Elem. Math. 62 (2007) 106 – 117
0013-6018/07/030106-12

Elemente der Mathematik

Idempotente Zahlen

Günter Köhler und Jürgen Spilker

Beide Verfasser sind pensionierte Professoren für Mathematik – in Würzburg beziehungsweise in Freiburg, und beide verbindet die Freude an Problemen und Ideen aus der elementaren Zahlentheorie und Analysis.

1 Einleitung

Es seien k, r und g natürliche Zahlen und $g \geq 2$. Eine ganze Zahl n nennen wir *k-idempotent modulo g^r* oder kürzer *idempotent*, wenn

$$n^k \equiv n \mod g^r$$

gilt. Das bedeutet im Falle $n > 0$, dass die letzten (rechtsstehenden) r Ziffern von n und seiner k-ten Potenz n^k im Stellenwertsystem zur Basis g übereinstimmen. Wenn n selber höchstens r Stellen hat, dann stellen die letzten r Ziffern von n^k die Zahl n dar.

In den Abschnitten 2 und 3 bestimmen wir die sämtlichen idempotenten Zahlen. Für beliebige k, r und g beschreiben wir also die Menge aller k-idempotenten Zahlen modulo g^r. Wir wollen diese Menge mit

$$I^k(g^r)$$

bezeichnen. Wegen

$$(n + xg^r)^k \equiv n^k \mod g^r$$

für beliebige ganze n und x gilt im Falle $n \in I^k(g^r)$ stets auch $n + xg^r \in I^k(g^r)$ für beliebige ganze x. Die Menge $I^k(g^r)$ besteht also aus vollständigen Restklassen modulo

Die Zahlen 0 und 1 sind die einzigen ganzen Zahlen, die gleich ihren Quadraten sind. Bei manchen anderen natürlichen Zahlen bleiben beim Quadrieren wenigstens einige Endziffern erhalten, beispielsweise in $6^2 = 36$, $76^2 = 5776$, $25^2 = 625$. Diese „idempotenten“ oder „automorphen“ Zahlen kann man sämtlich bestimmen. Die Autoren tun das in diesem Artikel auch für höhere als zweite Potenzen und auch für die Ziffern-darstellungen zu beliebigen Basen $g \geq 2$ anstelle von 10. Sie studieren zudem einige zahlentheoretische Eigenschaften der idempotenten Zahlen.

g^r, und man muss zu ihrer Beschreibung nur die endlich vielen Restklassen angeben, aus denen sie besteht. Die Kongruenzbedingung $n^k \equiv n \mod g^r$ kann auch als Polynomgleichung $X^k = X$ im Restklassenring $\mathbb{Z}/g^r\mathbb{Z}$ gelesen werden.

In den Abschnitten 4 bis 7 behandeln wir zahlentheoretische Eigenschaften von idempotenten Zahlen. Wir diskutieren Nachkommen, verwandte, komplementäre sowie Gemeinschaften von idempotenten Zahlen. Den quadratischen Fall ($k = 2$) hat C. Groß [1] untersucht.

Notationen. Wie üblich sei $\mathbb{Z}$ die Menge aller ganzen Zahlen, $\mathbb{N} = \{1, 2, 3, \ldots\}$ die Menge aller natürlichen Zahlen und $\mathbb{P}$ die Menge aller Primzahlen. Für $a, b \in \mathbb{Z}$ besagt $a|b$, dass a ein Teiler von b ist; die Negation dieser Aussage wird mit $a \nmid b$ notiert. Für $p \in \mathbb{P}$ besagt $p^\alpha \parallel b$, dass $p^\alpha | b$ und $p^{\alpha+1} \nmid b$ gilt. Den größten gemeinsamen Teiler von a und b bezeichnen wir mit (a, b). Die Kongruenz $a \equiv b \mod m$ ist äquivalent mit $m|(a-b)$. Mit g ist stets eine ganze Zahl ≥ 2 gemeint. Es bezeichne $\mathbb{P}_g = \left\{p \in \mathbb{P} \;\middle|\; p\,|g\right\}$ die Menge ihrer Primteiler und $\omega(g)$ die Anzahl der verschiedenen Primteiler von g, also die Anzahl der Elemente von $\mathbb{P}_g$.

2 Kleine Potenzen

In diesem Abschnitt werden alle k-idempotenten Zahlen für die Exponenten $k \in \{1, 2, 3\}$ bestimmt. Für beliebige k gilt

$$I^k(g^r) = \bigcap_{p^\alpha \parallel g} I^k(p^{\alpha r}), \tag{1}$$

und aus den Zahlen in den Mengen $I^k(p^{\alpha r})$ kann man mit dem Chinesischen Restsatz die Zahlen im Durchschnitt $I^k(g^r)$ bestimmen. Deshalb können wir uns auf Moduln $g = p^r$ beschränken, die Primzahlpotenzen sind.

Satz 1. *Für beliebige Primzahlen p und natürliche Zahlen k, r gilt*

(a) $I^1(p^r) = \mathbb{Z}$,

(b) $I^2(p^r) = p^r\mathbb{Z} \cup (p^r\mathbb{Z} + 1)$,

(c) $$I^3(p^r) = \begin{cases} p^r\mathbb{Z} \cup (p^r\mathbb{Z} + 1) \cup (p^r\mathbb{Z} - 1) & \text{für} \quad p \geq 3, \\ 2^r\mathbb{Z} \cup (2^{r-1}\mathbb{Z} + 1) \cup (2^{r-1}\mathbb{Z} - 1) & \text{für} \quad p = 2, r \geq 4, \\ 2^r\mathbb{Z} \cup (2\mathbb{Z} + 1) & \text{für} \quad p = 2, r \leq 3. \end{cases}$$

Beweis. Die Aussage (a) ist klar. Zur Begründung der anderen Behauptungen nutzen wir die Polynomzerlegungen

$$X^2 - X = X(X-1), \qquad X^3 - X = X(X-1)(X+1)$$

aus. Eine ganze Zahl n gehört genau dann zu $I^2(p^r)$, wenn $p^r|(n^2 - n)$ ist. Äquivalent hierzu ist, dass die Primzahlpotenz p^r einen der beiden Faktoren n oder $n - 1$ teilt, und dies ist äquivalent zu

$$n \in p^r\mathbb{Z} \qquad \text{oder} \qquad n \in (p^r\mathbb{Z} + 1).$$

Damit ist (b) bewiesen.

Eine ganze Zahl n gehört genau dann zu $I^3(p^r)$, wenn $p^r|(n^3-n)$ ist. Äquivalent hierzu ist im Falle $p \geq 3$, dass die Primzahlpotenz p^r einen der drei Faktoren n, $n-1$ oder $n+1$ teilt. Wie zuvor führt das auf die in (c) angegebenen Restklassen modulo p^r. Nun sei $p=2$. Dann können wir nur schließen, dass $n \in I^3(2^r)$ äquivalent zu

$$2^r|n \qquad \text{oder} \qquad 2^r|(n-1)(n+1)$$

ist. Zu diskutieren ist der zweite Fall $2^r|(n-1)(n+1)$. Dann ist jeder der beiden Faktoren $n-1$ und $n+1$ gerade und genau einer durch 4 teilbar. Also ist dieser Fall äquivalent zu

$$2^{r-1}|(n-1) \qquad \text{oder} \qquad 2^{r-1}|(n+1).$$

Damit folgen die Aussagen in (c) für $p=2$. □

3 Beliebige Potenzen

Die Beweisidee in Satz 1 ist für Exponenten $k > 3$ nicht brauchbar, weil die Polynome $X^k - X$ über $\mathbb{Z}$ nicht vollständig in Linearfaktoren zerfallen. Stattdessen wird uns die bekannte Struktur der primen Restklassengruppe modulo p^r zum Ziel führen. Wie wir in der Einleitung bereits bemerkt haben, besteht $I^k(g^r)$ aus vollständigen Restklassen modulo g^r. Wir bezeichnen (falls g und r aus dem Kontext hervorgehen) mit $\overline{n}$ die Restklasse von n modulo g^r, und wir setzen

$$\overline{I}^k(g^r) = \{\overline{n} \in \mathbb{Z}/g^r\mathbb{Z} \mid n \in I^k(g^r)\}.$$

Mit $a^k(g^r)$ bezeichnen wir die Anzahl der Elemente in $\overline{I}^k(g^r)$. Die Abbildung $x \bmod m \mapsto (x \bmod p^\alpha)_{p^\alpha \| m}$ ist nach dem Chinesischen Restsatz ein Ringisomorphismus von $\mathbb{Z}/m\mathbb{Z}$ auf das direkte Produkt der Ringe $\mathbb{Z}/p^\alpha\mathbb{Z}$ mit $p^\alpha \parallel m$. Daher gilt

$$\overline{I}^k(g^r) = \prod_{p^\alpha \| g} \overline{I}^k(p^{\alpha r}), \tag{2}$$

und die Anzahl der Elemente ist eine multiplikative Funktion von g, also

$$a^k(g^r) = \prod_{p^\alpha \| g} a^k(p^{\alpha r}). \tag{3}$$

Wir bezeichnen mit

$$(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{n} \in \mathbb{Z}/m\mathbb{Z} \mid (n,m) = 1\}$$

die prime Restklassengruppe modulo m. Für Potenzen $m = p^r$ von Primzahlen $p \neq 2$ ist $(\mathbb{Z}/p^r\mathbb{Z})^*$ nach einem Resultat von Gauß eine zyklische Gruppe von der Ordnung $p^{r-1}(p-1)$ ([2, Kap. 6, § 2]). Jedes erzeugende Element der Gruppe heißt eine *Primitivwurzel* modulo p^r. Wenn e eine Primitivwurzel modulo p ist, dann ist e oder $e+p$ eine Primitivwurzel zu jeder Potenz p^r. Die Gruppe $(\mathbb{Z}/2^r\mathbb{Z})^*$ ist für $r \leq 2$ zyklisch und für $r \geq 3$ ein direktes Produkt zweier zyklischer Gruppen der Ordnungen 2^{r-2} und 2, die von den Restklassen der Zahlen 5 und -1 erzeugt werden.

Satz 2. *Es seien r und k natürliche Zahlen, $k \geq 2$, p eine Primzahl, $p \neq 2$. Es sei $d = (p-1, k-1)$, die Zahl s sei durch $p^s \parallel (k-1)$ bestimmt, und e sei eine Primitivwurzel modulo p^r. Dann gilt:*

(a) *Die Gleichung $x^k = x$ hat in $\mathbb{Z}/p^r\mathbb{Z}$ genau*

$$a^k(p^r) = 1 + p^{\min\{r-1,s\}} \cdot d$$

Lösungen.

(b) *Die sämtlichen Lösungen $x \neq \overline{0}$ sind*

$$x = f^j \quad \textit{mit} \quad 1 \leq j \leq p^{r-1}d \quad \textit{für} \quad r \leq s,$$
$$x = f^{jp^{r-1-s}} \quad \textit{mit} \quad 1 \leq j \leq p^s d \quad \textit{für} \quad r > s.$$

Dabei ist

$$f = e^{(p-1)/d}.$$

Beweis. Die Lösung $x = \overline{0}$ bringt den Summanden 1 in der Formel für $a^k(p^r)$. Lösungen $x \neq \overline{0}$ sind teilerfremd zu p; für diese ist also $x^k \equiv x \mod p^r$ äquivalent zu

$$x^{k-1} \equiv 1 \mod p^r.$$

Somit ist $a^k(p^r) = 1 + b^k(p^r)$, wobei $b^k(p^r)$ die Anzahl der Lösungen von $x^{k-1} = \overline{1}$ in $(\mathbb{Z}/p^r\mathbb{Z})^*$ ist. Jedes Element x dieser zyklischen Gruppe ist eindeutig in der Form $x = e^m$ mit $1 \leq m \leq p^{r-1}(p-1)$ darstellbar. Damit wird $x^{k-1} = \overline{1}$ zu $e^{m(k-1)} = \overline{1}$. Äquivalent hierzu ist, dass $m(k-1)$ ein Vielfaches der Gruppenordnung ist, also

$$p^{r-1}(p-1) \mid m(k-1).$$

Es gilt $p - 1 = dc$, $k - 1 = p^s db$, worin b und c untereinander und zu p teilerfremde natürliche Zahlen sind. Wir setzen $t = \min\{r-1, s\}$ und erhalten die Äquivalenzen

$$\begin{aligned} p^{r-1}(p-1) \mid m(k-1) &\iff p^{r-1}c \mid p^s mb \\ &\iff p^{r-1}c \mid p^s m \\ &\iff p^{r-1-t}c \mid p^{s-t}m. \end{aligned}$$

Zunächst sei $t = r - 1$. Die letzte Teilerbedingung lautet dann $c \mid p^{s-r+1}m$, und das ist wegen $p \nmid c$ äquivalent zu $c \mid m$. Die Lösungen m sind

$$m = jc \qquad \text{mit} \qquad 1 \leq j \leq \frac{p^{r-1}(p-1)}{c} = p^t d.$$

Wir erhalten die Lösungen $x = e^{cj} = \left(e^{(p-1)/d}\right)^j = f^j$.

Nun sei $t = s$. Dann lautet die Teilerbedingung $p^{r-1-s}c \mid m$. Die Lösungen m sind

$$m = jp^{r-1-s}c \qquad \text{mit} \qquad 1 \leq j \leq \frac{p^{r-1}(p-1)}{p^{r-1-s}c} = p^t d.$$

Wir erhalten die Lösungen $x = \left(e^{p^{r-1-s}c}\right)^j = \left(e^{p^{r-1-s}(p-1)/d}\right)^j = f^{jp^{r-1-s}}$. Damit sind alle Behauptungen bewiesen. □

Die Primzahl 2 spielt eine Ausnahmerolle, weil die prime Restklassengruppe modulo 2^r für $r \geq 3$ nicht zyklisch ist.

Satz 3. *Es seien $k \geq 2$ und $r \geq 3$ natürliche Zahlen, und s und u seien durch $k-1 = 2^s u$ mit ungeradem u definiert. Dann gilt:*

(a) *Die Gleichung $x^k = x$ hat in $\mathbb{Z}/2^r\mathbb{Z}$ genau 2 Lösungen, wenn k gerade ist, und genau*

$$a^k(2^r) = 1 + 2^{1+\min\{r-2,s\}}$$

Lösungen, wenn k ungerade ist.

(b) *Für gerades k sind $\overline{0}$ und $\overline{1}$ die einzigen Lösungen. Für ungerades k sind die sämtlichen Lösungen $x \neq \overline{0}$ gegeben durch*

$$\begin{aligned} \pm\,\overline{5}^j \quad & \textit{mit} \quad 1 \leq j \leq 2^{r-2} \quad \textit{für} \quad r-2 \leq s, \\ \pm\,\overline{5}^{2^{r-2-s}j} \quad & \textit{mit} \quad 1 \leq j \leq s \qquad \textit{für} \quad r-2 \geq s. \end{aligned}$$

Beweis. Außer $x = \overline{0}$ hat $x^k = x$ nur ungerade Lösungen, und diese gehören zur Gruppe $(\mathbb{Z}/2^r\mathbb{Z})^*$ und erfüllen $x^{k-1} = \overline{1}$. Alle Elemente $x \neq \overline{1}$ in dieser Gruppe haben gerade Ordnung. Für ungerades $k-1$ ist also $x = \overline{1}$ die einzige Lösung von $x^{k-1} = \overline{1}$. Nun sei $k-1$ gerade, also $s \geq 1$. Es bestehen die Äquivalenzen

$$x^{k-1} = \overline{1} \quad \Longleftrightarrow \quad \left(x^{2^s}\right)^u = \overline{1} \quad \Longleftrightarrow \quad x^{2^s} = \overline{1}.$$

Nach der Bemerkung vor Satz 2 hat jede Restklasse $x \in (\mathbb{Z}/2^r\mathbb{Z})^*$ eine eindeutige Darstellung $x = \pm\,\overline{5}^j$ mit $1 \leq j \leq 2^{r-2}$. Die Lösungen der Gleichung $x^{2^s} = \overline{1}$ sind daher durch

$$2^{r-2} | 2^s j$$

gekennzeichnet. Die sämtlichen nicht-trivialen Lösungen sind also

$$\begin{aligned} \pm\,\overline{5}^j \quad & \text{mit} \quad 1 \leq j \leq 2^{r-2} \quad \text{für} \quad r-2 \leq s, \\ \pm\,\overline{5}^{2^{r-2-s}j} \quad & \text{mit} \quad 1 \leq j \leq s \qquad \text{für} \quad r-2 \geq s. \end{aligned}$$

Damit sind alle Behauptungen des Satzes bewiesen. □

Beispiel 1 Die Sätze 2 und 3 besagen für $k = 2$, dass die Gleichung $x^2 = x$ in jedem der Ringe $\mathbb{Z}/p^r\mathbb{Z}$ nur die beiden trivialen Lösungen $\overline{0}$ und $\overline{1}$ hat. Aus (3) folgt daher $a^2(g^r) = 2^{\omega(g)}$. Nicht-triviale idempotente Zahlen modulo g^r existieren also genau dann, wenn g mindestens 2 Primteiler hat ([1, Satz 2]).

4 Nachkommen

Streicht man bei einer idempotenten Zahl $n \in I^k(g^r)$ mit $r \geq 2$ die Ziffer bei g^{r-1}, dann erhält man eine idempotente Zahl $m \in I^k(g^{r-1})$. Denn aus $n^k \equiv n \mod g^r$ und $n = \sum_\nu a_\nu g^\nu = a_{r-1}g^{r-1} + m$ mit $0 \leq a_\nu < g$, folgt

$$m^k = (n - a_{r-1}g^{r-1})^k \equiv n^k \equiv n \equiv m \mod g^{r-1}.$$

Man erhält also durch Streichen vorderer Ziffern eine Folge idempotenter Zahlen zu fallenden Moduln $g^{r-1}, g^{r-2}, \ldots, g$. Ein Beispiel hierzu ist die Folge idempotenter Zahlen $625 \in I^2(10^4)$, $625 \in I^2(10^3)$, $25 \in I^2(10^2)$, $5 \in I^2(10)$. (Das Streichen der ersten Ziffer 6 in $625 \in I^2(10^4)$ liefert keine Zahl in $I^2(10^3)$.)

Interessant erscheint uns die umgekehrte Prozedur: Kann man durch Vorschalten einer geeigneten Ziffer eine idempotente Zahl in eine ebensolche zu einem höheren Modul überführen? Wir behandeln das Problem allgemeiner für beliebige Polynome und wenden das Ergebnis dann auf den Spezialfall $X^k - X$ an.

Definition. Es sei $f(X)$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$, und es sei $n \in \mathbb{Z}$, $f(n) \equiv 0 \mod g^r$. Eine ganze Zahl $\widetilde{n}$ heißt ein *Nachkomme* von n (bezüglich $f(X)$ und g^r), falls

$$f(\widetilde{n}) \equiv 0 \mod g^{r+1} \qquad \text{und} \qquad \widetilde{n} \equiv n \mod g^r$$

gilt.

Lemma 4. *Es sei $f(X)$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$ und $f'(X)$ seine Ableitung, und es sei $n \in \mathbb{Z}$, $f(n) \equiv 0 \mod g^r$. Dann gilt:*

(a) *Wenn $f'(n)$ und g teilerfremd sind, dann hat n einen Nachkommen.*

(b) *Ist $g = p$ eine Primzahl, dann ist die Anzahl der Nachkommen von n modulo p^r gleich*

$$\begin{cases} 1, & \text{falls} \quad f'(n) \not\equiv 0 \mod p\,, \\ p, & \text{falls} \quad f'(n) \equiv 0 \mod p \quad \text{und} \quad f(n) \equiv 0 \mod p^{r+1}\,, \\ 0, & \text{falls} \quad f'(n) \equiv 0 \mod p \quad \text{und} \quad f(n) \not\equiv 0 \mod p^{r+1}\,. \end{cases}$$

Beweis. Jeder denkbare Nachkomme von n kann in der Form $\widetilde{n} = n + xg^r$ mit $x \in \mathbb{Z}$ geschrieben werden. Für jeden Exponenten j gilt $(n+xg^r)^j \equiv n^j + jn^{j-1}xg^r \bmod g^{r+1}$, und es folgt $f(\widetilde{n}) \equiv f(n) + f'(n)xg^r \mod g^{r+1}$. Somit ist $\widetilde{n}$ genau dann ein Nachkomme von n, wenn x eine Lösung der linearen Kongruenz

$$\frac{f(n)}{g^r} + f'(n)x \equiv 0 \mod g$$

ist. Diese Kongruenz ist lösbar, wenn $f'(n)$ und g teilerfremd sind. Nun sei $g = p$ eine Primzahl. Dann kann die lineare Kongruenz als lineare Gleichung über dem Körper $\mathbb{Z}/p\mathbb{Z}$ gelesen werden, und die Anzahl der Lösungen x modulo p ist durch die Liste in (b) gegeben. □

Wir wenden das Lemma auf idempotente Zahlen an:

Satz 5. *Die Zahlen $k-1$ und g seien teilerfremd. Dann besitzt jede Zahl $n \in I^k(g^r)$ einen Nachkommen $\widetilde{n} \in I^k(g^{r+1})$.*

Man kann sich die Menge $\bigcup_{r\geq 0} \overline{I}^k(g^r)$ als Graphen oder „Stammbaum“ vorstellen, und dieser besteht unter den Voraussetzungen in Satz 5 aus endlich vielen, unendlich langen (und möglicherweise verzweigten) Ketten von Nachkommen.

Beweis des Satzes. Es sei $n \in I^k(g^r)$. Dann gilt $\left(kn^{k-1}-1\,,\ g\right)=1$. Denn anderenfalls wäre $p\,|(kn^{k-1}-1)$ und $p\,|g$ für eine Primzahl p, und wegen $g^r|(n^k-n)$ folgt hieraus der Reihe nach $p\nmid n$, $p\,|(n^{k-1}-1)$, $p\,|(k-1)n^{k-1}$ und $p\,|(k-1,g)$, im Widerspruch zur Voraussetzung $(k-1,g)=1$. Somit ist Lemma 4(a) auf das Polynom $f(X)=X^k-X$ anwendbar, und man erhält eine Zahl $\widetilde{n}$ mit den behaupteten Eigenschaften $\widetilde{n}\in I^k(g^{r+1})$ und $\widetilde{n}\equiv n \mod g^r$. □

Beispiel 2 Die Voraussetzung der Teilerfremdheit von $k-1$ und g ist im quadratischen Fall $(k=2)$ stets erfüllt. Auf diese Voraussetzung kann nicht verzichtet werden. Beispielsweise besitzt $125\in I^3(10^3)$ keinen Nachfolger. Denn anderenfalls hätte

$$(125+x\,10^3)^3\equiv 125+x\,10^3 \mod 10^4$$

eine Lösung $x\in\mathbb{Z}$. Hieraus folgt $125^3-125+x\,10^3(3\cdot 125^2-1)\equiv 0 \mod 10^4$ und $125^3-125\equiv 0 \mod 2\cdot 10^3$ im Widerspruch zu $125^3-125=1953\cdot 10^3$.

In der folgenden Tabelle sind alle Elemente der Mengen $\overline{I}^k(10^r)$ für $k\le 3$ und $r\le 4$ aufgelistet, wobei anstelle der Restklassen $\overline{n}$ ihre Vertreter n mit $0\le n<10^r$ angegeben sind. Ein Verfahren zur Berechnung der Tabellenwerte ergibt sich aus dem Beweis von Lemma 4. Aus den Sätzen 2 und 3 und aus dem Chinesischen Restsatz erhält man die Lösungsanzahl $a^3(10^r)=a^3(2^r)a^3(5^r)=5\cdot 3=15$ für $r\ge 3$.

	$k=2$	$k=3$
$r=1$	0, 1, 5, 6	0, 1, 4, 5, 6, 9
$r=2$	0, 1, 25, 76	0, 1, 51, 24, 25, 75, 76, 49, 99
$r=3$	0, 1, 625, 376	0, 1, 251, 624, 125, 375, 376, 249, 499, 501, 751, 625, 875, 749, 999
$r=4$	0, 1, 625, 9376	0, 1, 3751, 624, 625, 4375, 9376, 1249, 4999, 5001, 8751, 5625, 9375, 6249, 9999

In einer zweiten Anwendung des Lemmas geben wir die Anzahl der Nachkommen einer idempotenten Zahl an, falls der Modul eine Primzahlpotenz ist.

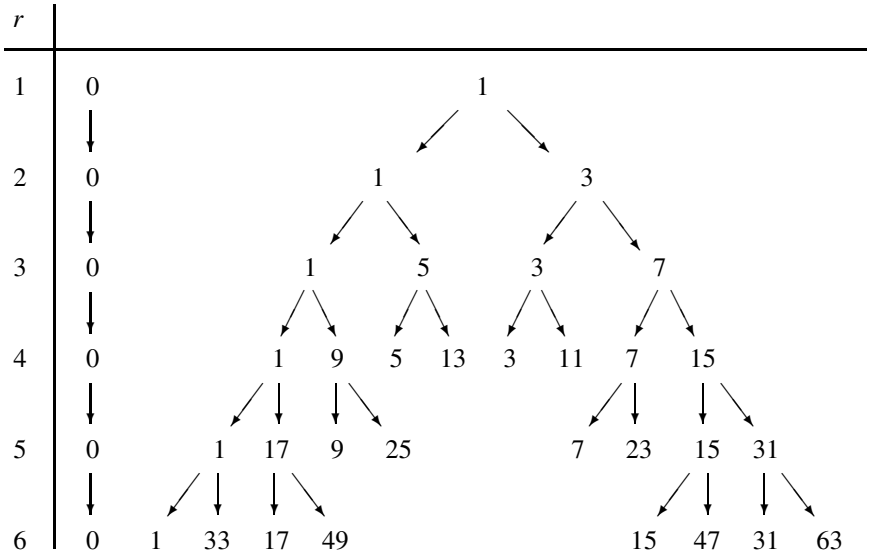
Satz 6. *Die Anzahl der Nachkommen einer idempotenten Zahl $n\in I^k(p^r)$ modulo einer Primzahlpotenz p^r ist*

$$\begin{aligned}
&1, \quad \textit{falls} \quad kn^{k-1}\not\equiv 1 \mod p,\\
&p, \quad \textit{falls} \quad kn^{k-1}\equiv 1 \mod p,\ n^k\equiv n \mod p^{r+1},\\
&0, \quad \textit{falls} \quad kn^{k-1}\equiv 1 \mod p,\ n^k\not\equiv n \mod p^{r+1}.
\end{aligned}$$

Beweis. Man wendet Lemma 4(b) auf das Polynom $f(X)=X^k-X$ an. □

Beispiel 3 Wir geben den „Stammbaum“ für $n^5\equiv n \mod 2^r$ an. Die Relation „ist Nachkomme von“ stellen wir durch einen Pfeil dar, und anstelle der Restklassen $\overline{n}$ geben wir ihre Vertreter n mit $0\le n<2^r$ an. Aus Satz 3 folgt $a^5(2^r)=1+2^3=9$ für $r\ge 4$.

Für $r \geq 4$ stehen also jeweils 9 Zahlen in der r-ten Zeile. Von den 8 Zahlen $\neq 0$ in der r-ten Zeile haben 4 keine Nachkommen, und die übrigen 4 Zahlen n haben die beiden Nachkommen n und $n + 2^r$. Verfolgt man eine von 0 und 1 verschiedene idempotente Zahl n im Stammbaum von oben nach unten, dann stirbt sie irgendwann aus, das heißt sie hat keinen Nachfolger mehr: Sie tritt letztmalig in der r-ten Zeile auf, wobei r durch $2^r \parallel (n^4 - 1)$ definiert ist.



5 Verwandte idempotente Zahlen

Wir betrachten Paare idempotenter Zahlen, die aus denselben Primteilern von g zusammengesetzt sind.

Definition. Zwei idempotente Zahlen $n_1 \in I^k(g^{r_1})$ und $n_2 \in I^k(g^{r_2})$ heißen *verwandt*, falls für alle Primteiler p von g gilt: Genau dann ist $p \,|n_1$, wenn $p \,|n_2$ ist. Wir nennen dann auch die Restklassen $\overline{n}_1, \overline{n}_2$ *verwandt*.

Für jedes k ist die Verwandtschaft offenbar eine Äquivalenzrelation auf $\bigcup_{r\geq 1} I^k(g^r)$ und auch auf jeder Menge $I^k(g^r)$, und der Begriff der Verwandtschaft von Restklassen ist wohldefiniert und eine Äquivalenzrelation auf $\bigcup_{r\geq 1} \overline{I}^k(g^r)$ und auf $\overline{I}^k(g^r)$. Diese Äquivalenzklassen nennen wir *Verwandtschaftsklassen*.

Es sei k ungerade und $n \in I^k(g^r)$. Dann sind die idempotenten Zahlen n und $\widetilde{n} = g^r - n \in I^k(g^r)$ verwandt. Denn für jede Nullstelle x ist auch $-x$ eine Nullstelle des Polynoms $X^k - X$, und offenbar teilen Primteiler p von g entweder beide Zahlen n und $\widetilde{n}$ oder keine davon. Für ungerade k zerfällt also $I^k(g^r) \setminus \left(g^r\mathbb{Z} \cup \left(\frac{1}{2}g^r + g^r\mathbb{Z}\right)\right)$ in Paare verwandter Zahlen. (Für ungerade g ist $\frac{1}{2}g^r + g^r\mathbb{Z}$ durch die leere Menge zu ersetzen.) Eine Verwandtschaftsklasse in $I^k(g^r)$ kann aus mehreren solchen Paaren bestehen. Die Tabelle in Beispiel 2 enthält Verwandtschaftsklassen, die aus 4 beziehungsweise 8 Zahlen bestehen.

Satz 7. *Es sei $k \geq 2$. Es bezeichne $\mathbb{P}_g$ die Menge der Primteiler von g und $\omega(g)$ die Anzahl der Elemente von $\mathbb{P}_g$. Dann gilt:*

(a) *Zu jedem $r \geq 1$ und zu jeder Teilmenge $Q \subseteq \mathbb{P}_g$ gibt es eine idempotente Zahl $n \in I^k(g^r)$ mit $\{p \in \mathbb{P}_g \mid p \mid n\} = Q$. Zu jeder idempotenten Zahl $n \in I^k(g^r)$ und zu jeder natürlichen Zahl $\widetilde{r} \geq r$ gibt es eine mit n verwandte Zahl $\widetilde{n} \in I^k(g^{\widetilde{r}})$; in jeder anderen Generation gibt es mit n verwandte idempotente Zahlen $\widetilde{n}$.*

(b) *Für jedes $r \geq 1$ besteht eine Bijektion zwischen den Verwandtschaftsklassen idempotenter Zahlen in $I^k(g^r)$ und der Menge aller Teilmengen von $\mathbb{P}_g$. Die Anzahl der Verwandtschaftsklassen ist $2^{\omega(g)}$.*

Beweis. Für $n \in I^k(g^r)$ setzen wir $Q(n) = \{p \in \mathbb{P}_g \mid p \mid n\}$. Aus der Definition verwandter idempotenter Zahlen folgt unmittelbar, dass $Q(\widetilde{n}) = Q(n)$ für alle mit n verwandten Zahlen $\widetilde{n} \in I^k(g^{\widetilde{r}})$ gilt. Desgleichen folgt $Q(n_1) \neq Q(n_2)$, falls $n_1 \in I^k(g^{r_1})$ und $n_2 \in I^k(g^{r_2})$ nicht miteinander verwandt sind. Also induziert $n \mapsto Q(n)$ eine injektive Abbildung zwischen den Verwandtschaftsklassen in $I^k(g^r)$ und den Teilmengen von $\mathbb{P}_g$.

Es sei eine Teilmenge $Q \subseteq \mathbb{P}_g$ gegeben. Diese bestimmt eine Zerlegung $g = qt$ mit natürlichen Zahlen q und t, worin q ein Potenzprodukt der Primzahlen $p \in Q$ ist und $p \nmid t$ für alle $p \in Q$ gilt. Insbesondere sind q und t teilerfremd. Zu jedem $r \geq 1$ gibt es also nach dem Chinesischen Restsatz eine ganze Zahl n mit $n \equiv 0 \mod q^r$ und $n \equiv 1 \mod t^r$. Es folgt $n^k \equiv 0 \equiv n \mod q^r$ und $n^k \equiv 1 \equiv n \mod t^r$, also $n^k \equiv n \mod g^r$, und somit ist $n \in I^k(g^r)$. Offenbar gilt $Q(n) = Q$. Damit ist eine Bijektion zwischen den Verwandtschaftsklassen und den Teilmengen von $\mathbb{P}_g$ gefunden. Die Anzahl dieser Teilmengen ist $2^{\omega(g)}$. Damit sind alle Behauptungen des Satzes bewiesen. – Zur leeren Teilmenge von $\mathbb{P}_g$ gehört die Verwandtschaftsklasse der idempotenten Zahl 1, und zur Menge $\mathbb{P}_g$ selber gehört die Klasse der idempotenten Zahl 0. □

Bemerkung. Mit ähnlichen Ideen wie im Beweis von Satz 7 findet man eine Parametrisierung von $\overline{I}^2(g^r)$: Jeder Teilmenge $Q \subseteq \mathbb{P}_g$ wird in diesem Beweis eine Zerlegung $g = qt$ zugeordnet. Man verifiziert nun, dass durch

$$Q \mapsto t^{r\varphi(q^r)} + g^r\mathbb{Z}$$

eine injektive Abbildung der Potenzmenge von $\mathbb{P}_g$ nach $\overline{I}^2(g^r)$ definiert ist; hierbei bezeichnet φ die Eulersche Funktion. Die Abbildung ist sogar bijektiv, weil die Anzahl $a^2(g^r) = 2^{\omega(g)}$ der Elemente der beiden Mengen nach Beispiel 1 gleich sind.

Satz 8. *Die idempotenten Zahlen $n \in I^k(g^r)$ und $\widetilde{n} \in I^k(g^{\widetilde{r}})$ seien verwandt, und es sei $r \leq \widetilde{r}$. Dann gilt*

$$n^{k-1} \equiv \widetilde{n}^{k-1} \mod g^r.$$

Im Ziffernsystem zur Basis g stimmen die $(k-1)$-ten Potenzen von n und $\widetilde{n}$ in den letzten r Ziffern überein.

Bemerkung. Der Spezialfall $k = 2$ ist [1, Satz 4]. – Für $k \geq 3$ ist die Aussage $n \equiv \widetilde{n} \mod g^r$ nicht immer wahr, wie die Zahlen $125 \in I^3(10^3)$ und $625 \in I^3(10^4)$ mit $625 \not\equiv 125 \mod 10^3$ in Beispiel 2 zeigen.

Beweis des Satzes. Wie im Beweis von Satz 7 zerlegen wir $g = qt$ in teilerfremde Faktoren q und t, worin q ein Potenzprodukt derjenigen Primteiler von g ist, die auch n (und somit auch $\widetilde{n}$) teilen. Aus $n^k \equiv n \mod g^r$ und $\widetilde{n}^k \equiv \widetilde{n} \mod g^{\widetilde{r}}$ folgt dann, da n und $\widetilde{n}$ teilerfremd zu t sind,

$$n \equiv 0 \mod q^r, \qquad n^{k-1} \equiv 1 \mod t^r,$$
$$\widetilde{n} \equiv 0 \mod q^{\widetilde{r}}, \qquad \widetilde{n}^{k-1} \equiv 1 \mod t^{\widetilde{r}},$$

also $n \equiv \widetilde{n} \mod q^r$ und $n^{k-1} \equiv \widetilde{n}^{k-1} \mod t^r$. Somit folgt $n^{k-1} \equiv \widetilde{n}^{k-1} \mod g^r$. □

6 Komplementäre idempotente Zahlen

Wir diskutieren eine Eigenschaft idempotenter Zahlen, die zur Verwandtschaft komplementär ist.

Definition. Zwei idempotente Zahlen $n_1 \in I^k(g^{r_1})$ und $n_2 \in I^k(g^{r_2})$ heißen *komplementär*, falls für alle Primteiler p von g gilt: Genau dann ist $p \mid n_1$, wenn $p \nmid n_2$ ist.

Korollar 9. *Es sei $n \in I^k(g^r)$ und $k \geq 2$. Zu jeder natürlichen Zahl $\widetilde{r}$ gibt es dann eine zu n komplementäre idempotente Zahl $\widetilde{n} \in I^k(g^{\widetilde{r}})$.*

Beweis. Wie im Beweis von Satz 7 bezeichne $Q(n)$ die Menge der gemeinsamen Primteiler von g und n, und es sei $T(n) = \mathbb{P}_g \setminus Q(n)$ die Menge der Primteiler p von g mit $p \nmid n$. Nach Satz 7(a) gibt es zu jeder natürlichen Zahl $\widetilde{r}$ ein $\widetilde{n} \in I^k(g^{\widetilde{r}})$ mit $Q(\widetilde{n}) = T(n)$. Diese Zahl $\widetilde{n}$ ist komplementär zu n. □

Bemerkung. Nach Satz 7 ist die Verwandtschaftsklasse einer zu n komplementären Zahl $\widetilde{n}$, nicht jedoch $\widetilde{n}$ selber, eindeutig durch n bestimmt. Beispiele entnimmt man der Liste in Beispiel 2.

Satz 10. *Es sei $k \geq 2$. Die Zahlen n_1 und n_2 in $I^k(g^r)$ seien komplementär. Dann gilt*

$$n_1^{k-1} + n_2^{k-1} \equiv 1 \mod g^r,$$
$$n_1 n_2 \equiv 0 \mod g^r.$$

Beweis. Für $n \in I^k(g^r)$ seien $Q(n)$ und $T(n)$ wie im Beweis von Korollar 9 erklärt. Dann gilt $Q(n_1) = T(n_2)$, $Q(n_2) = T(n_1)$, und es besteht eine Zerlegung $g = qt$ in teilerfremde Faktoren q und t, worin q nur Primteiler in $Q(n_1)$ und t nur Primteiler in $Q(n_2)$ hat. Aus den Voraussetzungen folgt $q^r t^r \mid n_1(n_1^{k-1} - 1)$ und $q^r t^r \mid n_2(n_2^{k-1} - 1)$, und somit

$$n_1 \equiv 0 \mod q^r, \quad n_1^{k-1} \equiv 1 \mod t^r, \quad n_2 \equiv 0 \mod t^r, \quad n_2^{k-1} \equiv 1 \mod q^r.$$

Wegen der Teilerfremdheit von q und t ist damit die zweite Behauptung klar, und wegen $n_1^{k-1} \equiv n_1 \equiv 0 \mod q^r$, $n_2^{k-1} \equiv n_2 \equiv 0 \mod t^r$ folgt auch die erste Behauptung. □

Beispiel 4 Es sei $k = 2$, und wir nehmen $n_j \in I^k(g^r)$ mit $1 \leq n_j < g^r$ für $j = 1, 2$ an. Aus Satz 10 folgt dann $n_1 + n_2 = g^r + 1$, und im Ziffernsystem zur Basis g ist $n_1 + n_2 = 100\ldots01$ und $n_1 n_2 = *\ldots*00\ldots0$ mit $r - 1$ beziehungsweise r Nullen ([1, Satz 6]). Insbesondere gibt es zu jeder Zahl $n \in I^2(g^r)$ im Intervall $1 \leq n < g^r$ genau eine komplementäre Zahl in diesem Intervall.

7 Gemeinschaften idempotenter Zahlen

In diesem Abschnitt verallgemeinern wir die Aussagen über zwei komplementäre Zahlen auf mehrere solche Zahlen.

Definition. Es sei $m \geq 2$. Die idempotenten Zahlen $n_1, n_2, \ldots, n_m \in I^k(g^r)$ bilden eine *Gemeinschaft der Größe m*, falls die Mengen $T_j = T(n_j) = \left\{p \in \mathbb{P}_g \;\middle|\; p \nmid n_j\right\}$ für $j = 1, \ldots, m$ eine Zerlegung von $\mathbb{P}_g$ in disjunkte Teilmengen bilden.

Beispielsweise bilden zwei komplementäre Zahlen eine Zweier-Gemeinschaft. Die Zahlen 6, 10, 15 in $I^2(30)$ bilden eine Dreier-Gemeinschaft. Eine triviale Gemeinschaft ist 1, 0, ..., 0. Wir zeigen, dass es in jeder Menge $I^k(g^r)$ nicht-triviale kleine Gemeinschaften gibt:

Satz 11. *In jeder Menge $I^k(g^r)$ existiert eine Gemeinschaft der Größe m aus paarweise verschiedenen Zahlen, falls $2 \leq m \leq \omega(g) + 1$ ist.*

Beweis. Wegen $m \leq \omega(g)+1$ gibt es eine Zerlegung von $\mathbb{P}_g$ in m verschiedene, paarweise disjunkte Teilmengen $T_1, \ldots, T_m$. (Beispielsweise kann $T_1, \ldots, T_{m-1}$ aus jeweils einem Primteiler und T_m aus den restlichen Primteilern von g bestehen.) Zu jedem $j = 1, \ldots, m$ wähle man nach Satz 7(a) eine idempotente Zahl $n_j \in I^k(g^r)$ mit $Q(n_j) = \mathbb{P}_g \setminus T_j$. Diese Zahlen $n_1, \ldots, n_m$ bilden eine Gemeinschaft. Wir zeigen, dass sie paarweise verschieden sind: Für $j \neq l$ ist $T_j \neq T_l$. Es gibt also einen Primteiler p von g, der genau einer dieser Mengen angehört, und wir dürfen $p \in T_j$, $p \notin T_l$ annehmen. Es folgt $p | n_l$, $p \nmid n_j$, also $n_j \neq n_l$. □

Es besteht die folgende Verallgemeinerung von Satz 10:

Satz 12. *Es sei $k \geq 2$, und $n_1, n_2, \ldots, n_m$ sei eine Gemeinschaft der Größe m in $I^k(g^r)$. Dann gilt*

$$\begin{aligned} n_1^{k-1} + n_2^{k-1} + \ldots + n_m^{k-1} &\equiv 1 \mod g^r, \\ n_\mu n_\nu &\equiv 0 \mod g^r \end{aligned}$$

für alle Indizes $\mu \neq \nu$.

Beweis. Zu jedem $p \in \mathbb{P}_g$ gibt es genau einen Index μ mit $p \in T_\mu$ und $p \notin T_\nu$ für alle $\nu \neq \mu$. Es sei $p^\alpha \parallel g$. Dann gilt $p^{\alpha r} | (n_\mu^k - n_\mu)$, und wegen $p \nmid n_\mu$ folgt $p^{\alpha r} | (n_\mu^{k-1} - 1)$, also $n_\mu^{k-1} \equiv 1 \mod p^{\alpha r}$. Für alle $\nu \neq \mu$ gilt $p | n_\nu$ und $p^{\alpha r} | (n_\nu^k - n_\nu)$, und hieraus folgt $p^{\alpha r} | n_\nu$, also $n_\nu \equiv 0 \mod p^{\alpha r}$ und somit auch $n_\nu^{k-1} \equiv 0 \mod p^{\alpha r}$. Aufsummieren ergibt $n_1^{k-1} + n_2^{k-1} + \ldots + n_m^{k-1} \equiv 1 \mod p^{\alpha r}$. Das gilt für alle $p \in \mathbb{P}_g$, und somit folgt die erste Behauptung.

Es seien Indizes $\mu \neq \nu$ gegeben, und es sei $p \in \mathbb{P}_g$, $p^\alpha \parallel g$. Dann gilt $p \notin T_\mu$ oder $p \notin T_\nu$. Es genügt, den Fall $p \notin T_\nu$ zu diskutieren. Wie im ersten Teil des Beweises folgt dann $n_\nu \equiv 0 \mod p^{\alpha r}$. Hieraus folgt auch $n_\mu n_\nu \equiv 0 \mod p^{\alpha r}$. Das gilt für alle $p \in \mathbb{P}_g$, und somit folgt die zweite Behauptung. □

Literatur

[1] Groß, C.: Idempotente (automorphe) Zahlen in q-Stellenwertsystemen. *Math. Semesterber.* 52 (2005), 127–151.

[2] Remmert, R.; Ullrich, P.: *Elementare Zahlentheorie*. Birkhäuser, 1987.

Günter Köhler
Universität Würzburg
Mathematisches Institut
Am Hubland
D-97074 Würzburg, Deutschland
e-mail: koehler@mathematik.uni-wuerzburg.de

Jürgen Spilker
Albert-Ludwigs-Universität Freiburg
Mathematisches Institut
Eckerstr. 1
D-79104 Freiburg, Deutschland
e-mail: spilker@mathematik.uni-freiburg.de