Matyáš Lerch
Über eine Eigenschaft der Factorielle

Zprávy Král. Čes. spol. nauk, II. tř., 1898, č. 2, 1–4

Persistent URL: http://dml.cz/dmlcz/501515

II.

Ueber eine Eigenschaft der Factorielle.

Von M. Lerch in Freiburg (Schweiz).

(Vorgelegt den 14. Jänner 1898.)

Ist p eine Primzahl von der Form $4n+1$, so hat das Product

$$A_p = 1 . 2 . 3 \ldots \frac{p-1}{2}$$

nach Lagrange die Eigenschaft, dass

$$A_p^2 + 1 \equiv 0 \pmod{p}.$$

Wenn aber die Primzahl p die Form $4n-1$ hat, so ist

$$A_p^2 - 1 \equiv 0 \pmod{p}.$$

Aus dieser Congruenz, welche Lagrange aus dem Wilson'schen Satze abgeleitet hat, schliesst Dirichlet,*) dass entweder $A_p - 1$ oder $A_p + 1$ durch p theilbar sein muss, oder mit anderen Worten

$$A_p \equiv \varepsilon \pmod{p}; \quad p = 4n-1, \; \varepsilon = \pm 1.$$

Die Bestimmung des Zeichens ε wird von Dirichlet als eine Aufgabe gestellt.

Weil für die Zahlen von der Form $4n-1$ die Identität besteht

$$\left(\frac{\varepsilon}{p}\right) = \varepsilon, \quad (\varepsilon = \pm 1),$$

*) Question d' Analyse indéterminée (Journal für die reine und angewandte Mathematik, Bd. 3; Dirichlet's Werke, I. Band, p. 107).

so verlangt die Aufgabe, das Legendre'sche Zeichen

$$\left(\frac{A_p}{p}\right)$$

in einer für die wirkliche Ausrechnung zugänglichen Form zu bestimmen. In dieser Fassung hat aber die Aufgabe auch einen Sinn, wenn p die Form $4n + 1$ hat, und wir wollen daher vorläufig unter p irgend welche ungerade Primzahl verstehen. Eine weitere Verallgemeinerung wäre, für p auch zusammengesetzte Zahlen zuzulassen, aber in diesem Falle haben A_p und p einen gemeinsamen Theiler und es ist also

$$\left(\frac{A_p}{p}\right) = 0.$$

Es sei also p eine ungerade Primzahl; als dann ist

$$\left(\frac{A_p}{p}\right) = \left(\frac{1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)\cdots\cdots\left(\frac{\frac{1}{2}(p-1)}{p}\right);$$

es wird daher

$$\left(\frac{A_p}{p}\right) = (-1)^{\sigma}, \tag{1}$$

wenn in dem letzten Producte σ Factoren den Werth -1 haben. Diese Anzahl hat aber den Werth

$$\sigma = \sum_{\nu=1}^{\frac{1}{2}(p-1)} \frac{1}{2}\left[1 - \left(\frac{\nu}{p}\right)\right],$$

oder

$$\sigma = \frac{p-1}{4} - \frac{1}{2}\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left(\frac{\nu}{p}\right).$$

Ist nun $p = 4n + 1$, so folgt aus der Identität

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) = 0$$

mit Hilfe des Umstandes, dass die Zeichen

$$\left(\frac{\nu}{p}\right) \text{ und } \left(\frac{p-\nu}{p}\right)$$

im Falle $p = 4n + 1$ einander gleich sind, unmittelbar die Beziehung

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left(\frac{\nu}{p}\right) = 0,$$

und daher $\sigma = \frac{p-1}{4}$.

„Für Primzahlen p von der Form $4n + 1$ hat die Factorielle

$$A_p = \left(\frac{p-1}{2}\right)!$$

die Eigenschaft

$$\left(\frac{A_p}{p}\right) = (-1)^{\frac{p-1}{4}}.“$$

Ist zweitens $p = 4n - 1$, so hat die Summe

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left(\frac{\nu}{p}\right)$$

nicht mehr den Werth Null, und zwar wird sie durch die Classenanzahl ausgedrückt. Bezeichnet man mit Cl. $(-p)$ die Anzahl der primitiven und positiven Classen quadratischer Formen wie

$$ax^2 + bxy + cy^2,$$

in welchen die Discriminante $b^2 - 4ac$ den negativen Werth $-p$ hat, so besteht die Gleichung

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left(\frac{\nu}{p}\right) = \left[2 - \left(-1\right)^{\frac{p^2-1}{8}}\right] \text{Cl. } (-p),$$

wenn $p > 3$.

Man hat daher

$$(2) \qquad 4\sigma = p - 1 - 2\left[2 - (-1)^{\frac{p^2-1}{8}}\right] \text{Cl. } (-p),$$

oder was dasselbe ist

$$4\sigma = p - 1 - 2\,\mathrm{Cl.}\,(-4p).$$

„Für die Primzahlen $p = 4n - 1$ hat die Factorielle

$$A_p = \left(\frac{p-1}{2}\right)!$$

die Eigenschaft

$$\left(\frac{A_p}{p}\right) = (-1)^\sigma,$$

wobei

$$\sigma = \frac{2n - 1 - \mathrm{Cl.}\,(-4p)}{2}.$$

Es besteht zu gleicher Zeit die Congruenz

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^\sigma \pmod{p}."$$

Für $p = 3$ gilt der Satz nicht.

Diese Lösung der Dirichlet'schen Aufgabe setzt die Kenntniss des Restes der Classenanzahl modulo 4 voraus, und erst durch Erforschung dieses Restes wird sie eine zweckmässige Einfachheit erreichen. Vorläufig müssen wir uns jedoch mit dieser zu sehr complicirten Formel begnügen.

Als Beispiele mögen folgende drei Fälle erwähnt werden, aus welchen ersichtlich ist, dass der Ausdruck σ doch eine wesentliche Erleichterung leistet.

1. $p = 11$; $\mathrm{Cl.}\,(-11) = 1$, $\sigma = 1$;

$$1 . 2 . 3 . 4 . 5 + 1 = 11 . 11.$$

2. $p = 19$; $\mathrm{Cl.}\,(-19) = 1$, $\sigma = 3$;

$$1 . 2 . 3 . 4 . 5 . 6 . 7 . 8 . 9 + 1 = 19099 . 19$$

3. $p = 23$; $\mathrm{Cl.}\,(-23) = 3$, $\sigma = 4$;

$$1 . 2 . 3 . 4 . 5 . 6 . 7 . 8 . 9 . 10 . 11 - 1 = 1735513 . 23.$$

Verlag der kön. böhm. Gesellschaft der Wissenschaften. — Druck von Dr. Ed. Grégr in Prag.