

Simultanbeweis des Fermatschen und Wilsonschen Satzes

Autor(en): **Stöwener, F.**

Objektyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **30 (1975)**

Heft 2

PDF erstellt am: **11.05.2021**

Persistenter Link: <http://doi.org/10.5169/seals-30647>

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.

und

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > n \cdot \frac{1}{\sqrt{n}} = \sqrt{n}$$

kann man die noch einfachere Reihe

$$1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{3} + \frac{1}{3} + \frac{1}{3} + \frac{1}{4} + \cdots$$

verwenden, wo $\frac{1}{4}$ viermal vorkommt und allgemein $\frac{1}{n}$ n -mal vorkommt. Man erhält aus dieser sofort auch die einfache bedingt konvergente Reihe

$$1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{2} - \frac{1}{2} + \frac{1}{3} - \frac{1}{3} + \frac{1}{3} - \frac{1}{3} + \frac{1}{3} - \frac{1}{3} + \frac{1}{3} - \frac{1}{3} + \cdots,$$

wobei wieder $\frac{1}{n} - \frac{1}{n}$ genau n -mal angeschrieben werden soll. Dass eine bedingt konvergente Reihe bei einer Umordnung mit einer anderen Summe konvergent werden kann, bereitet dem Schüler Schwierigkeiten beim Verständnis, weil Beispiele dazu oft etwas kompliziert sind. Das folgende Beispiel scheint mir recht einfach zu sein. Offenbar hat die Reihe

$$1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{2} - \frac{1}{2} + \frac{1}{4} - \frac{1}{4} + \frac{1}{4} - \frac{1}{4} + \frac{1}{4} - \frac{1}{4} + \frac{1}{4} - \frac{1}{4} + \frac{1}{8} - \frac{1}{8} + \cdots$$

die Summe Null. Ordnen wir sie ein wenig anders, so entsteht die Reihe

$$-1 + 1 - \frac{1}{2} - \frac{1}{2} + \frac{1}{2} - \frac{1}{4} - \frac{1}{4} + \frac{1}{2} - \frac{1}{4} - \frac{1}{4} + \frac{1}{4} - \frac{1}{8} - \frac{1}{8} + \cdots$$

wo $\frac{1}{4} - \frac{1}{8} - \frac{1}{8}$ viermal angeschrieben werden soll und dann $\frac{1}{8} - \frac{1}{16} - \frac{1}{16}$ achtmal usw. Diese Reihe hat offensichtlich die Summe (-1) , also eine Summe $\neq 0$. Natürlich ist es leicht, auch eine divergente Reihe zu erhalten:

$$1 - 1 + \frac{1}{2} + \frac{1}{2} - \frac{1}{2} - \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} - \frac{1}{4} - \frac{1}{4} - \frac{1}{4} - \frac{1}{4} + \frac{1}{8} + \cdots$$

K. Prachar, Wien

Simultanbeweis des Fermatschen und Wilsonschen Satzes

Der Fermatsche Satz $a^{p-1} \equiv 1 \pmod{p}$ und die Wilsonsche Kongruenz $(p-1)! \equiv -1 \pmod{p}$ gestatten einen einfachen gemeinsamen Beweis, der ihren inneren Zusammenhang durch eine interessante Identität (1) erkennen lässt.

Sei p eine Primzahl, $a \not\equiv 0 \pmod{p}$ eine beliebige ganze Zahl und $a_i = a/i$; $1 \leq i \leq p-1$. Dann gilt

$$a_1 (a_1 - a_2) (a_1 - a_3) \dots (a_1 - a_{p-1}) \\ = \frac{a}{1} \frac{a(2-1)}{2} \frac{a(3-1)}{3} \dots \frac{a(p-2)}{p-1} = \frac{a^{p-1}}{p-1}$$

oder

$$[a_1 (a_1 - a_2) (a_1 - a_3) \dots (a_1 - a_{p-1})] (p-1) = a^{p-1}. \quad (1)$$

Die $p-1$ Faktoren in der eckigen Klammer sind mod p ganz und offensichtlich nicht durch p teilbar. Sie sind paarweise inkongruent, denn aus $a_1 \equiv a_1 - a_x$ würde sich $a_x \equiv 0$ und daraus $a \equiv 0$ ergeben, und aus $a_1 - a_x \equiv a_1 - a_y$ würde $a_x \equiv a_y$ und daraus $x \equiv y$ folgen. Das Produkt von $p-1$ paarweise inkongruenten Faktoren, die nicht durch p teilbar sind, ist $\equiv (p-1)!$. Nach (1) gilt somit

$$-(p-1)! \equiv a^{p-1} \pmod{p}. \quad (2)$$

Die Kongruenz (2) gilt entsprechend unserer Voraussetzung für jede beliebige ganze Zahl $a \not\equiv 0 \pmod{p}$. Wegen $1 \equiv 1^{p-1}$ folgt daher aus (2)

$$1 \equiv 1^{p-1} \equiv -(p-1)! \equiv a^{p-1} \pmod{p}.$$

Damit sind beide Titelsätze simultan bewiesen.

F. Stöwener, Mannheim

Aufgaben

Aufgabe 713. Give a proof of

$$c(m, n) = \sum_{\substack{d|n \\ d|m}} \mu\left(\frac{n}{d}\right) d,$$

where

$$c(m, n) := \sum_{\substack{1 \leq h \leq n \\ (h, n) = 1}} \exp\left(\frac{2\pi i h m}{n}\right),$$

using only the formula

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

D. Suryanarayana, Waltair, India

Lösung: Wir gehen von der bekannten Formel

$$\sum_{k=1}^d \exp\left(2\pi i k \frac{m}{d}\right) = \begin{cases} d & \text{falls } d | m \\ 0 & \text{falls } d \nmid m \end{cases}$$