

Zwei Sätze von Joseph Wolstenholme

Johann Cigler

Vor einiger Zeit sandte mir Herr P., ein philosophisch gebildeter älterer Mann, einige Bemerkungen zu einem Resultat von Joseph Wolstenholme, das er folgendermaßen formulierte:

Wenn $n \geq 4$ und $p = n + 1$, also immer $p \geq 5$, und wenn in

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \frac{a}{b}$$

das Ergebnis $\frac{a}{b}$ so gekürzt ist, dass a und b teilerfremd sind, dann kann der Zähler a immer nur dann durch $(n+1)^2 = p^2$ geteilt werden, wenn p eine Primzahl ist.

Er hat die Fälle $5 \leq p \leq 13$ mit Hilfe eines programmierbaren Taschenrechners verifiziert und schrieb: „Wolstenholmes theoretischer Beweis (der ... schon seit 1862 existiert) ist mir leider unbekannt. Ich nehme an, dass er auch vielen professionellen Mathematikern unbekannt ist, obwohl er (im Gegensatz z.B. zu den „transfiniten Zahlen“ des G. Cantor) sicherlich zu den interessanten und unumstößlichen Ergebnissen der echten Mathematik gehört.“

Er wollte von mir wissen, wie man dieses Resultat mit den ihm zur Verfügung stehenden Vorkenntnissen aus der Schulmathematik beweisen kann. Ich nehme an, dass ihn dieser Satz besonders deshalb fasziniert hat, weil er ihn für eine Charakterisierung der Primzahlen > 3 hielt. Ob das wirklich der Fall ist, ist aber nach wie vor ein offenes Problem. Bewiesen ist bis jetzt nur die folgende Aussage:

Satz von Wolstenholme über harmonische Zahlen

Wenn $p > 3$ eine Primzahl ist, dann ist in

$$S(p) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b} \quad (1)$$

der Zähler a durch p^2 teilbar. Das gilt unabhängig davon, ob der Bruch gekürzt ist oder nicht, da der gemeinsame Nenner $(p-1)!$ nicht durch p teilbar ist.

Der Satz sagt nichts über $S(n)$ aus, falls n keine Primzahl ist.

Da ich den Satz damals auch nicht kannte, habe mich in der Literatur ein wenig umgesehen. Außer dem Buch [4] von Hardy und Wright habe ich kein Lehrbuch gefunden, wo dieses Problem ausführlich behandelt wird, obwohl es sich zumindest als Übungsaufgabe für Algebra- oder Zahlentheorie-Vorlesungen sehr gut eignen würde. (In [4] wird übrigens darauf hingewiesen, dass dieser Satz zum ersten Mal schon 80 Jahre vor Wolstenholme 1782 von Waring gefunden wurde. Er wird aber üblicherweise nach Wolstenholme benannt, der von 1829-1891 lebte und ihn unabhängig wiederentdeckte). Allerdings gibt es eine Reihe von Arbeiten, wo Verallgemeinerungen bzw. Verschärfungen dieses Resultats bewiesen werden, wie etwa [1],[3],[5]. Daraus ergeben sich auch einfache Beweise des ursprünglichen Resultats.

Da Herr P. mit dem Kongruenzbegriff nicht vertraut war, suchte ich zuerst einen Beweis, der ohne den Begriff der Kongruenz auskommt. Ein derartiger Beweis, der von Lagrange stammt, findet sich im Buch von Hardy und Wright.

Die Aussage, dass $S(p)$ durch p^2 teilbar ist, ist gleichbedeutend damit, dass die ganze Zahl $(p-1)!S(p)$ durch p^2 teilbar ist. Dadurch wird das Problem auf ganze Zahlen zurückgeführt. Das vereinfacht vieles. Betrachten wir nun das Polynom

$$(x-1)(x-2)\cdots(x-p+1) = x^{p-1} - s_{p-2}(p)x^{p-2} + \cdots - s_1(p)x + s_0(p). \quad (2)$$

Hier ist $s_0(p) = (p-1)!$ und $s_1(p) = (p-1)!S(p)$.

Die Aussage des Satzes von Wolstenholme ist äquivalent mit der Aussage, dass $s_1(p)$ durch p^2 teilbar ist.

In jeder Vorlesung über Algebra lernt man (vgl. z.B. [2], p. 205), dass im Ring $\mathbb{F}_p[x]$ der Polynome über dem Körper \mathbb{F}_p der Restklassen modulo p

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)) \quad (3)$$

gilt. Das bedeutet, dass alle $s_i(p)$ mit $1 \leq i \leq p-2$ durch p teilbar sind. Außerdem ergibt sich $(p-1)! \equiv -1 \pmod{p}$, ein Resultat, das als Satz von Wilson bekannt ist.

Beispielsweise ist für $p=5$

$$(x-1)(x-2)(x-3)(x-4) = x^4 - 10x^3 + 35x^2 - 50x + 24$$

$$\text{und } s_1(5) = 2 \cdot 3 \cdot 4 + 1 \cdot 3 \cdot 4 + 1 \cdot 2 \cdot 4 + 1 \cdot 2 \cdot 3 = 4! \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \right) = 50 = 2 \cdot 5^2.$$

Der Beweis von Lagrange leitet dieses Resultat ganz elementar ohne Verwendung des Kongruenzbegriffs oder der Theorie der endlichen Körper ab.

Dazu multipliziere man beide Seiten von (2) mit x und ersetze dann x durch $x-1$. Es ergibt sich

$$\begin{aligned} (x-1)^p - s_{p-2}(p)(x-1)^{p-1} + \cdots + s_0(p)(x-1) &= (x-1)(x-2)\cdots(x-p) \\ &= (x-p) \left(x^{p-1} - s_{p-2}(p)x^{p-2} + \cdots - s_1(p)x + s_0(p) \right). \end{aligned}$$

Entwickelt man jedes $(x-1)^j$ nach dem binomischen Lehrsatz und vergleicht die Koeffizienten von x^{p-i} so ergibt sich

$$\binom{p}{1} + s_{p-2}(p) = p + s_{p-2}(p),$$

$$\binom{p}{2} + \binom{p-1}{1} s_{p-2}(p) + s_{p-3}(p) = s_{p-3}(p) + p s_{p-2}(p)$$

und allgemeiner

$$\binom{p}{i} + s_{p-2}(p) \binom{p-1}{i-1} + s_{p-3}(p) \binom{p-2}{i-2} + \cdots + s_{p-i}(p) \binom{p-i+1}{1} + s_{p-i-1}(p) = s_{p-i-1}(p) + p s_{p-i}(p)$$

für alle i .

Das gibt

$$s_{p-2}(p) = \binom{p}{2},$$

$$2s_{p-3}(p) = \binom{p}{3} + s_{p-2}(p) \binom{p-1}{2}$$

und allgemein

$$(i-1)s_{p-i}(p) = \binom{p}{i} + s_{p-2}(p) \binom{p-1}{i-1} + s_{p-3}(p) \binom{p-2}{i-2} + \cdots + s_{p-i+1}(p) \binom{p-i+2}{2}.$$

Daraus ergibt sich der Reihe nach, dass jedes $s_i(p)$ mit $i > 0$ durch p teilbar ist.

Für $i = 0$ ergibt sich

$$(p-1)s_0(p) = 1 + s_{p-2}(p) + \cdots + s_1(p)$$

und somit, dass $1 + s_0(p)$ durch p teilbar ist.

Der Rest des Beweises ist nun sehr einfach:

Wählt man $x = p$ in (2), so erhält man

$$(p-1)! = (p-1)(p-2)\cdots(p-p+1) = p^{p-1} - s_{p-2}(p)p^{p-2} + \cdots - s_1(p)p + s_0(p)$$

und somit wegen $s_0(p) = (p-1)!$

$$p^{p-2} - s_{p-2}(p)p^{p-3} + \cdots + p s_2(p) = s_1(p). \quad (4)$$

Da $p > 3$ ist und alle Terme auf der linken Seite durch p^2 teilbar sind, ist auch $s_1(p)$ durch p^2 teilbar. Damit ist der Satz von Wolstenholme bewiesen.

Wie bereits erwähnt, lässt sich alles viel einfacher formulieren und beweisen, wenn man den Kongruenzbegriff verwendet.

Aus dem obigen Beweis ergibt sich auch sofort der

Satz von Wolstenholme über Binomialkoeffizienten

Für jede Primzahl $p > 3$ gilt

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}. \quad (5)$$

Denn $\binom{2p-1}{p-1} = \frac{(p+1)(p+2)\cdots(2p-1)}{(p-1)!} \equiv 1 \pmod{p^3}$ ist gleichbedeutend mit

$$\frac{p^{p-1} + s_{p-2}(p)p^{p-2} + \cdots + s_1(p)p + s_0(p)}{s_0(p)} \equiv 1 \pmod{p^3}. \text{ Und das ist wieder äquivalent mit}$$

$p^{p-1} + s_{p-2}(p)p^{p-2} + \cdots + s_1(p)p \equiv 0 \pmod{p^3}$, d.h. mit der Aussage, dass $s_1(p)$ durch p^2 teilbar ist.

Man beachte dabei, dass für rationale Zahlen $\frac{a}{b}, \frac{c}{d}$, deren Nenner zu m teilerfremd

sind, $\frac{a}{b} \equiv \frac{c}{d} \pmod{m}$ bedeutet, dass in $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$ der Zähler $ad-bc$ ein

Vielfaches von m ist, dass also $ad \equiv bc \pmod{m}$ gilt.

Einfachere Beweise

Um den Satz von Wolstenholme über harmonische Zahlen zu beweisen, genügt es zu zeigen, dass

$$\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}\right) \equiv 0 \pmod{p} \quad (6)$$

ist.

Denn dann ist

$$2S(p) = \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \cdots + \left(\frac{1}{p-1} + \frac{1}{p-(p-1)}\right) = p \left(\frac{1}{1(p-1)} + \frac{1}{2(p-2)} + \cdots + \frac{1}{(p-1)1}\right)$$

und wegen $\frac{1}{i(p-i)} \equiv -\frac{1}{i^2} \pmod{p}$ ist

$$\frac{1}{1(p-1)} + \frac{1}{2(p-2)} + \cdots + \frac{1}{(p-1)1} \equiv -\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}\right) \equiv 0 \pmod{p}.$$

Wenn also (6) gilt, dann ist $S(p)$ ein rationales Vielfaches von p^2 .

Der Beweis von (6) kann auf verschiedene Weise geführt werden. Wenn man

beachtet, dass die Menge der Inversen $\frac{1}{i}$ der Zahlen $1, \dots, p-1$ modulo p wieder

mit der Menge der Zahlen $1, \dots, p-1$ übereinstimmt, dann stimmt auch die Menge

der Quadrate $\frac{1}{i^2}$ mit der Menge der Quadrate i^2 modulo p überein und daher ist

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv \sum_{i=1}^{p-1} i^2 = \frac{p(p-1)(2p-1)}{6} \equiv 0 \pmod{p}. \quad (7)$$

Oder man beachtet, dass die Menge der Zahlen $2, 4, \dots, 2(p-1)$ modulo p mit der Menge der Zahlen $1, \dots, p-1$ übereinstimmt.

Dann ist also auch

$$\frac{1}{4} \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(p-1)^2} \right) = \frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{6^2} + \dots + \frac{1}{(2(p-1))^2} \equiv 1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(p-1)^2} \pmod{p}$$

oder

$$3 \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(p-1)^2} \right) \equiv 0 \pmod{p}. \quad (8)$$

Da $p > 3$ ist, folgt (6) aus (8).

Daraus ergibt sich auch ein einfacherer Zugang zum Satz von Wolstenholme über Binomialkoeffizienten.

Denn es gilt ohne jede Kenntnis über das Kongruenzverhalten von $s_i(p)$ jedenfalls

$$\binom{2p-1}{p-1} = \frac{p^{p-1} + s_{p-2}(p)p^{p-2} + \dots + s_1(p)p + s_0(p)}{s_0(p)} \equiv \frac{s_2(p)p^2 + s_1(p)p + s_0(p)}{s_0(p)} \pmod{p^3}$$

Aus (6) ergibt sich $s_1(p) \equiv 0 \pmod{p^2}$ und daher auch

$$\binom{2p-1}{p-1} \equiv 1 + \frac{s_2(p)}{s_0(p)} p^2 \pmod{p^3}.$$

Es muss also nur noch gezeigt werden, dass $\frac{s_2(p)}{s_0(p)} \equiv 0 \pmod{p}$ ist.

Nun ist aber

$$\frac{s_2(p)}{s_0(p)} = \sum_{1 \leq i < j \leq p-1} \frac{1}{ij}.$$

Daher folgt aus (6)

$$2 \frac{s_2(p)}{s_0(p)} = 2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} = \left(\sum_{i=1}^{p-1} \frac{1}{i} \right)^2 - \sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \pmod{p},$$

womit alles gezeigt ist.

Bemerkung

Die einfachere Kongruenz $\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}$ wurde bereits 1819 von Charles Babbage bewiesen.

Sein Beweis verwendet die wohlbekannt Formel $\sum_{j=0}^n \binom{n}{j}^2 = \binom{2n}{n}$.

Damit ergibt sich

$$\binom{2p-1}{p-1} = \frac{1}{2} \binom{2p}{p} = \frac{1}{2} \sum_{j=0}^n \binom{p}{j}^2 \equiv \frac{1}{2} \left(\binom{p}{0}^2 + \binom{p}{p}^2 \right) = 1 \pmod{p^2},$$

weil $\binom{p}{j}^2$ für $1 \leq j \leq p-1$ durch p^2 teilbar ist.

Literatur

- [1] G.E. Andrews, q-analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher, *Discr. Math.* 205 (1999), 15-25
- [2] J. Cigler, *Körper, Ringe, Gleichungen*, Spektrum Verlag 1995 (siehe auch <http://homepage.univie.ac.at/johann.cigler/skripten/algebra.pdf>)
- [3] I.M. Gessel, Wolstenholme revisited, *Amer. Math. Monthly* 105 (1998), 657–658.
- [4] G.H. Hardy & E.M. Wright, *An Introduction to the Theory of Numbers*, 3rd Edition, Oxford 1954
- [5] R.J. McIntosh, On the converse of Wolstenholme's theorem. *Acta Arith.* 71 (1995), no. 4, 381–389