Kleine Mitteilung

Kleine Mitteilung

Kombinatorische Deutung und Verallgemeinerung des Fermatschen Satzes

Der sogenannte «kleine» Fermatsche Satz, wonach für eine Primzahl p und eine beliebige Zahl a stets $a^p \equiv a(p)$ gilt und für $p \nmid a$ dann $a^{p-1} - 1$ durch p teilbar wird, ist – völlig zurecht – als wesentlich gruppentheoretischer Satz gedeutet worden. Er hat dann sinngemäss die Verallgemeinerung von EULER $a^{\varphi(n)} \equiv 1(n)$ für beliebige n und $(a, n) = 1$ mit der Eulerschen φ-Funktion. Dass der Fermatsche Satz aber auch eine andere einfache, und zwar rein kombinatorische Deutung zulässt, welche dann zu einer anderen Verallgemeinerung führt, darauf sei nun in dieser Notiz hingewiesen.

Sei zunächst p eine Primzahl. Wir bilden alle Variationen (mit Wiederholung) von a Elementen zur p-ten Klasse, das sind insgesamt a^p. Nun fassen wir je p zusammen, welche auseinander durch zyklische Vertauschung hervorgehen. Man überzeugt sich leicht, dass, weil p Primzahl ist, diese alle verschieden sind, ausser in dem Fall, dass ein p-Tupel mit lauter gleichen Elementen $(x, x, \ldots x)$ vorliegt. Solche gibt es aber bei a Elementen im ganzen a, somit $a^p - a$ übrige, welche zu je p zusammengefasst sind; also ist $a^p - a$ durch p teilbar.

Nehmen wir nun statt der Primzahl p eine beliebige Zahl n, so gibt es wohl ausser dem Typ $(x, x, \ldots x)$ noch andere n-Tupel $(x_1, x_2, \ldots x_n)$, welche bei bestimmten zyklischen Vertauschungen in sich selbst übergehen. Der Ansatz hiefür,

$$x_i = x_{i+d} \text{ für alle mod } n \text{ zu nehmenden Indizes,}$$

zeigt, dass d ein Teiler von n ist und die Folge $(x_1, x_2, \ldots x_n)$ aus mehreren gleichen Teilen besteht (wie etwa $x\,y\,x\,y$). Will man nun diese Fälle ausscheiden und alle n-Tupel übrigbehalten, welche bei zyklischer Vertauschung lauter verschiedene Bilder ergeben, so berechnet sich deren Zahl durch die Möbiussche Umkehrformel als

$$\sum_{d \mid n} \mu(d)\, a^{n/d}$$

mit der Möbiusschen μ-Funktion und diese Anzahl muss aus kombinatorischen Gründen durch n teilbar sein. Es werden ja unter diesen Variationen je n durch zyklische Verschiebung zusammengefasst. Die Beziehung

$$\sum_{d \mid n} \mu(d)\, a^{n/d} \equiv 0(n)$$

ist also die sinngemässe kombinatorische Verallgemeinerung des Fermatschen Satzes $a^p - a \equiv 0(p)$ für Primzahlen. Im Falle der Teilerfremdheit $(a, n) = 1$ könnte man noch durch eine entsprechende Potenz von a dividieren; zum Beispiel für $n = 12$ wird $a^{12} - a^6 - a^4 + a^2 \equiv 0(12)$ oder $a^{10} - a^4 - a^2 + 1 \equiv 0(12)$ für $(a, 12) = 1$. Durch Zerlegung solcher Polynome tritt oft eine Analogie zur Eulerschen Verallgemeinerung des Fermatschen Satzes zutage; speziell ergibt sich für $n = p^k$ (Primzahlpotenz) direkt $a^{\varphi(n)} - 1 \equiv 0(n)$.

Auf diese Tatsachen und die Anzahlformel ist man auch in der Informationstheorie bei gewissen Problemen der Codierung gestossen, siehe etwa [1]; allerdings ohne Bezug auf den kleinen Fermatschen Satz und die Primzahlen. Auf diesen beachtlichen Zusammenhang sei hiemit aufmerksam gemacht.

A. AIGNER, Graz

LITERATUR

[1] S. W. GOLOMB, BASIL GORDON, and L. R. WELCH, *Comma-free Codes*, Can. J. Math. *10*, 202–209 (1958).