

Kleine Mitteilungen

Objektyp: **Group**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **35 (1980)**

Heft 3

PDF erstellt am: **22.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

<http://www.e-periodica.ch>

LITERATURVERZEICHNIS

- 1 G. Birkhoff und S. Mac Lane: A Survey of modern Algebra, 4. Aufl. New York, London 1977.
- 2 M. Jeger: Algorithmische Kombinatorik auf der Stufe programmierbarer Taschen-Rechner. ZAMP, Heft 2, S.243–260 (1979).
- 3 R. Kochendörffer: Einführung in die Algebra, 4. Aufl. Berlin 1974.
- 4 W. Krull: Elementare und klassische Algebra vom modernen Standpunkt, Band I. Sammlung Götschen, Bd.930, 3. Aufl. Berlin 1963.
- 5 N. Obreschkoff: Verteilung und Berechnung der Nullstellen reeller Polynome. Berlin 1963.
P. Henrici: Applied and computational complex Analysis. New York, London, Sydney, Toronto 1974.

Kleine Mitteilungen

Der Wolstenholmesche Satz

Sei p eine Primzahl > 3 . Definiert man

$$f(x) = (x-1)(x-2)\cdots(x-p+1),$$

so ist $f(0) = (p-1)! = f(p)$. Durch elementare Multiplikation hat man

$$f(x) = x^{p-1} - A_1 x^{p-2} + A_2 x^{p-3} - \cdots - A_{p-2} x + (p-1)! \quad (1)$$

Da $1, 2, \dots, p-1$ genau die Wurzeln der Kongruenz $x^{p-1} \equiv 1 \pmod{p}$ sind, so folgt aus (1)

$$x^{p-1} - 1 \equiv x^{p-1} - A_1 x^{p-2} + A_2 x^{p-3} - \cdots - A_{p-2} x + (p-1)! \pmod{p}. \quad (2)$$

Man erhält sofort den *Wilsonschen Satz* $(p-1)! \equiv -1 \pmod{p}$ und ferner (für jedes x)

$$-A_1 x^{p-2} + A_2 x^{p-3} - \cdots - A_{p-2} x \equiv 0 \pmod{p}.$$

Deshalb ist

$$p \mid A_1, A_2, \dots, A_{p-2}. \quad (3)$$

Weiterhin hat man durch Differentiation

$$f'(x) = (x-2)\cdots(x-p+1) + \cdots + (x-1)\cdots(x-p+2)$$

und daraus

$$f'(0) = -f'(p) = -\{1 \cdot 2 \cdots (p-2) + \cdots + 2 \cdot 3 \cdots (p-1)\}.$$

Der Taylorsche Satz gibt:

$$f(x) = f(0) + \frac{x}{1!} f'(0) + \frac{x^2}{2!} f''(0) + \dots + \frac{x^{p-1}}{(p-1)!} f^{(p-1)}(0).$$

Wegen $f(p) = f(0)$ ergibt sich

$$0 = f'(0) + \frac{p}{2} f''(0) + \dots + \frac{p^{p-2}}{(p-1)!} f^{(p-1)}(0). \quad (4)$$

Nun ist $f''(0)/2 = A_{p-3}$, und wegen (3) gilt deshalb $p \mid f''(0)$.

Unter Benutzung von (4) findet man jetzt

$$p^2 \mid f'(0). \quad (5)$$

Weiter hat man

$$\frac{-f'(0)}{(p-1)!} = \frac{1}{p-1} + \frac{1}{p-2} + \dots + 1. \quad (6)$$

Der Zähler der auf der rechten Seite von (6) stehenden Summe ist also wegen (5) durch p^2 teilbar, und das ist der Satz von Wolstenholm.

Bemerkung 1: Dieser Beweis des Wolstenholmeschen Satzes ist verschieden von allen von mir in der Literatur gefundenen Beweisen.

Bemerkung 2: Ist p eine Primzahl > 5 , so gilt der folgende Satz: Addiert man die reziproken 3-Kombinationen von $1, 2, \dots, p-1$

$$\frac{1}{1 \cdot 2 \cdot 3} + \frac{1}{1 \cdot 2 \cdot 4} + \frac{1}{1 \cdot 2 \cdot 5} + \dots + \frac{1}{(p-3)(p-2)(p-1)},$$

so ist der Zähler der Summe durch p^2 teilbar.

Beweis: Benutzt man die Taylorsche Formel

$$f'''(x) = f'''(0) + x f^{(4)}(0) + \frac{x^2}{2} f^{(4)}(0) + \dots + \frac{x^{p-3}}{(p-3)!} f^{(p-1)}(0),$$

so erhält man, da $f'''(p) = f'''(0)$,

$$0 = f^{(4)}(0) + \frac{p}{2} f^{(4)}(0) + \dots + \frac{p^{p-4}}{(p-3)!} f^{(p-1)}(0). \quad (7)$$

Da $f^{(4)}(0)/4! = A_{p-5}$, hat man wegen (3) $p \mid f^{(4)}(0)$ und wegen (7) $p^2 \mid f^{(4)}(0)$. Weiterhin ist $f^{(4)}(0) = -2 \cdot 3 \cdot \sum 1 \cdot 2 \cdot \dots \cdot (p-4)$, wo die Summe über alle $(p-4)$ -Kombinationen von $1, 2, \dots, p-1$ erstreckt ist. Hieraus folgt

$$-\frac{f'''(0)}{2 \cdot 3(p-1)!} = \frac{1}{1 \cdot 2 \cdot 3} + \cdots + \frac{1}{(p-3)(p-2)(p-1)} \equiv 0 \pmod{p^2}.$$

L. Kuipers, Mollens

Aufgaben

Aufgabe 822. Es sei $a \equiv 2 \pmod{3}$ and $a+1$ genau durch 3^s ($s \geq 1$) teilbar. Man bestimme für beliebiges $k \in \mathbf{N}_0$ die Ordnung der Restklasse von a in der primen Restklassengruppe $\text{mod } 3^{s+k}$.
L. Kuipers, Mollens

Lösung: Es ist die kleinste der natürlichen Zahlen m gesucht, für die

$$a^m \equiv 1 \pmod{3^{s+k}}$$

gilt. Bezeichnen wir sie mit $b(k)$, so ist sicher $b(k)$ ein Teiler von $\varphi(3^{s+k}) = 2 \cdot 3^{s-1+k}$. Wäre $b(k)$ ungerade, so ergäbe sich aus $a \equiv -1 \pmod{3}$ der Widerspruch

$$1 \equiv a^{b(k)} \equiv -1 \pmod{3}.$$

Also hat $b(k)$ die Form

$$b(k) = 2 \cdot 3^{c(k)} \quad \text{mit } c(k) \geq 0.$$

Schreibt man nun

$$a = -1 + 3^s u \quad \text{mit } 3 \nmid u.$$

so behaupten wir, dass für jedes $k \geq 0$

$$a^{2 \cdot 3^k} = 1 - 2u \cdot 3^{s+k} + v(k) \cdot 3^{s+k+1} \quad \text{mit } v(k) \in \mathbf{Z} \quad (*)$$

gilt. Für $k=0$ ist dies evident; wird $(*)$ für ein $k \geq 0$ als richtig angenommen, so bestätigt man ihre Gültigkeit für $k+1$ durch Erheben in die dritte Potenz und Berechnung der wesentlichen Summanden rechts. Aus $(*)$ liest man unmittelbar $c(k) \leq k$ für alle $k \geq 0$ ab. Wir zeigen nun $c(k) = k$ für alle $k \geq 0$ und haben damit die Aufgabe gelöst. Aus

$$a^{2 \cdot 3^{c(k)}} = 1 + A \cdot 3^{s+k} \quad \text{mit } A \in \mathbf{Z}$$

folgt

$$a^{2 \cdot 3^k} = (1 + A \cdot 3^{s+k})^{3^{k-c(k)}} = 1 + B \cdot 3^{s+2k-c(k)} \quad \text{mit } B \in \mathbf{Z}.$$