Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 18 (1963)
Heft: 5

Rubrik: Kleine Mitteilungen

Kleine Mitteilungen

Kleine Bemerkung zum Wilsonschen Satz

Seit langem ist es üblich, den Fermatschen Satz in Vorlesungen über Algebra und Zahlentheorie als rein gruppentheoretischen Satz zu bringen. Dass dasselbe auch für den Wilsonschen Satz leicht möglich ist, scheint weniger geläufig zu sein.

Satz 1: In einer Abelschen Gruppe bilden die involutorischen Elemente zusammen mit dem Einselement 1 eine Untergruppe.

Satz 2: Das Produkt aller Elemente einer endlichen Gruppe G aus lauter involutorischen Elementen ausser der 1 ist das Einselement, ausser wenn G genau zwei Elemente hat.

Der Beweis ergibt sich, da eine solche Gruppe elementarabelsch ist, ganz leicht. Die Gruppenordnung sei 2^m. Ist U eine Untergruppe vom Index 2, also von der Ordnung 2^{m-1}, und $v \notin U$, so durchlaufen die Elemente $u \in U$ und $u'v$ mit $u' \in U$ alle Elemente von G. Ihr Produkt ist v im Fall $m = 1$ und 1 in jedem anderen Fall.

Satz 3: Das Produkt aller Elemente einer endlichen abelschen Gruppe G ist gleich dem Produkt ihrer involutorischen Elemente.

Die von 1 und den involutorischen Elementen verschiedenen $x \in G$ lassen sich nämlich zu Paaren x, x^{-1} zusammenfassen, deren Produkt 1 ist.

Satz 4: Das Produkt aller Elemente einer endlichen abelschen Gruppe G ist 1, ausser wenn G genau ein involutorisches Element i hat. In diesem Fall ist das Produkt aller Gruppenelemente i.

Das folgt unmittelbar aus den vorigen Sätzen.

Die Gruppe G der primen Restklassen modulo einer ganzen Zahl m enthält genau ein involutorisches Element, nämlich die Klasse von -1, wenn und nur wenn G zyklisch von gerader Ordnung ist und mindestens zwei Elemente enthält, also für $m = 4$ oder $m = p^k$ oder $2p^k$, wobei p^k eine ungerade Primzahlpotenz ist. Dass in allen anderen Fällen mindestens zwei involutorische Elemente auftreten, ergibt sich so: Für $m = 2^e$, $e > 2$, sind die beiden $\pm 5^{2^{e-3}}$ enthaltenden Restklassen involutorisch. Enthält m zwei verschiedene Primzahlpotenzen q und $r > 2$ als Teiler, etwa $m = qrs$ mit $(q, r) = (qr, s) = 1$, so hat die Kongruenz $x^2 \equiv 1$ neben der trivialen auch eine nichttriviale Lösung mod q und mod r. Daraus ergeben sich nach dem chinesischen Restsatz in bekannter Weise mindestens zwei nichttriviale Lösungen mod m. Das Produkt aller primen Reste mod m ist also kongruent zu -1, falls $m = 4$ oder $m = p^k$ oder $m = 2p^k$ ist, und zu $+1$ in allen anderen Fällen. Das ist die Gaußsche Verallgemeinerung des Wilsonschen Satzes (vgl. HARDY-WRIGHT, *An Introduction to the Theory of Numbers*, 3rd ed., Oxford 1954, p. 103). Weitere Sonderfälle von Satz 4 liegen auf der Hand, zum Beispiel: Das Produkt aller quadratischen Reste modulo einer ungeraden Primzahl p ist kongruent zu $+1$, falls $p \equiv 3 \pmod 4$ und zu -1, falls $p \equiv 1 \pmod 4$ ist.

HANFRIED LENZ, München

Aufgaben

Aufgabe 434. Man beweise folgende Umkehrformel: f und g sind zahlentheoretische Funktionen (das heisst Abbildungen der Menge der nicht negativen ganzen Zahlen in eine additive abelsche Gruppe, zum Beispiel die reellen oder komplexen Zahlen). Dann sind die beiden Aussagen

$$g(x) = \sum_{k=0}^{x} \binom{x}{k} f(k) \tag{1}$$

und

$$f(x) = \sum_{k=0}^{x} (-1)^{x+k} \binom{x}{k} g(k) \tag{2}$$

gleichbedeutend.

A. BAGER, Hjørring, Dänemark