MATH SCAND 54 (1984), 310 316

ERWEITERUNG DREIELEMENTIGER BASEN BEI KONSTANTER FROBENIUSZAHL

CHRISTOPH KIRFEL

Eine Menge $A_k=\{a_1,a_2,\ldots,a_k\}\subset \mathbf{N}=\{1,2,\ldots\}$ mit $(a_1,a_2,\ldots,a_k)=1$ heißt eine *Basis*. Nur solche Mengen A_k werden hier betrachtet.

Eine Zahl $n\in \mathbf{N}_0$ heißt *darstellbar* mit der Basis A_k, falls

$$n=\sum_{i=1}^{k} x_i a_i\ ;\ x_i\in \mathbf{N}_0=\{0,1,2,\ldots\},\qquad i=1,2,\ldots,k\ .$$

Die größte mit einer Basis A_k nicht darstellbare Zahl heißt die *Frobeniuszahl* $g(A_k)$ der Basis.

Sei $a\in \mathbf{N}$, a nicht mit A_k darstellbar. Selmer [5, § 4] hat das Problem der *Basiserweiterung* $A_{k+1}=A_k\cup\{a\}$ bei gleichbleibender Frobeniuszahl aufgeworfen. Es geht dabei darum, A_k und a so zu bestimmen, daß $g(A_k)=g(A_{k+1})$ möglich wird. Er zeigt dort, daß dies für $k=2$ unmöglich ist, sodaß bei der Erweiterung von A_3 zu A_4 erstmals die Möglichkeit konstanter Frobeniuszahl auftritt. Um diese Frage, die auch von Metternich [3] untersucht worden ist, dreht sich dieser Artikel.

Diejenige Menge $T(a_1)$, die aus jeder Restklasse $(\mathrm{mod}\, a_1)$ den kleinsten mit A_k darstellbaren Vertreter enthält, nennen wir das *Minimalsystem* für A_k $(\mathrm{mod}\, a_1)$.

Brauer und Shockley [1] haben einen grundlegenden Zusammenhang zwischen Minimalsystem und Frobeniuszahl einer Basis entdeckt:

$$g(A_k)=\max T(a_1)-a_1\ . \tag{1}$$

Dies gibt uns leicht die Frobeniuszahl zweielementiger Basen: $g(A_2)=a_1a_2-a_1-a_2$.

Für dreielementige Basen A_3 hat Rödseth [4] das Minimalsystem mit seinem Algorithmus berechnet. Die unten benutzte Darstellung geht auf Metternich [3] zurück, der Rödseths Algorithmus um einiges verallgemeinerte.

Sei $(a_1,a_2,a_3)=1$, $(a_1,a_2)=d$. (Rödseth setzt $d=1$ voraus.) Wir definieren

$$s_{-1}=a_1/d\ .$$

Eingegangen am 21. Februar, 1983.

Dann existiert eine eindeutig bestimmte Lösung s_0 der linearen Kongruenz

$$a_2 s_0 \equiv d a_3 \pmod{a_1}, \quad 0 \leqq s_0 < s_{-1} .$$

Falls $s_0 = 0$, so setzen wir $m = -1$. Falls $s_0 > 0$, so benutzen wir den folgenden euklidischen Divisionsalgorithmus:

$$\begin{aligned}
s_{-1} &= q_1 s_0 - s_1, & 0 < s_1 < s_0 \\
s_0 &= q_2 s_1 - s_2, & 0 < s_2 < s_1 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
s_{m-2} &= q_m s_{m-1} - s_m, & 0 < s_m < s_{m-1} \\
s_{m-1} &= q_{m+1} s_m - s_{m+1}, & 0 = s_{m+1} < s_m .
\end{aligned}$$

Sodann definieren wir

$$P_{-1} = 0, \; P_0 = d \; ; \; P_{i+1} = q_{i+1} P_i - P_{i-1}, \quad i = 0, 1, \ldots, m$$

$$R_i = \frac{s_i a_2 - P_i a_3}{a_1}, \quad i = -1, 0, \ldots, m+1 . \tag{2}$$

Insbesondere gilt $R_i \in \mathbf{Z}$, weil $s_i a_2 \equiv P_i a_3 \pmod{a_1}$. Klar ist auch $R_{-1} > 0$, $R_{i+1} < R_i$ für $i = -1, 0, \ldots, m$, und $R_{m+1} < 0$. Bestimmt man nun $-1 \leqq v \leqq m$ so, daß

$$R_{v+1} \leqq 0 < R_v ,$$

dann gilt nach Rödseth:

$$\begin{aligned}
T(a_1) = \{ & x a_2 + y a_3 \mid 0 \leqq x < s_v - s_{v+1}, \; 0 \leqq y < P_{v+1} \} \\
\cup \{ & x a_2 + y a_3 \mid s_v - s_{v+1} \leqq x < s_v, \; 0 \leqq y < P_{v+1} - P_v \} ,
\end{aligned}$$

und deshalb nach (1):

$$g(A_3) = s_v a_2 + P_{v+1} a_3 - a_1 - a_2 - a_3 + \max \{ -s_{v+1} a_2, -P_v a_3 \} . \tag{3}$$

Wie schon erwähnt, ist das in unserem Artikel untersuchte Problem die Konstanz der Frobeniuszahl $g(A_3)$ bei einer Erweiterung der dreielementigen Basis A_3 zu einer vierelementigen Basis $A_4 = A_3 \cup \{a\}$, also die Bedingungen für

$$g(A_3) = g(A_4) . \tag{4}$$

Natürlich gilt stets $g(A_4) \leqq g(A_3)$.

Es existieren eindeutig bestimmte $\alpha, \beta \in \mathbf{N}_0$, sodaß

$$\begin{aligned}
& \alpha a_2 + \beta a_3 \equiv a \pmod{a_1} , \\
& (0 \leqq \alpha < s_v - s_{v+1} \wedge 0 \leqq \beta < P_{v+1}) \\
\vee \; & (s_v - s_{v+1} \leqq \alpha < s_v \wedge 0 \leqq \beta < P_{v+1} - P_v) ,
\end{aligned}$$

d.h. $\alpha a_2+\beta a_3 \in T(a_1)$. Dies ist der Fall, weil das Restsystem $T(a_1)$ vollständig ist und von jeder Restklasse genau einen Vertreter enthält. Wir definieren

$$R = \frac{\alpha a_2+\beta a_3-a}{a_1} \in \mathbf{Z} . \tag{5}$$

Falls a darstellbar ist mit A_3, so nennen wir a ein abhängiges Erweiterungselement. Dies ist genau dann der Fall, wenn $a \geqq \alpha a_2+\beta a_3$. Dann gilt natürlich (4). Im weiteren wollen wir uns nur noch mit *unabhängigen* Erweiterungselementen a beschäftigen. Dann ist also

$$a < \alpha a_2+\beta a_3, \quad R>0 .$$

Auch die Größenordnung der Basiselemente von A_3 wollen wit jetzt hier festlegen:

$$a_1 < a_2 < a_3 .$$

Falls $a<a_2$, können wir die Basen $A_4=A_3 \cup \{a\}$ mit (4) vollständig beschreiben.

I) Sei zuerst $P_v a_3 < s_{v+1} a_2$.

1) $\beta < P_{v+1}-P_v$. Dann ist nach (3) und (5)

$$\begin{aligned} g(A_3) &= (s_v-1)a_2+(P_{v+1}-P_v-1)a_3-a_1 \\ &= (s_v-1-\alpha)a_2+(P_{v+1}-P_v-1-\beta)a_3+(R-1)a_1+a . \end{aligned}$$

Damit is also eine Darstellung der Frobeniuszahl $g(A_3)$ mit nichtnegativen Koeffizienten mit der Basis A_4 gefunden, also ist (4) unmöglich. — Dasselbe Prinzip wird nun wiederholt (ohne weitere Kommentare) verwendet.

2) $\beta \geqq P_{v+1}-P_v$. Hier ist wegen (2) und (5)

$$g(A_3) = (s_v-s_{v+1}-1-\alpha)a_2+(2P_{v+1}-P_v-1-\beta)a_3+(R+R_{v+1}-1)a_1+a .$$

Falls $\alpha>0$ oder $\beta>P_{v+1}-P_v$, so ist

$$\begin{aligned} (R+R_{v+1})a_1 &= (\alpha+s_{v+1})a_2+(\beta-P_{v+1})a_3-a \\ &= \alpha a_2+(\beta-(P_{v+1}-P_v))a_3-a+s_{v+1}a_2-P_v a_3 > 0 , \end{aligned} \tag{6}$$

weil $a<a_2<a_3$ und $s_{v+1}a_2>P_v a_3$. Dann ist wieder (4) unmöglich.

Sei nun $\alpha=0$ und $\beta=P_{v+1}-P_v$ (d.h. $P_v>0$), dann ist

$$\begin{aligned} g(A_3) &= (s_v-s_{v+1}-1-2\alpha)a_2+(2P_{v+1}-P_v-1-2\beta)a_3 \\ &\quad +(2R+R_{v+1}-1)a_1+2a \\ &= (s_v-s_{v+1}-1)a_2+(P_v-1)a_3+(2R+R_{v+1}-1)a_1+2a . \end{aligned}$$

Falls $\beta = P_{v+1} - P_v > 1$, so ist

$$(2R + R_{v+1})a_1 = (P_{v+1} - P_v)a_3 - 2a + s_{v+1}a_2 - P_v a_3 > 0 .$$

Übrig bleibt $\alpha = 0$, $\beta = P_{v+1} - P_v = 1$, also $a \equiv a_3 \pmod{a_1}$. Dann ist aber

$$\begin{aligned} g(A_3) &= (s_v - 1)a_2 - a_1 = (s_v - s_{v+1} - 1)a_2 + P_{v+1}a_3 + (R_{v+1} - 1)a_1 \\ &= (s_v - s_{v+1} - 1)a_2 + (P_{v+1}R + R_{v+1} - 1)a_1 + P_{v+1}a . \end{aligned}$$

Weil $P_v < s_{v+1}a_2/a_3 < s_{v+1}$, ist dabei

$$(P_{v+1}R + R_{v+1})a_1 = s_{v+1}a_2 - P_{v+1}a > (s_{v+1} - P_v - 1)a_2 \geqq 0 .$$

Zusammenfassend läßt sich also sagen, daß, *falls* $P_v a_3 < s_{v+1}a_2$ *und* $a < a_2$, *so ist* $g(A_3) > g(A_4)$.

II) Sei nun $P_v a_3 \geqq s_{v+1}a_2$.

1) $\alpha < s_v - s_{v+1}$. Dann ist nach (3) und (5)

$$\begin{aligned} g(A_3) &= (s_v - s_{v+1} - 1)a_2 + (P_{v+1} - 1)a_3 - a_1 \\ &= (s_v - s_{v+1} - 1 - \alpha)a_2 + (P_{v+1} - 1 - \beta)a_3 + (R - 1)a_1 + a . \end{aligned}$$

2) $\alpha \geqq s_v - s_{v+1}$. Hier ist wegen (2) und (5)

$$g(A_3) = (2s_v - s_{v+1} - 1 - \alpha)a_2 + (P_{v+1} - P_v - 1 - \beta)a_3 + (R - R_v - 1)a_1 + a .$$

Falls $\alpha > s_v - s_{v+1}$ oder $\beta > 0$, so ist

$$\begin{aligned} (7) \qquad (R - R_v)a_1 &= \alpha a_2 + \beta a_3 - a - s_v a_2 + P_v a_3 \\ &= (\alpha - (s_v - s_{v+1}))a_2 + \beta a_3 - a + P_v a_3 - s_{v+1}a_2 > 0 , \end{aligned}$$

weil $a < a_2 < a_3$ und $P_v a_3 \geqq s_{v+1}a_2$.

Sei nun $\alpha = s_v - s_{v+1}$ (d.h. $s_{v+1} > 0$) und $\beta = 0$, dann ist

$$\begin{aligned} g(A_3) &= (2s_v - s_{v+1} - 1 - 2\alpha)a_2 + (P_{v+1} - P_v - 1 - 2\beta)a_3 \\ &\quad + (2R - R_v - 1)a_1 + 2a \\ &= (s_{v+1} - 1)a_2 + (P_{v+1} - P_v - 1)a_3 + (2R - R_v - 1)a_1 + 2a . \end{aligned}$$

Falls $\alpha = s_v - s_{v+1} > 1$, so ist

$$(2R - R_v)a_1 = (s_v - s_{v+1})a_2 - 2a + P_v a_3 - s_{v+1}a_2 > 0 .$$

Übrig bleibt $\alpha = s_v - s_{v+1} = 1$, $\beta = 0$, also $a \equiv a_2 \pmod{a_1}$. Sei zusätzlich $P_v a_3 > s_v a$, dann schließen wir

$$\begin{aligned} g(A_3) &= (P_{v+1} - 1)a_3 - a_1 = s_v a_2 + (P_{v+1} - P_v - 1)a_3 + (-R_v - 1)a_1 \\ &= (P_{v+1} - P_v - 1)a_3 + (s_v R - R_v - 1)a_1 + s_v a . \end{aligned}$$

Wieder ist (4) unmöglich, weil hier

$$(s_v R - R_v)a_1 = s_v(a_2 - a) - s_v a_2 + P_v a_3 > 0 .$$

Wir können auch zeigen, daß $P_v a_3 \leqq s_v a$ für (4) hinreichend ist:

SATZ 1. *Sei* $A_4 = A_3 \cup \{a\}$, $1 < a < a_2$, *und* $a_1 \nmid a$. *Dann sind die beiden folgenden Aussagen äquivalent*:

(i) $a \equiv a_2 \pmod{a_1}$, $s_v - s_{v+1} = 1$, $s_v a \geqq P_v a_3 \geqq s_{v+1} a_2$
(ii) $g(A_3) = g(A_4)$.

KOROLLAR. *Sei* $A_4 = A_3 \cup \{a\}$ *mit* $1 < a < a_1$. *Dann ist* $g(A_4) < g(A_3)$.

Wäre nämlich $g(A_4) = g(A_3)$, so ergeben $a \equiv a_2 \pmod{a_1}$ und $a < a_2$, daß $a_2 \geqq a_1 + a$. Mit $s_{v+1} = s_v - 1 > 0$ und $a < a_1$, folgt dann

$$\begin{aligned} P_v a_3 \geqq s_{v+1} a_2 &\geqq s_{v+1} a_1 + s_{v+1} a = s_{v+1} a_1 + s_v a - a \\ &\geqq a_1 + s_v a - a > s_v a , \end{aligned}$$

also ein Widerspruch.

Um Satz 1 zu beweisen, bemerken wir zuerst, daß (ii) $\Rightarrow$ (i) schon oben gezeigt wurde. Die umgekehrte Beweisrichtung erfordert einige neue Gedankengänge. Wir definieren

$$\begin{aligned} L_i = x_i a_2 + y_i a_3 + ia &\equiv g(A_3) \pmod{a_1}, \qquad i \in \mathbb{N}_0 , \\ &(0 \leqq x_i < s_v - s_{v+1} \wedge 0 \leqq y_i < P_{v+1}) \\ &\vee \ (s_v - s_{v+1} \leqq x_i < s_v \wedge 0 \leqq y_i < P_{v+1} - P_v) , \end{aligned}$$

d.h. $x_i a_2 + y_i a_3 \in T(a_1)$. Hier sind dann L_i, x_i und y_i eindeutig bestimmt.

Der Beweis läuft nun darauf hinaus zu zeigen, daß $L_i > g(A_3)$ für alle $i \in \mathbb{N}_0$. Dies bewirkt aber die Konstanz der Frobeniuszahl, denn angenommen $g(A_3) > g(A_4)$, dann ist $g(A_3)$ mit A_4 darstellbar, also

$$\begin{aligned} g(A_3) &= \hat{x}_1 a_1 + \hat{x}_2 a_2 + \hat{x}_3 a_3 + ia \\ g(A_3) - ia &\equiv \hat{x}_2 a_2 + \hat{x}_3 a_3 \equiv x_i a_2 + y_i a_3 \pmod{a_1} \\ g(A_3) &\geqq \hat{x}_2 a_2 + \hat{x}_3 a_3 + ia \geqq x_i a_2 + y_i a_3 + ia , \end{aligned}$$

weil $T(a_1)$ das Minimalsystem ist.

Induktionsanfang: $L_0 = g(A_3) + a_1$,

$$\begin{aligned} L_1 &= (s_v - 1)a_2 + (P_{v+1} - P_v - 1)a_3 + a \\ &= g(A_3) + a_1 + (s_v - 1)(a_2 - a) + s_v a - P_v a_3 > g(A_3) . \end{aligned}$$

Induktionsschritt: Es sei bereits gezeigt, daß $L_k > g(A_3)$ für $k \leqq i$.

A) $x_i = 0$.

a) $y_i \geqq P_v \Rightarrow L_{i+1} = (s_v - 1)a_2 + (y_i - P_v)a_3 + (i+1)a$, denn

$$L_{i+1} - L_i = (s_v - 1)(a_2 - a) + s_v a - P_v a_3 \equiv 0 \pmod{a_1}.$$

$$L_{i+1} \geqq L_i > g(A_3).$$

b) $y_i < P_v \Rightarrow L_{i+1} = (y_i + P_{v+1} - P_v)a_3 + (i+1)a$, denn

$$L_{i+1} - L_i = (P_{v+1} - P_v)a_3 + a \equiv (P_{v+1} - P_v)a_3 + (s_v - s_{v+1})a_2 \equiv 0 \pmod{a_1}.$$

$$L_{i+1} > L_i > g(A_3).$$

B) $x_i > 0$, dann ist $y_i < P_{v+1} - P_v$ und

$$L_{i+1} = (x_i - 1)a_2 + y_i a_3 + (i+1)a.$$

Nun ist $i + x_i - s_v = 0$ für $i = 1$ und $i + x_i - s_v \geqq 0$ für $i > 1$, denn wächst i um 1, so fällt x_i höhstens um 1.

$$L_{i+x_i-s_v} = (y_i + P_v)a_3 + (i + x_i - s_v)a,$$

denn

$$L_{i+1} - L_{i+x_i-s_v} = (x_i - 1)(a_2 - a) + s_v a - P_v a_3 \equiv 0 \pmod{a_1}.$$

$$L_{i+1} \geqq L_{i+x_i-s_v} + s_v a - P_v a_3 \geqq L_{i+x_i-s_v} > g(A_3).$$

Damit ist Satz 1 bewiesen, und wir können das Erweiterungsproblem für $a < a_2$ als gelöst betrachten.

Bereits für den Fall $a < a_3$ wird die Charakterisierung der Basen A_4 mit (4) recht kompliziert. Wir wollen uns hier mit der Erwähnung eines charakteristischen Kriteriums begnügen, ohne den Beweis auszugeben. Vollständig finden sich die Resultate in Kirfel [2].

SATZ 2. *Sei* $A_4 = A_3 \cup \{a\}$, *a unabhängig von* A_3 *und* $1 < a < a_3$. *Sei zusätzlich* $P_v a_3 \geqq s_{v+1} a_2$, *dann sind die beiden folgenden Aussagen äquivalent*:

(i) $\alpha \geqq s_v - s_{v+1}, \quad \beta = 0;$

$$cR_v \geqq \left[\frac{(c+1)s_v - s_{v+1} - 1}{\alpha}\right] R, \quad 1 \leqq c \leqq \left[\frac{P_{v+1} - 1}{P_v}\right] = q_{v+1} - 1$$

(ii) $g(A_3) = g(A_4)$.

Auch für den Fall $P_v a_3 < s_{v+1} a_2$ läßt sich ein Kriterium aufstellen, das A_4 im Falle (4) vollständig beschreibt. Dieses ist natürlich mit Satz 2 eng verwandt.

Zum Schluß soll noch erwähnt werden, daß für den Fall $a > a_3$ die hier benutzten Mittel nur noch wenig hergeben, sodaß dieser Teil der Erweiterungsproblematik noch ungelöst bleibt.

Für den Fall eines generellen a mit $g(A_3) = g(A_4)$ können wir doch eine untere Schranke angeben. Aus (6) und (7) folgt $s_{v+1}a_2 - P_v a_3 \leqq a$ falls $s_{v+1}a_2 > P_v a_3$, $P_v a_3 - s_{v+1}a_2 \leqq a$ falls $P_v a_3 \geqq s_{v+1}a_2$. Insgesamt gilt also für ein unabhängiges Erweiterungselement a mit (4):

$$|P_v a_3 - s_{v+1}a_2| \leqq a .$$

Das bekannte Beispiel $A_3 = \{137, 251, 256\}$ ist in Rödseth [4] durchgerechnet. Es gilt $v = 4$, $P_v a_3 - s_{v+1}a_2 = 1049$. Metternich [3, S. 72] gibt drei Möglichkeiten für a an, nämlich $a = 1597$, 1802, 1817. Jeweils gilt $g(A_3) = g(A_4) = 4948$.

Ich muß hier auch einen besonderen Dank an Prof. E. S. Selmer richten, von dem ich das Problem der Basiserweiterung erhalten habe, und der mir bei der Ausarbeitung des Artikels behilflich war.

LITERATURHINWEISE

1. A. Brauer und J. E. Shockley, *On a problem of Frobenius*, J. Reine Angew. Math. 211 (1962), 215–220.
2. J. C. Kirfel, *Erweiterung dreielementiger Basen bei konstanter Frobeniuszahl und Reichweite*, Hovedoppgave, Math. Inst., Univ. Bergen, 1982.
3. H. Metternich, *Über ein Problem bei Frobenius. Basiserweiterung bei konstanter Frobeniuszahl*, Diplomarbeit Mathematik, Joh. Gutenberg-Univ., Mainz, 1981.
4. Ö. J. Rödseth, *On a linear diophantine problem of Frobenius*, J. Reine Angew. Math. 301 (1978), 171–178.
5. E. S. Selmer, *On the linear diophantine problem of Frobenius*, J. Reine Angew. Math. 293/294 (1977), 1–17.

MATHEMATISCHES INSTITUT
UNIVERSITÄT BERGEN
N-5000 BERGEN
NORWEGEN