Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 32 (1977)
Heft: 5

Artikel: Bemerkungen über gewisse nichtlineare Kongruenzen
Autor: Rieger, G.J.
DOI: https://doi.org/10.5169/seals-32161

Bemerkungen über gewisse nichtlineare Kongruenzen

Für $m \in \mathbf{N}, a \in \mathbf{Z}, (a,m)=1$ sei $g(a;m)$ die kleinste Zahl aus $\mathbf{N}$ mit $a^{g(a;m)} \equiv 1 \bmod m$; mit der φ-Funktion von Euler gilt

$$g(a;m) \mid \varphi(m), \tag{1}$$

und für $n \in \mathbf{N}$ mit $n \mid m$ gilt

$$g(a;n) \mid g(a;m). \tag{2}$$

Das letzte Kapitel des interessanten Buches «Sieve methods, Cambridge 1976» von C. Hooley gab den Anlass zu diesen Überlegungen.
Wir beginnen mit Beispielen. Wie verteilen sich die Zahlen der Folge $(2^x + x : x \geq 0)$ auf die Restklassen mod m? Es sei etwa $m=5$; wegen $g(2;5)=4$ hat die Folge $(2^x \bmod 5 : x \geq 0)$ die Periode 4; daher hat die Folge $(2^x + x \bmod 5 : x \geq 0)$ die Periode $[5,4]=20$; für $0 \leq x < 20$ gibt aber $2^x + x$ bei Division mit 5 die Reste 1, 3, 1, 1, 0, 2, 0, 0, 4, 1, 4, 4, 3, 0, 3, 3, 2, 4, 2, 2; man stellt fest, dass jeder Rest gleich oft (und zwar 20/5-mal) vorkommt. Jetzt sei etwa $m=7$; wegen $g(2;7)=3$ hat die Folge $(2^x + x \bmod 7 : x \geq 0)$ die Periode 21; für $0 \leq x < 21$ gibt $2^x + x$ bei Division mit 7 die Reste 1, 3, 6, 4, 6, 2, 0, 2, 5, 3, 5, 1, 6, 1, 4, 2, 4, 0, 5, 0, 3; wieder kommt jeder Rest gleich oft vor. Wie verteilen sich die Zahlen der Folge $(2^x + 3^x + x : x \geq 0)$ auf die Restklassen mod m? Es sei etwa $m=7$; wegen $g(2;7)=3$ und $g(3;7)=6$ hat die Folge $(2^x + 3^x + x \bmod 7 : x \geq 0)$ die Periode $[7,3,6]=42$; für $0 \leq x < 42$ gibt $2^x + 3^x + x$ bei Division mit 7 die Reste 2, 6, 1, 3, 3, 0, 1, 5, 0, 2, 2, 6, 0, 4, 6, 1, 1, 5, 6, 3, 5, 0, 0, 4, 5, 2, 4, 6, 6, 3, 4, 1, 3, 5, 5, 2, 3, 0, 2, 4, 4, 1; wieder kommt jeder Rest gleich oft vor. Das soll jetzt allgemein bewiesen werden.

Satz 1. *Es sei* $s \in \mathbf{N}$, $a_j \in \mathbf{Z}\ (1 \leq j \leq s)$, $b_j \in \mathbf{Z}\ (1 \leq j \leq s)$, $0 \neq a \in \mathbf{Z}$, $m \in \mathbf{N}$, $(m, b_1 \cdots b_s a)=1$, $h(m) := [g(b_1;m), \ldots, g(b_s;m)]$; *für* $x \in \mathbf{Z}$ *mit* $0 \leq x < [m, h(m)]$ *liefert* $a_1 b_1^x + \cdots + a_s b_s^x + a x$ *jeden Rest mod* m *gleich oft und damit genau* $[m, h(m)]/m$*-mal.*

Beweis (Induktion nach m): Wegen $g(b_j;m) \mid \varphi(m)\ (1 \leq j \leq s)$ nach (1) ist $h(m) \mid \varphi(m)$. Es sei $P(x) := a_1 b_1^x + \cdots + a_s b_s^x$. Für gegebenes $b \in \mathbf{Z}$ betrachten wir

$$P(x) + a x \equiv b \bmod m. \tag{3}$$

Für $m=1$ ist nichts zu beweisen. Es sei $m > 1$. Für $n := (m, h(m))$ gilt $n \mid m, (n, b_1 \cdots b_s a)=1$ und wegen $h(m) \leq \varphi(m) < m$ noch $0 < n < m$. Nach Induktionsvoraussetzung gibt es paarweise verschiedene Zahlen $x_j \in \mathbf{Z}\ (1 \leq j \leq ([n, h(n)]/n))$ mit $P(x_j) + a x_j \equiv b \bmod n$ und

$$0 \leq x_j < [n, h(n)]. \tag{4}$$

Es ist hinreichend, die Behauptung für m mit «mindestens» statt «genau» zu beweisen. Es sei $x_{j,t} := x_j + t[n, h(n)]\ [0 \leq t < (h(m)/[n, h(n)])]$; wegen $g(b_j;n) \mid g(b_j;m)$

$(1 \leq j \leq s)$ nach (2) ist $h(n) \mid h(m)$, und wegen $n \mid h(m)$ folgt $h(m)/[n, h(n)] \in \mathbf{N}$. Man prüft sofort, dass die $x_{j,t}$ paarweise verschieden sind und dass gilt

$$0 \leq x_{j,t} < h(m). \tag{5}$$

Für $x \equiv y \bmod h(n)$ ist $P(x) \equiv P(y) \bmod n$ termweise; für $x \equiv y \bmod n$ ist $ax \equiv ay \bmod n$; für $x \equiv y \bmod [n, h(n)]$ ist folglich $P(x) + ax \equiv P(y) + ay \bmod n$. Das ergibt

$$P(x_{j,t}) + a x_{j,t} \equiv P(x_j) + a x_j \equiv b \bmod n.$$

Wegen $(a, m) = 1$ ist $n = (m, a h(m))$. Also gibt es Zahlen $y_{j,t} \in \mathbf{N}$, $z_{j,t} \in \mathbf{Z}$ mit

$$P(x_{j,t}) + a x_{j,t} - b = m z_{j,t} - a h(m) y_{j,t}. \tag{6}$$

Es sei $r_{j,t} := x_{j,t} + h(m) y_{j,t}$. Für $x \equiv y \bmod h(m)$ ist $P(x) \equiv P(y) \bmod m$ termweise. Aus (6) folgt daher

$$P(r_{j,t}) + a r_{j,t} \equiv b \bmod m,$$

und (3) ist gelöst. Die $r_{j,t}$ erweisen sich aber als paarweise inkongruent mod $[m, h(m)]$; denn aus $r_{j,t} \equiv r_{i,v} \bmod [m, h(m)]$ folgt $x_{j,t} \equiv x_{i,v} \bmod h(m)$ und wegen (5) daraus

$$x_{j,t} = x_{i,v} \tag{7}$$

und daraus $x_j \equiv x_i \bmod [n, h(n)]$ und wegen (4) daraus $j = i$ und wegen (7) daraus $t = v$. Die Anzahl der $r_{j,t}$ ist aber

$$\frac{[n, h(n)]}{n} \frac{h(m)}{[n, h(n)]} = \frac{[m, h(m)]}{m}.$$

Dieser Beweis erlaubt es noch, in Satz 1 den Exponenten x von b_j durch ein Polynom $F_j(x) \in \mathbf{Z}[x]$ mit $F_j(x) \geq 0 (x \geq 0)$ zu ersetzen $(1 \leq j \leq s)$.

Satz 2. *Es sei* $s \in \mathbf{N}$, $a_j \in \mathbf{Z} (1 \leq j \leq s)$, $b_j \in \mathbf{Z} (1 \leq j \leq s)$, $b \in \mathbf{Z}$, $0 \neq a \in \mathbf{Z}$, $m \in \mathbf{N}$, $(m, b_1 \cdots b_s a) = 1$; *$h(m)$ und $P(x)$ seien wie oben erklärt; für $\sigma \in \mathbf{R}$ bezeichne $A(\sigma)$ die Anzahl der $x \in \mathbf{N}$ mit $x \leq \sigma$ und $P(x) + ax \equiv b \bmod m$; für $0 \leq \sigma \in \mathbf{R}$ gilt dann*

$$\left| A(\sigma) - \frac{\sigma}{m} \right| < \frac{[m, h(m)]}{m} \left(< \varphi(m) \right).$$

Beweis: Es sei $M := [m, h(m)]$, $B := M/m$. Wie im Anschluss an (5) folgt, dass die Funktion $x \mapsto P(x) + ax \bmod m (0 \leq x \in \mathbf{Z})$ die Periode M hat. Wir unterteilen das Intervall von 0 bis σ mit Hilfe der Vielfachen von M. Ist σ ein Vielfaches von M, entstehen dabei genau σ/M Intervalle der Länge M, und Satz 1 liefert $A(\sigma) = (\sigma/M) B = \sigma/m$. Ist σ kein Vielfaches von M, entstehen dabei $[\sigma/M]$ Intervalle der Länge M und noch ein Intervall von einer Länge $< M$, und Satz 1 liefert $A(\sigma)$

$=[\sigma/M]\,B+\theta\,B$ für ein gewisses $\theta\in\mathbf{R}$ mit $0\leq\theta\leq 1$, wobei wir noch $\sigma/M-1<[\sigma/M]<\sigma/M$ beachten.
Durch Satz 2 wird die Siebmethode anwendbar auf die Folge $(P(x)+a\,x:x\geq 0)$.
In ähnlicher Weise behandelt man andere Folgen wie $(x\,a^x:x\geq 0)$ mit $a\in\mathbf{Z}$; statt (6) hat man

$$x_{j,t}\,a^{x_{j,t}}-b=m\,z_{j,t}-a^{x_{j,t}}\,g\,(a;m)\,y_{j,t}$$

mit $m\in\mathbf{N}$, $(m,a)=1$.
Für Folgen wie etwa $(2^x+x^2:x\geq 0)$ oder $(x^2\,2^x:x\geq 0)$ fehlen uns befriedigende Ergebnisse. Stets ist $2^x+x^2\not\equiv 0 \bmod 7$.

G. J. Rieger, Technische Universität Hannover

Kleine Mitteilungen

Zur Abwicklung des schiefen Kreiskegels

Ein schiefer Kreiskegel, festgelegt durch seinen Basisradius r, die Höhe Z und die Exzentrizität $X>0$ des Höhenfusspunktes, erfordert bekanntlich zur exakten Verebnung seines Mantels elliptische Integrale [1]. In der Praxis behilft man sich daher mit der Ausbreitung des Mantels einer eingeschriebenen Ersatzpyramide mit hinreichend vielen Kanten. Für die Aneinanderreihung der auftretenden Teildreiecke benötigt man dabei die Längen der Mantelkanten. Obwohl diese «wahren Längen» mit Hilfe der ersten Massaufgabe der darstellenden Geometrie leicht zu ermitteln sind [2], soll hier ein anderes Verfahren auseinandergesetzt werden, das nicht unmittelbar auf der Hand liegt, aber ebenfalls sehr einfach und vielleicht etwas übersichtlicher zu handhaben ist.
Setzt man unter Verwendung kartesischer Koordinaten den Basiskreis k durch

$$x=r\cos u\,,\qquad y=r\sin u\,,\qquad z=0 \tag{1}$$

an, so ergibt sich die Entfernung R eines Basispunktes $P(x,y,0)$ von der Kegelspitze $Q(X,0,Z)$ in Abhängigkeit vom Parameter u aus

$$R^2=(X-r\cos u)^2+(r\sin u)^2+Z^2=X^2+Z^2+r^2-2\,rX\cos u\,. \tag{2}$$

Hieraus ist zu ersehen, dass dieselben Erzeugendenlängen nicht nur auf dem Ausgangskegel vorhanden sind, sondern in gleicher Verteilung auch noch auf unendlich vielen weiteren Kegeln, wenn bloss die Angabestücke den Bedingungen

$$rX=a^2\,,\qquad X^2+Z^2+r^2=b^2 \tag{3}$$

mit Konstanten a und b genügen.