ACTA ARITHMETICA
LXX.1 (1995)

Rekurrente Folgen mit lokal gleichmäßig beschränkter Primteileranzahl

von

Cordelia Methfessel (Clausthal)

1. Einleitung. Es sei K ein Körper, 0 sein Nullelement und F_K der Vektorraum der K-wertigen Folgen $g : \mathbb{N} \to K$, speziell sei $\mathbb{F} := F_{\mathbb{C}}$. Das Symbol 0 stehe auch für die Nullabbildung aus F_K.

Eine Folge $g \in F_K$ heißt *rekurrent*, falls es ein $k \in \mathbb{N}$ und Zahlen $a_\kappa \in K$ für $\kappa = 0, 1, \ldots, k-1$ mit $a_0 \neq 0$ gibt, so daß

$$g(n+k) + a_{k-1}g(n+k-1) + \ldots + a_0 g(n) = 0 \tag{1}$$

für alle $n \in \mathbb{N}$ erfüllt ist.

Die Gleichung (1) wird als *homogene lineare Rekursion mit konstanten Koeffizienten* bezeichnet, k als ihre *Ordnung*.

In dieser Arbeit werden diejenigen rekurrenten Folgen $g \in \mathbb{F}$ charakterisiert, deren von Null verschiedene Folgenglieder bei fest vorgegebenem $m \in \mathbb{N}$ jeweils nur höchstens m Primteiler haben. Es besteht nämlich der folgende

Satz. *Es sei $m \in \mathbb{N}$ und $g : \mathbb{N} \to \mathbb{Z}$ rekurrent mit $\omega(|g(n)|) \leq m$ für alle $n \in \mathbb{N}$ mit $g(n) \neq 0$. Dann ist die Menge $P_g := \{p \in \mathbb{P} :$ es gibt ein $n \in \mathbb{N}$ mit $g(n) \neq 0$ und $p \,|\, g(n)\}$ der Primteiler von g bereits endlich.*

Wie üblich gibt dabei die Funktion $\omega : \mathbb{N} \to \mathbb{N}_0$ die Anzahl der verschiedenen Primteiler einer natürlichen Zahl an.

Als Spezialfall unseres Ergebnisses ergibt sich ein Resultat von Erdős, Maxsein und Smith [1]: Es sei g eine rekurrente Folge, die nur aus Primzahlpotenzen besteht. Dann ist die Menge P_g der Primteiler von g endlich.

Andererseits erweitert unser Ergebnis ein Resultat von Pólya [4], der rekurrente Folgen mit endlicher Primteileranzahl untersuchte. Er zeigte, daß solche Folgen in eine endliche Anzahl von Teilfolgen zerfällen, die rekurrent von der Ordnung eins sind. Unser Satz zeigt, daß es genügt, statt der Endlichkeit der Primteilermenge lediglich die lokale gleichmäßige Beschränktheit der Primteileranzahl vorauszusetzen.

Die Beweisidee besteht in der Verwendung des Endomorphismus z von F_K, erklärt durch $g \mapsto zg$ mit

$$zg(n) = g(n+1) \qquad (n \in \mathbb{N}),$$

den Verschiebungsoperator. Wir schreiben $z^1 = z$ und $z^{l+1} = z \circ z^l$ $(l \in \mathbb{N})$ und können die Elemente

$$f(z) = z^k + a_{k-1}z^{k-1} + \ldots + a_0 \tag{2}$$

des Polynomrings $(K[z], +, \cdot)$ identifizieren mit den durch $g \mapsto f(z)g$,

$$f(z)g(n) = g(n+k) + a_{k-1}g(n+k-1) + \ldots + a_0 g(n) \qquad (n \in \mathbb{N}),$$

vermittelten Endomorphismen von F_K.

Das Polynom (2) heißt das *Begleitpolynom* der Rekursion (1).

Bevor wir unseren Satz im Abschnitt 3 beweisen, stellen wir einige für den Beweis benötigte Hilfssätze zusammen.

2. Grundlegende Lemmas. Gewisse Teilfolgen der untersuchten Folge g werden wiederholt auftreten; mit ihnen beschäftigt sich das erste Lemma.

LEMMA 1. *Die Folge $g : \mathbb{N} \to \mathbb{C}$ genüge einer Rekursion der Ordnung $k \in \mathbb{N}$. Dann genügt auch jede Teilfolge $g_{a,q} : \mathbb{N} \to \mathbb{C}$ mit $n \mapsto g_{a,q}(n) := g(a + (n-1)q)$ von g für $a, q \in \mathbb{N}$ einer Rekursion der Ordnung k.*

Beweis. Nach Voraussetzung gilt $(z - \alpha_1) \ldots (z - \alpha_k)g(n) = 0$ mit gewissen $\alpha_\kappa \in \mathbb{C}$ für $\kappa = 1, \ldots, k$ und alle $n \in \mathbb{N}$.

Es sei nun $f_q(z) := (z - \alpha_1^q)(z - \alpha_2^q) \ldots (z - \alpha_k^q)$; dann folgt wegen $f(z) \mid f_q(z^q)$

$$f_q(z^q)g(n) = 0 \qquad \text{für alle } n \in \mathbb{N}.$$

Das bedeutet mit $(z-\alpha_1^q) \ldots (z-\alpha_k^q) = z^k + a_{q,k-1}z^{k-1} + \ldots + a_{q,1}z + a_{q,0}$

$$g(n+kq) + a_{q,k-1}g(n+(k-1)q) + \ldots + a_{q,1}g(n+q) + a_{q,0}g(n) = 0$$

für alle $n \in \mathbb{N}$, also insbesondere für $n \equiv a \bmod q$. Damit erhalten wir sofort

$$(z - \alpha_1^q) \ldots (z - \alpha_k^q)g_{a,q}(n) = 0 \qquad \text{für alle } n \in \mathbb{N}. \ \blacksquare$$

Das folgende Lemma und sein Beweis stehen bei Pólya [4].

LEMMA 2 (Pólya). *Die Folge $g : \mathbb{N} \to \mathbb{Z}$ sei von Anfang an rekurrent, und die Menge P_g der Primteiler von g sei endlich. Dann gibt es Zahlen $q \in \mathbb{N}$ und $d_a \in \mathbb{Z}$ für $a = 1, \ldots, q$, so daß*

$$(z - d_a)g_{a,q}(n) = 0 \qquad \textit{für alle } n \in \mathbb{N}.$$

Es genügt, für d_a natürliche Zahlen zuzulassen:

FOLGERUNG 1. *Die Folge $g : \mathbb{N} \to \mathbb{Z}$ sei von Anfang an rekurrent, und die Menge P_g der Primteiler von g sei endlich. Dann gibt es Zahlen $q \in \mathbb{N}$*

und $d_a \in \mathbb{N}$ *für* $a = 1, \ldots, q$, *so daß*

$$(z - d_a)g_{a,q}(n) = 0 \qquad \textit{für alle } n \in \mathbb{N}. \tag{3}$$

B e w e i s. Falls $d_a = 0$ für ein $a \in \{1, \ldots, q\}$, dann gilt $g_{a,q}(n) = 0$ für $n > 1$. Da $g_{a,q}$ nach Lemma 1 rekurrent ist, folgt $g_{a,q}(1) = 0$, und für d_a kann jede natürliche Zahl gewählt werden.

Die Rekursion $(z - d_a)g_{a,q}(n) = 0$ hat zur Folge

$$(z + d_a)(z - d_a)g_{a,q}(n) = (z^2 - d_a^2)g_{a,q}(n) = 0,$$

d.h.

$$g(a + (n + 1)q) - d_a^2 g(a + (n - 1)q) = 0,$$

also

$$(z - d_a^2)g_{a,2q}(n) = (z - d_a^2)g_{a+q,2q}(n) = 0 \qquad \text{für alle } n \in \mathbb{N}.$$

Somit können durch Verdoppelung des Moduls q immer natürliche Faktoren d_a erreicht werden. ∎

B e m e r k u n g. Die Rekursionsgleichung (3) besagt, daß es ein $q \in \mathbb{N}$ und natürliche Zahlen d_a gibt, so daß $g(a + nq) = g(a)d_a^n$ für $a = 1, \ldots, q$ und alle $n \in \mathbb{N}$ gilt. Eine Folge, die auf diese Weise in Teilfolgen zerfällt, hat offensichtlich nur endlich viele Primteiler.

Bei rekurrenten Folgen ganzer Zahlen können auch die Rekursionskoeffizienten ganz gewählt werden:

Lemma 3. *Es sei* $g : \mathbb{N} \to \mathbb{Z}$ *von Anfang an rekurrent. Dann genügt* g *einer Rekursion*

$$a_k g(n + k) + a_{k-1} g(n + k - 1) + \ldots + a_0 g(n) = 0 \tag{4}$$

mit $a_\kappa \in \mathbb{Z}$ *für* $\kappa = 0, 1, \ldots, k$ *und* $(a_0, a_1, \ldots, a_k) = 1$.

B e w e i s. Es sei $f(z) = z^k + b_{k-1}z^{k-1} + \ldots + b_1 z + b_0$ das normierte Polynom kleinsten Grades mit $f(z)g = 0$. Dann ist das lineare Gleichungssystem $f(z)g(n) = 0$ für $n = 1, 2, \ldots, k$ eindeutig lösbar, und deshalb gilt $b_\kappa \in Q$ für $\kappa = 0, 1, \ldots, k - 1$. Es folgt die Behauptung. ∎

Mit Hilfe des folgenden Lemmas über rekurrente Folgen in endlichen Körpern (vgl. Lidl und Niederreiter [2]) können wir eine Aussage über die Periodizität von $g(n)$ modulo $p \in \mathbb{P}$ machen. Es bezeichne $\mathbb{P}^*$ die Menge der Primzahlpotenzen und $GF(q)$ für $q \in \mathbb{P}^*$ den endlichen Körper mit q Elementen.

Dann gilt:

Lemma 4. *Es sei* $q \in \mathbb{P}^*$ *und* $a_\kappa \in GF(q)$ *für* $\kappa = 0, 1, \ldots, k$ *mit* $a_0 \neq 0$. *Die Folge* $g \in F_{GF(q)}$ *genüge der Rekursionsgleichung*

$$g(n + k) + a_{k-1} g(n + k - 1) + \ldots + a_0 g(n) = 0 \tag{5}$$

für alle $n \in \mathbb{N}$. Dann gibt es ein $r \in \mathbb{N}$, so daß $g(n+r) = g(n)$ für alle $n \in \mathbb{N}$.

Auf unseren Fall angewandt, ergibt sich

LEMMA 5. *Es sei $g : \mathbb{N} \to \mathbb{Z}$ rekurrent von der Ordnung k und $p \in \mathbb{P}$. Dann gibt es ein $r \in \mathbb{N}$, so daß $g(n+r) \equiv g(n) \bmod p$ für alle $n \in \mathbb{N}$, $n > k$.*

Beweis. Nach Lemma 3 gibt es ein Polynom $f(z)$ mit ganzen teilerfremden Koeffizienten, so daß $f(z)g(n) = 0$ für alle $n \in \mathbb{N}$. Dann ist wenigstens einer der Koeffizienten von f modulo p von Null verschieden. Folglich genügt g modulo p jedenfalls für $n > k$ einer Rekursionsgleichung, die die Voraussetzung von Lemma 4 erfüllt. Es folgt die Behauptung. ∎

Erdős, Maxsein und Smith [1] geben eine gleichmäßige Schranke für das Einsetzen der Periodizität von g allgemeiner für Primzahlpotenzmoduln an. Uns wird dieses einfachere Lemma genügen.

3. Der Beweis des Satzes. Der Beweis wird über vier weitere Lemmas geführt. Zuerst zeigen wir, daß g wenigstens eine Teilfolge enthält, die einer Rekursion der Ordnung eins genügt:

LEMMA 6. *Es sei $m \in \mathbb{N}_0$ und $g : \mathbb{N} \to \mathbb{Z}$ rekurrent mit $\omega(|g(n)|) \le m$ für alle $n \in \mathbb{N}$ mit $g(n) \neq 0$. Dann gibt es eine Teilfolge $g_{a,q} : \mathbb{N} \to \mathbb{Z}$ von g und ein $d \in \mathbb{N}$, so daß*

$$(z-d)g_{a,q}(n) = 0 \qquad \textit{für alle } n \in \mathbb{N}.$$

Beweis. Für $m = 0$ gilt $g(n) \in \{-1, 1\}$ für alle $n \in \mathbb{N}$ und Folgerung 1 liefert die Behauptung. Wir schließen induktiv.

Es sei also die Aussage von Lemma 6 für ein festes $m \in \mathbb{N}_0$ wahr und $g : \mathbb{N} \to \mathbb{Z}$ eine rekurrente Folge mit $\omega(|g(n)|) \le m+1$ für alle $n \in \mathbb{N}$ mit $g(n) \neq 0$.

Wir dürfen annehmen, daß es ein $a \in \mathbb{N}$, $a > k$, mit $g(a) \neq 0$ und $\omega(|g(a)|) = m+1$ gibt, denn sonst folgt die Behauptung schon aus der Induktionsvoraussetzung.

Nach Lemma 5 gibt es dann zu jedem $p \mid g(a)$ ein $q_p \in \mathbb{N}$, so daß $g_{a,q_p}(n) \equiv 0 \bmod p$ für alle $n \in \mathbb{N}$. Mit

$$q^* := \prod_{p \mid g(a)} q_p$$

folgt, daß $g_{a,q^*}(n)$ für alle $n \in \mathbb{N}$ genau dieselben Primteiler wie $g(a)$ hat.

Schließlich liefert Folgerung 1 die Existenz eines $q \in \mathbb{N}$ mit $q^* \mid q$ und eines $d \in \mathbb{N}$, so daß

$$(z-d)g_{a,q}(n) = 0 \qquad \text{für alle } n \in \mathbb{N}. \ \blacksquare$$

Im nächsten Lemma dehnen wir die Behauptung von Lemma 6 induktiv auf r aufeinanderfolgende Teilfolgen von g aus.

LEMMA 7. *Es sei $m \in \mathbb{N}_0$, $g : \mathbb{N} \to \mathbb{Z}$ rekurrent und $\omega(|g(n)|) \leq m$ für alle $n \in \mathbb{N}$ mit $g(n) \neq 0$. Dann gibt es zu jedem $r \in \mathbb{N}$ Zahlen $a, q \in \mathbb{N}$ und $d_1, \ldots, d_r \in \mathbb{N}$ mit*

$$(z - d_\varrho) g_{a+\varrho,q}(n) = 0 \quad (\varrho = 1, \ldots, r).$$

Beweis. Für $r = 1$ entspricht die Behauptung Lemma 6.

Es seien nun $a, q \in \mathbb{N}$ und $d_\varrho \in \mathbb{N}$ für $\varrho = 1, \ldots, r-1$ so gewählt, daß

$$(z - d_\varrho) g_{a+\varrho,q}(n) = 0 \quad \text{für alle } n \in \mathbb{N}.$$

Wir betrachten die rekurrente Teilfolge $g_{a+r,q}$ von g. Nach Lemma 6 existieren $a^*, q^*, d^* \in \mathbb{N}$, so daß

$$(z - d^*) g_{a+r,q}(a^* + nq^*) = 0 \quad \text{für alle } n \in \mathbb{N}.$$

Mit $a^+ := a + a^*q$, $q^+ := q^*q$, $d_\varrho^+ := d_\varrho^{q^*}$ für $\varrho = 0, 1, \ldots, r-1$ und $d_r^+ := d^*$ folgt die Behauptung. ∎

Bei dieser Konstruktion kann allerdings in jedem Schritt der Modul q wachsen.

Im folgenden Lemma werden wir zeigen, daß vom Verhalten von k aufeinanderfolgenden Teilfolgen modulo q einer rekurrenten Folge g der Ordnung k bereits auf das Verhalten fast aller Teilfolgen modulo q geschlossen werden kann.

LEMMA 8. *Die Folge $g : \mathbb{N} \to \mathbb{C}$ genüge einer Rekursion der Ordnung $k \in \mathbb{N}$. Es gebe Zahlen $a, q \in \mathbb{N}$ und Polynome $f_1(z), \ldots, f_k(z) \in \mathbb{C}[z]$ mit*

$$f_\kappa(z) g_{a+\kappa,q}(n) = 0 \quad \textit{für } \kappa = 1, \ldots, k.$$

Mit dem kleinsten gemeinschaftlichen Vielfachen $F(z) = [f_1(z), \ldots, f_k(z)]$ in $\mathbb{C}[z]$ gilt dann auch $F(z) g_{b,q}(n) = 0$ für alle $b \in \mathbb{N}$, $b > a$.

Beweis. Wir zeigen, daß $g_{b,q}$ für alle $b \in \mathbb{N}$ mit $b > a$ eine Darstellung der Gestalt

$$g_{b,q}(n) = c_{b,1} g_{a+1,q}(n) + c_{b,2} g_{a+2,q}(n) + \ldots + c_{b,k} g_{a+k,q}(n) \tag{6}$$

mit gewissen $c_{b,\kappa} \in \mathbb{C}$ für $\kappa = 1, \ldots, k$ besitzt. Dann folgt sofort

$$F(z) g_{b,q}(n) = F(z)(c_{b,1} g_{a+1,q}(n) + c_{b,2} g_{a+2,q}(n) + \ldots + c_{b,k} g_{a+k,q}(n)) = 0,$$

weil $F(z)$ eine lineare Abbildung ist.

Für $a < b \leq a + k$ ist die Existenz einer Darstellung (6) trivial. Es sei also $b > a + k$ fest und die Behauptung für $g_{a+1,q}, g_{a+2,q}, \ldots, g_{b-1,q}$ erfüllt. Da g rekurrent von der Ordnung k ist, gilt

$$g(a + nq) = a_{k-1} g(a - 1 + nq) + \ldots + a_0 g(a - k + nq)$$

mit gewissen $a_\kappa \in \mathbb{C}$ $(\kappa = 0, 1, \ldots, k-1)$ für alle $n \in \mathbb{N}$ und die Induktionsvoraussetzung liefert die Behauptung. ∎

Zuletzt können wir den Beweis unseres Satzes abschließen. Dafür verwenden wir noch das folgende bekannte Lemma über die allgemeine Lösungsstruktur einer linearen Rekursion für den Fall $K = \mathbb{C}$ (vgl. z.B. Narkiewicz [3]).

LEMMA 9. *Es sei* $f(z) = (z-\alpha_1)^{k_1} \ldots (z-\alpha_r)^{k_r} \in \mathbb{C}[z]$ *mit paarweise verschiedenen* $\alpha_\varrho \in \mathbb{C} \setminus \{0\}$ *und* $k_\varrho \in \mathbb{N}$ *für* $\varrho = 1, \ldots, r$. *Die Lösungen* $g \in \mathbb{F}$ *der Rekursionsgleichung*

$$f(z)g(n) = 0 \qquad \textit{für alle } n \in \mathbb{N}$$

sind dann von der Gestalt

$$g(n) = \sum_{\varrho=1}^{k} \sum_{\kappa=0}^{k_\varrho - 1} c_{\varrho,\kappa} n^\kappa \alpha_\varrho^n,$$

mit Parametern $c_{\varrho,\kappa} \in \mathbb{C}$ *für* $\kappa = 0, 1, \ldots, k_\varrho - 1$ *und* $\varrho = 1, \ldots, r$.

Nun setzen wir $r := k$ in Lemma 7. Dann gibt es $a, q \in \mathbb{N}$ und $d_\kappa \in \mathbb{N}$ für $\kappa = 1, \ldots, k$, so daß

$$(z - d_\kappa) g_{a+\kappa,q}(n) = 0 \qquad \text{für alle } n \in \mathbb{N}.$$

Lemma 8 liefert mit $f(z) := [(z-d_0), (z-d_1), \ldots, (z-d_{k-1})]$ für alle $b \in \mathbb{N}$, $b > a$,

$$f(z) g_{b,q}(n) = 0 \qquad \text{für alle } n \in \mathbb{N}.$$

Das Polynom $f(z)$ hat höchstens k einfache Nullstellen $\delta_1, \ldots, \delta_j \in \mathbb{N}$. Mit Lemma 9 folgt

$$g_{b,q}(n) = c_{b,1}\delta_1^n + c_{b,2}\delta_2^n + \ldots + c_{b,j}\delta_j^n$$

mit gewissen $c_{b,1}, c_{b,2}, \ldots, c_{b,j} \in \mathbb{C}$. Wegen Lemma 6 enthält $g_{b,q}$ eine Teilfolge

$$\begin{aligned} g_{b,q}(a + q^* n) &= c_{b,1}\delta_1^{a+q^*n} + c_{b,2}\delta_2^{a+q^*n} + \ldots + c_{b,j}\delta_j^{a+q^*n} \\ &= c_{b,1}\delta_1^a(\delta_1^{q^*})^n + c_{b,2}\delta_2^a(\delta_2^{q^*})^n + \ldots + c_{b,j}\delta_j^a(\delta_j^{q^*})^n, \end{aligned}$$

die für ein $d \in \mathbb{N}$ durch $(z-d)$ annulliert wird.

Die natürlichen Zahlen $\delta_1^{q^*}, \ldots, \delta_j^{q^*}$ sind paarweise verschieden.

Deshalb kann nur höchstens einer der Koeffizienten $c_{b,1}, \ldots, c_{b,j}$ von Null verschieden sein. Für $b > a$ besitzt die Teilfolge $g_{b,q}$ folglich eine Darstellung der Form

$$g_{b,q}(n) = cd^n$$

mit $c \in \mathbb{Z}$, $d \in \mathbb{N}$, und die Primteilermenge $P_{g_{b,q}}$ von $g_{b,q}$ ist endlich für alle $b \in \mathbb{N}$, $b > a$.

Die Menge P_g der Primteiler von g zerfällt nun in

$$P_g = \bigcup_{a<b\le a+q} P_{g_{b,q}}$$
$$\cup \{p \in \mathbb{P} : \text{es gibt ein } n \in \mathbb{N},\ n \le a,\ \text{mit } g(n) \ne 0 \text{ und } p \,|\, g(n)\}$$

und ist offensichtlich endlich. Es folgt die Behauptung des Satzes. ∎

Literaturverzeichnis

[1] P. Erdős, Th. Maxsein und P. R. Smith, *Primzahlpotenzen in rekurrenten Folgen*, Analysis 10 (1990), 71–83.

[2] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Press, 1986.

[3] W. Narkiewicz, *Uniform Distribution of Sequences of Integers in Residue Classes*, Lecture Notes in Math. 1087, Springer, 1984.

[4] G. Pólya, *Arithmetische Eigenschaften der Reihenentwicklung rationaler Funktionen*, J. Reine Angew. Math. 151 (1921), 1–31.

INSTITUT FÜR MATHEMATIK
TECHNISCHE UNIVERSITÄT CLAUSTHAL
ERZSTR. 1
D-38678 CLAUSTHAL-ZELLERFELD, GERMANY
E-mail: MACM@MAJESTIX.RZ.TU-CLAUSTHAL.DE

Eingegangen am 19.7.1993
und in revidierter Form am 21.10.1993 (2464)