{A}^m \cdot (0,1)^T = (0, v' \cdot v^{-1})^T.$$

Somit gibt es eine 1-1 Beziehung zwischen Nullen in der Folge mit Startwerten $u = 0$ und $v = 1$ und den Nullen in Folgen mit beliebigen Startwerten, die mindestens eine Null enthalten.

Falls $p$ eine Primzahl maximaler Ordnung ist, die die Voraussetzungen des Lemmas erfüllt, gibt es $(p-1)/\operatorname{ord}_p(-b)$ verschiedene Bahnen und nach Lemma 2.8 enthält die Folge $u = 0$ und $v = 1$ in diesem Fall $\operatorname{ord}_p(-b)$ Nullen. Durch einfaches Abzählen sehen wir, dass $p$ eine sehr gute Primzahl ist.

Wenn $p$ eine sehr gute Primzahl ist, dann gilt nach Lemma 2.7, dass $\gamma = \nu \cdot (p+1)$, und nach Lemma 2.8, dass $\nu = \operatorname{ord}_p(-b)$ oder $\nu = 2 \cdot \operatorname{ord}_p(-b)$. Da $\gamma \mid \operatorname{ord}_p(-b) \cdot (p+1)$, folgern wir $\nu = \operatorname{ord}_p(-b)$. Somit muss $p$ eine Primzahl maximaler Ordnung sein und $-b$ ist kein Quadrat modulo $p$. □

**Bemerkung 2.10.** Wir erinnern daran, dass das charakteristische Polynom genau dann modulo $p$ irreduzibel ist, wenn $a^2 + 4b$ kein Quadrat in $\mathbb{F}_p$ ist. Eine Primzahl $p$ ist somit eine sehr gute Primzahl genau dann, wenn $a^2 + 4b$ und $-b$ keine Quadrate in $\mathbb{F}_p$ sind und $\gamma = \mathrm{ord}_p(-b) \cdot (p+1)$ ist. Nach Eulers Kriterium muss in diesem Fall $\left(a^2+4b\right)^{\frac{p-1}{2}} \equiv (-b)^{\frac{p-1}{2}} \equiv -1 \mod p$ gelten.

In nächsten Abschnitt werden wir explizite Beispiele für gute und sehr gute Primzahlen geben.

## 3 Beispiele und Anwendungen

Unsere Verallgemeinerung erlaubt es, den Trick auf weitere Primzahlen $p$ anzuwenden und damit mehr Werte $s_p$ abzudecken. Bereits in [1] finden wir die folgende Modifikation: Wenn wir die Folge $g'_i$ definiert durch

$$g'_0 = a, g'_1 = b, g'_{n+2} = \begin{cases} g'_n + g'_{n+1} & \text{falls } g'_n + g'_{n+1} \leq p \\ g'_n + g'_{n+1} - p & \text{sonst} \end{cases}$$

mit $u, v \in \{1, \ldots, p\}$, $(u, v) \neq (p, p)$ betrachten, können wir statt $s_p = p^2$ die Summe $s'_p = p^2 + 2p$ erzeugen. Der Fibonacci-Trick kann damit zum Beispiel mit $p = 7$ auf einem 49. oder 63. Geburtstag präsentiert werden.

Mit $(a, b)$-Fibonacci-Folgen sind weitere Werte möglich. Aus Satz 2.6 und Lemma 2.9 können wir leicht das folgende Lemma ableiten.

**Lemma 3.1.** *Für eine $(a, b)$-Fibonacci-Folge und eine sehr gute Primzahl $p$ gilt*

$$s_p = \frac{1}{2} \cdot \mathrm{ord}_p(-b) \cdot p^2 \text{ und } s'_p = \frac{1}{2} \cdot \mathrm{ord}_p(-b) \cdot p^2 + \mathrm{ord}_p(-b) \cdot p.$$

Man beachte, dass für eine sehr gute Primzahl $-b$ kein quadratischer Rest modulo $p$ ist (vgl. Lemma 2.9). Somit ist $\mathrm{ord}_p(-b)$ stets gerade.

In Tabelle 1 auf S. 112 geben wir für kleine Primzahlen $p$ $(a, b)$-Fibonacci-Folgen an, für die diese sehr gute Primzahlen sind, zusammen mit der Periode $\gamma$ und den Summenwerten $s_p$ bzw. $s'_p$.

Über die praktische Anwendbarkeit in der Zauberkunst lässt sich diskutieren. Sicher ist die Addition von 168 Zahlen dem Zuschauer nicht zuzumuten. Wenn der Zauberer das Publikum einbindet, erst einmal selbst einige Folgenglieder vorrechnet und sich dann vom Auditorium die restlichen Zahlen im Chor zurufen lässt (damit es nicht so langweilig wird), sind 24 Werte vielleicht noch machbar. In diesem Fall können neben den bekannten Zahlen 9, 15, 49 und 63 noch die runden Geburtstage 50 und 70 produziert werden. Mit der Primzahl 11 lässt sich in 24 Runden auch das Datum 12. Januar oder 14. März forcieren.

Interessanter, weil sie auf geringere Periodenlänge führen, sind Primzahlen, die zwei mögliche Summenwerte generieren. Stellen wir uns beispielsweise ein Hochzeitspaar vor, das 33 und 44 Jahre alt ist. Mit $p = 11$ und $(a, b) = (1, 10)$ erhalten wir $\gamma = 6$ und die beiden

| Primzahl $p$ | für $(a, b)$ | $\gamma$ | $s_p$ | $s'_p$ |
|---|---|---|---|---|
| 3 | $(1, 1)$ | 8 | 9 | 15 |
| 5 | $(3, 2)$ | 24 | 50 | 70 |
| 7 | $(1, 1)$ | 16 | 49 | 63 |
| | $(3, 2)$ | 48 | 147 | 189 |
| 11 | $(2, 1)$ | 24 | 121 | 143 |
| | $(1, 3)$ | 120 | 605 | 715 |
| 13 | $(1, 5)$ | 56 | 338 | 390 |
| | $(4, 2)$ | 168 | 1014 | 1170 |

Tabelle 1 Beispiele für $(a, b)$-Fibonacci-Folgen, für die $p \leq 13$ eine sehr gute Primzahl ist, die Periodenlänge $\gamma$ und die Werte $s_p$ und $s'_p$

möglichen Ordnungen $s'_p = 33$ und 44. Die Folge lässt sich statt $g_n \equiv g_{n-1} + 10 \cdot g_{n-2}$ mod 11 auch durch die Vorschrift $g_n \equiv g_{n-1} - g_{n-2} \mod 11$ erzeugen, da $(1, 10) \equiv (1, -1) \mod 11$. Eine der beiden Summen können wir nun durch beliebige Wahl der Anfangswerte von einem Zuschauer forcieren. Dann geben wir selbst Anfangswerte vor, die auf die zweite Summe führen und lassen die Folge ein zweites Mal durchrechnen.

Tabelle 2 gibt interessante Zahlenpaare für Hochzeiten, gemeinsame Geburtstage oder goldene Hochzeiten an.

| Primzahl $p$ | für $(a, b)$ | $\gamma$ | $s_p$ | $s'_p$ |
|---|---|---|---|---|
| 5 | $(1, 4)$ | 6 | $(10, 15)$ | $(20, 15)$ |
| | $(2, 1)$ | 12 | $(20, 30)$ | $(40, 30)$ |
| 7 | $(1, 3)$ | 24 | $(63, 84)$ | $(105, 84)$ |
| | $(1, 6)$ | 6 | $(14, 21)$ | $(28, 21)$ |
| | $(3, 6)$ | 8 | $(21, 28)$ | $(35, 28)$ |
| 11 | $(2, 2)$ | 10 | $(44, 55)$ | $(66, 55)$ |
| | $(3, 1)$ | 8 | $(33, 44)$ | $(55, 44)$ |
| | $(1, 10)$ | 6 | $(22, 33)$ | $(44, 33)$ |
| | $(5, 10)$ | 12 | $(55, 66)$ | $(77, 66)$ |
| 13 | $(4, 12)$ | 12 | $(65, 78)$ | $(91, 78)$ |
| | $(1, 12)$ | 6 | $(26, 39)$ | $(52, 39)$ |
| | $(8, 1)$ | 12 | $(52, 78)$ | $(104, 78)$ |
| | $(3, 12)$ | 14 | $(78, 91)$ | $(104, 91)$ |

Tabelle 2 Beispiele für $(a, b)$-Fibonacci-Folgen und Primzahlen $p \leq 13$, die auf zwei mögliche Ordnungen führen

**Bemerkung 3.2.** Die Ergebnisse lassen sich noch weiter verallgemeinern, indem lineare Rekursionen $k$-ter Ordnung betrachtet werden. Diese sind durch die Vorschrift

$$f_n = a_1 \cdot f_{n-1} + a_2 \cdot f_{n-2} + \cdots + a_k \cdot f_{n-k} \text{ für } n \geq k$$

mit Koeffizienten $a_1, \ldots, a_k$ und mit Startwerten $f_0 = u_0$, $f_1 = u_1, \ldots, f_{k-1} = u_{k-1}$ mit $(u_0, u_1, \ldots, u_{k-1}) \neq (0, 0, \ldots, 0)$ gegeben.

Auch hier lassen sich analog zu Abschnitt 2 sehr gute Primzahlen definieren. Die Periodenlängen steigen aber für $k \geq 3$ stark an, so dass sich kein präsentierbarer Zaubertrick daraus ableiten lässt.

## Literatur


[1] E. Behrends, *Fibonacci goes magic*, Elemente der Mathematik, 69(4) (2014), 169–177, DOI: 10.4171/EM/260

[2] E. Behrends, *Zaubern und Mathematik*, Springer-Verlag (2017), DOI: 10.1007/978-3-658-17505-4

[3] P. Diaconis, R. Graham, *Magical Mathematics*, Princeton University Press (2012), DOI: 10.1515/978-1-400-83938-4

[4] H. Kurzweil, *Endliche Körper – Verstehen, Rechnen, Anwenden*, Springer-Verlag, 2. Auflage (2008), DOI: 10.1007/978-3-540-79598-8

[5] H.-C. Li, *On second-order linear recurrence sequences: Wall and Wyler revisited*, Fibonacci Quarterly, 37(4) (1999), 342–349

[6] K. Reiss, G. Schmieder, *Basiswissen Zahlentheorie: Eine Einführung in Zahlen und Zahlbereiche*, Springer-Verlag, 3. Auflage (2014), DOI: 10.1007/b137976

[7] M. Renault, *The period, rank and order of the* $(a, b)$*-Fibonacci sequence* mod $m$, Mathematics Magazine, 86(5) (2013), 372-380, DOI: 10.4169/math.mag.86.5.372

[8] P. Ribenboim, *The little book of bigger primes*, Springer-Verlag, 2. Auflage (2010), DOI: 10.1007/b97621



Nina Strasser
e-mail: NinaStrasser@web.de

Annegret Weng
Hochschule für Technik
Schellingstr. 24
D-70174 Stuttgart, Germany
e-mail: annegret.weng@hft-stuttgart.de