Werk

Titel: Jahresbericht der Deutschen Mathematiker-Vereinigung
Verlag: Teubner
Jahr: 1917
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN37721857X_0025
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN37721857X_0025

LOG Id: LOG_0014
LOG Titel: Über Kongruenz x ... (mod. p.).
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN37721857X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN37721857X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=37721857X

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Über die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$.

Von I. SCHUR in Berlin.

Im 135. Bande des Journals für die reine und angewandte Mathematik (S. 134 und S. 181) hat Herr L. E. Dickson folgenden Satz bewiesen:

Die Kongruenz

$$x^m + y^m \equiv z^m \pmod{p} \tag{1}$$

läßt sich, sobald die Primzahl p eine gewisse allein von m abhängende Schranke M übertrifft, durch drei zu p teilerfremde ganze Zahlen x, y, z befriedigen.[1])

Dieser Satz steht in einer interessanten Beziehung zum sog. großen Fermatschen Theorem. Aus ihm geht hervor, daß der Versuch, die Unmöglichkeit der Gleichung $x^m + y^m = z^m$ mit Hilfe der zugehörigen Kongruenzen nachzuweisen, nicht zum Ziele führen kann.[2])

Die beiden Beweise, die Herr Dickson für seinen Satz angegeben hat, beruhen auf ziemlich umständlichen Rechnungen. Eine elegante, aber ebenfalls nicht ganz einfache Rechnung liegt dem Beweise zugrunde, der sich aus der allgemeineren Untersuchung von Herrn Hurwitz ergibt.

Im folgenden will ich zeigen, daß der Dicksonsche Satz sich fast unmittelbar aus einem sehr einfachen Hilfssatz ergibt, der mehr der Kombinatorik als der Zahlentheorie angehört:

Hilfssatz. *Verteilt man die Zahlen $1, 2, \ldots, N$ irgendwie auf m Zeilen, so müssen, sobald $N > m!\,e$ wird, in mindestens einer Zeile zwei Zahlen vorkommen, deren Differenz in derselben Zeile enthalten ist.*[3])

Nimmt man diesen Satz als bewiesen an, so ergibt sich der Dicksonsche Satz folgendermaßen.

Ist zunächst $p - 1 = mq$ durch m teilbar und bedeutet g eine primitive Wurzel mod. p, so sind die $p - 1$ Zahlen

$$g^\mu, \quad g^{\mu+m}, \quad g^{\mu+2m}, \quad \ldots, \quad g^{\mu+(q-1)m} \qquad (\mu = 0, 1, \ldots, m-1)$$

---

1) Herr Dickson spricht den Satz nur für den Fall aus, daß m eine Primzahl ist.

2) Vgl. A. Hurwitz, Über die Kongruenz $ax^e + by^e + cz^e \equiv 0 \pmod{p}$, Journal für die r. u. a. Math., Bd. 136, S. 272.

3) Unter e ist hier die Basis der natürlichen Logarithmen zu verstehen.

abgesehen von der Reihenfolge mod. p den Zahlen $1, 2 \ldots, p-1$ kongruent. Bezeichnet man daher den kleinsten positiven Rest von g^ν nach dem Modul p mit r_ν, so erscheinen die Zahlen $1, 2, \ldots, p-1$ auf die m Zeilen

$$r_\mu, \quad r_{\mu+m}, \quad r_{\mu+2m}, \quad \ldots, \quad r_{\mu+(q-1)m} \qquad (\mu = 0, 1, \ldots, m-1)$$

verteilt. Ist nun $p - 1 > m!\, e$, so gibt es nach dem Hilfssatz für mindestens ein μ drei Indizes α, β, γ, für die

$$r_{\mu+\gamma m} - r_{\mu+\beta m} = r_{\mu+\alpha m}$$

wird. Dann ist aber

$$g^{\mu+\gamma m} \equiv g^{\mu+\alpha m} + g^{\mu+\beta m} \pmod{p},$$

und daher genügen die Zahlen

$$x = g^\alpha, \quad y = g^\beta, \quad z = g^\gamma$$

der Kongruenz (1).

Ist ferner $p - 1$ nicht durch m teilbar, so sei d der größte gemeinsame Teiler von m und $p - 1$. Dann läßt sich, sobald $p - 1$ größer als $m!\, e$, also auch größer als $d!\, e$ wird, nach dem vorhin Bewiesenen die Kongruenz

$$x^d + y^d \equiv z^d \pmod{p}$$

durch drei zu p teilerfremde Zahlen befriedigen, und da bekanntlich jeder d-te Potenzrest mod. p zugleich auch als m-ter Potenzrest darstellbar ist, so gilt dasselbe auch für die Kongruenz (1).

Der Dicksonsche Satz ist also richtig, wenn M gleich $m!\, e + 1$ gesetzt wird.

Um nun den Hilfssatz zu beweisen, nehme man an, es sei für eine Zahl $N > m!\, e$ gelungen, die Zahlen $1, 2, \ldots, N$ auf m Zeilen so zu verteilen, daß keine Zeile die Differenz zweier ihrer Zahlen enthält. Man wähle dann eine Zeile Z_1, in der möglichst viele Zahlen vorkommen. Sind $x_1, x_2, \ldots, x_{n_1}$ die nach steigender Größe geordneten Zahlen von Z_1, so ist $N \leqq n_1 m$. Ferner gehören die $n_1 - 1$ Differenzen

$$x_2 - x_1, \quad x_3 - x_1, \quad \ldots, \quad x_{n_1} - x_1 \tag{2}$$

wieder der Reihe $1, 2, \ldots, N$ an, und da nach Voraussetzung keine von ihnen in Z_1 vorkommt, so verteilen sie sich auf die $m - 1$ übrigen Zeilen. Es sei Z_2 eine dieser Zeilen, in der möglichst viele unter den Differenzen (2) enthalten sind. Enthält Z_2 die n_2 Differenzen

$$x_\alpha - x_1, \quad x_\beta - x_1, \quad x_\gamma - x_1, \quad \ldots, \qquad (\alpha < \beta < \gamma < \ldots) \tag{3}$$

so ist

$$n_1 - 1 \leqq n_2 (m - 1).$$

Zieht man die erste der Zahlen (3) von den folgenden ab, so kommen die so entstehenden Differenzen

$$x_\beta - x_\alpha, \quad x_\gamma - x_\alpha, \quad \ldots \tag{4}$$

weder in Z_1 noch in Z_2 vor, sie verteilen sich also auf die übrigen $m-2$ Zeilen. Unter diesen Zeilen wähle man wieder eine, für die die Anzahl der in ihr vorkommenden Differenzen (4) möglichst groß wird. Enthält diese Zeile die n_3 Differenzen

$$x_\varkappa - x_\alpha, \quad x_\lambda - x_\alpha, \quad \ldots,$$

so wird

$$n_2 - 1 \leqq n_3(m-2).$$

Indem man in dieser Weise fortfährt, erhält man gewisse $m' \leqq m$ Zahlen $n_1, n_2, \ldots, n_{m'}$, die den Ungleichungen

$$n_\mu - 1 \leqq n_{\mu+1}(m-\mu) \tag{5}$$

genügen. Hierbei muß offenbar $n_{m'} = 1$ sein, da man sonst das Verfahren fortsetzen könnte. Aus (5) ergibt sich nun

$$\frac{n_\mu}{(m-\mu)!} \leqq \frac{n_{\mu+1}}{(m-\mu-1)!} + \frac{1}{(m-\mu)!},$$

und hieraus folgt durch Addition

$$\frac{n_1}{(m-1)!} \leqq \frac{1}{(m-1)!} + \frac{1}{(m-2)!} + \frac{1}{(m-m')!} < e.$$

Es müßte also

$$N \leqq m n_1 < m!\, e$$

sein, was der über N gemachten Annahme widerspricht.

Ich bemerke noch folgendes. Herr Dickson hat (a. a. O. S. 187) mit Hilfe der Theorie der Kreisteilung (allerdings nur für Primzahlen m) gezeigt, daß es genügt

$$M = m^4 - 6m^3 + 13m^2 - 6m + 1$$

zu setzen. Ein so günstiges Resultat läßt sich allein unter Benutzung unserer Hilfsbetrachtung nicht erzielen. Um nämlich auf dem hier eingeschlagenen Wege eine möglichst kleine Schranke M zu erhalten, handelt es sich darum, bei gegebenem m die größte Zahl N_m zu bestimmen, für die sich noch die Zahlen $1, 2, \ldots, N_m$ auf m Zeilen so verteilen lassen, daß keine Zeile die Differenz zweier ihrer Zahlen enthält. Genügt nun das Schema

$$\begin{array}{c} x_1, \; x_2, \; \ldots \\ \ldots\ldots\ldots \\ u_1, \; u_2, \; \ldots \end{array}$$