

Werk

Titel: Journal für die reine und angewandte Mathematik

Verlag: de Gruyter

Jahr: 1909

Kollektion: Mathematica

Werk Id: PPN243919689_0136

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN243919689_0136|LOG_0014

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

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

Zum letzten *Fermatschen* Theorem.

Von Herrn *Arthur Wieferich* in Münster i. W.

Im 128. Bande dieses Journals (1905, S. 45—68) hat Herr *Mirimanoff* als sog. *Kummersches* Kriterium folgenden Satz formuliert:

Wenn die *Fermatsche* Gleichung

$$x^p + y^p + z^p = 0$$

bei ungeraden Primzahlexponenten durch zu p prime x, y, z lösbar sein soll, so müssen die Kongruenzen

$$(1.) \quad \varphi_i B_{\frac{p-i}{2}} \equiv 0 \pmod{p}$$

befriedigt werden für $i = 3, 5, \dots, p-2$, wobei

$$(2.) \quad \varphi_i = \sum_{j=1}^{p-1} (-1)^{j-1} t^j j^{i-1}$$

ist und B_i die i -te *Bernoullische* Zahl bedeutet. In der vorliegenden Arbeit soll nunmehr nachgewiesen werden, daß das Bestehen der Kongruenzen (1.) notwendig die Kongruenz

$$2^{p-1} \equiv 1 \pmod{p^2}$$

nach sich zieht.

§ 1.

Es ist

$$(3.) \quad t e^v - t^p e^{pv} = (1 + t e^v) \sum_{i=1}^{p-1} (-1)^{i-1} t^i e^{iv}.$$

Die x -te Ableitung von (3.) nach v wird alsdann für $v=0$

$$t - t^p p^x = (1+t) \varphi_{x+1} + \binom{x}{1} t \varphi_x + \binom{x}{2} t \varphi_{x-1} + \cdots + \binom{x}{x-1} t \varphi_2 + \binom{x}{x} t \varphi_1.$$

Setze ich noch $\frac{1+t}{t} = \mathfrak{g}$, so erhalte ich leicht das Gleichungssystem

$$(4.) \quad \begin{aligned} \mathfrak{g} \varphi_{x+1} + \binom{x}{1} \varphi_x + \binom{x}{2} \varphi_{x-1} + \cdots + \binom{x}{x-1} \varphi_2 + \binom{x}{x} \varphi_1 &= 1 - t^{p-1} p^x, \\ \mathfrak{g} \varphi_x + \binom{x-1}{1} \varphi_{x-1} + \cdots + \binom{x-1}{x-2} \varphi_2 + \binom{x-1}{x-1} \varphi_1 &= 1 - t^{p-1} p^{x-1}, \\ \mathfrak{g} \varphi_{x-1} + \cdots + \binom{x-2}{x-3} \varphi_2 + \binom{x-2}{x-2} \varphi_1 &= 1 - t^{p-1} p^{x-2}, \\ &\vdots \\ \cdots + \binom{3}{2} \varphi_2 + \binom{3}{3} \varphi_1 &= 1 - t^{p-1} p^3, \\ \cdots + \binom{2}{1} \varphi_2 + \binom{2}{2} \varphi_1 &= 1 - t^{p-1} p^2, \\ \mathfrak{g} \varphi_2 + \binom{1}{1} \varphi_1 &= 1 - t^{p-1} p, \\ \mathfrak{g} \varphi_1 &= 1 - t^{p-1}. \end{aligned}$$

Aus (4.) will ich nunmehr $\varphi_{x+1} = \frac{A_{x+1}}{A}$ bestimmen. Es ergibt sich sofort

$$(5.) \quad A = \mathfrak{g}^{x+1}.$$

Ferner ist

$$A_{x+1} = \begin{vmatrix} 1 - t^{p-1} p^x & \binom{x}{1} & \binom{x}{2} & \cdots & \binom{x}{x-2} & \binom{x}{x-1} & \binom{x}{x} \\ 1 - t^{p-1} p^{x-1} & \mathfrak{g} & \binom{x-1}{1} & \cdots & \binom{x-1}{x-3} & \binom{x-1}{x-2} & \binom{x-1}{x-1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 1 - t^{p-1} p^2 & 0 & 0 & \cdots & \mathfrak{g} & \binom{2}{1} & \binom{2}{2} \\ 1 - t^{p-1} p & 0 & 0 & \cdots & 0 & \mathfrak{g} & \binom{1}{1} \\ 1 - t^{p-1} & 0 & 0 & \cdots & 0 & 0 & \mathfrak{g} \end{vmatrix}.$$

Multipliziere ich die Reihen obiger Determinante der Reihe nach mit $1, z, z(z-1), \dots, z(z-1) \dots 3 \cdot 2, z(z-1) \dots 2 \cdot 1$, so erhalte ich

$$A_{x+1} z^x (z-1)^{x-1} \dots 2^2 \cdot 1 = \begin{vmatrix} 1 - t^{p-1} p^x & \binom{x}{1} & \binom{x}{2} & \dots & \binom{x}{x} \\ (1 - t^{p-1} p^{x-1}) z & \vartheta z & \binom{x-1}{1} z \dots \binom{x-1}{x-1} z & & \\ \vdots & \vdots & \vdots & & \vdots \\ (1 - t^{p-1} p^2) z(z-1) \dots 3 & 0 & 0 & \dots & \binom{2}{2} z(z-1) \dots 3 \\ (1 - t^{p-1} p) z(z-1) \dots 2 & 0 & 0 & \dots & \binom{1}{1} z(z-1) \dots 2 \\ (1 - t^{p-1}) z(z-1) \dots 1 & 0 & 0 & \dots & \vartheta z(z-1) \dots 1 \end{vmatrix}.$$

Setze ich jetzt aus den Kolonnen der Reihe nach die Faktoren $1, z, z(z-1), \dots, z(z-1) \dots 2 \cdot 1$ heraus, so wird, wenn ich noch zur Abkürzung

$$\frac{1}{x!} = \alpha_x$$

setze,

$$A_{x+1} = \begin{vmatrix} 1 - t^{p-1} p^x & \alpha_1 & \alpha_2 & \dots & \alpha_{x-1} & \alpha_x \\ (1 - t^{p-1} p^{x-1}) z & \vartheta & \alpha_1 & \dots & \alpha_{x-2} & \alpha_{x-1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ (1 - t^{p-1} p^2) z(z-1) \dots 3 & 0 & 0 & \dots & \alpha_1 & \alpha_2 \\ (1 - t^{p-1} p) z(z-1) \dots 2 & 0 & 0 & \dots & \vartheta & \alpha_1 \\ (1 - t^{p-1}) z(z-1) \dots 1 & 0 & 0 & \dots & 0 & \vartheta \end{vmatrix}.$$

Es sei nun

$$(6.) \quad \begin{vmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{i-1} & \alpha_i \\ \vartheta & \alpha_1 & \dots & \alpha_{i-2} & \alpha_{i-1} \\ 0 & \vartheta & \dots & \alpha_{i-3} & \alpha_{i-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & \alpha_1 & \alpha_2 \\ 0 & 0 & \dots & \vartheta & \alpha_1 \end{vmatrix} = F_i$$

gesetzt. Dann wird

$$\begin{aligned} \mathcal{A}_{x+1} &= (1-t^{p-1}p^x) \mathcal{G}^x - x(1-t^{p-1}p^{x-1}) \mathcal{G}^{x-1} F_1 + \dots \\ &\quad + (-1)^{x-1} x(x-1) \dots 3 \cdot 2 (1-t^{p-1}p) \mathcal{G} F_{x-1} \\ &\quad + (-1)^x x(x-1) \dots 2 \cdot 1 (1-t^{p-1}) F_x, \end{aligned}$$

oder auch

$$\begin{aligned} \mathcal{A}_{x+1} &= x! \{ \alpha_x \mathcal{G}^x - \alpha_{x-1} \mathcal{G}^{x-1} F_1 + \alpha_{x-2} \mathcal{G}^{x-2} F_2 + \dots + (-1)^{x-2} \alpha_2 \mathcal{G}^2 F_{x-2} \\ &\quad + (-1)^{x-1} \alpha_1 \mathcal{G} F_{x-1} + (-1)^x F_x \} \\ (7.) \quad &- t^{p-1} \{ p^x \mathcal{G}^x - x p^{x-1} \mathcal{G}^{x-1} F_1 + x(x-1) p^{x-2} \mathcal{G}^{x-2} F_2 - \dots \\ &\quad + (-1)^{x-1} x(x-1) \dots 3 \cdot 2 p \mathcal{G} F_{x-1} + (-1)^x x(x-1) \dots 2 \cdot 1 F_x \}. \end{aligned}$$

Aus (6.) ergibt sich nun leicht, daß allgemein

$$\begin{aligned} (8.) \quad F_i &= \alpha_1 F_{i-1} - \alpha_2 \mathcal{G} F_{i-2} + \alpha_3 \mathcal{G}^2 F_{i-3} - \dots + (-1)^{i-2} \alpha_{i-1} \mathcal{G}^{i-2} F_1 \\ &\quad + (-1)^{i-1} \alpha_i \mathcal{G}^{i-1} \end{aligned}$$

ist. Es ist also

$$\begin{aligned} \alpha_x \mathcal{G}^x - \alpha_{x-1} \mathcal{G}^{x-1} F_1 + \dots + (-1)^{x-2} \alpha_2 \mathcal{G}^2 F_{x-2} + (-1)^{x-1} \alpha_1 \mathcal{G} F_{x-1} \\ = (-1)^{x-1} \mathcal{G} F_x. \end{aligned}$$

Folglich wird

$$\begin{aligned} \mathcal{A}_{x+1} &= x! \{ (-1)^{x-1} \mathcal{G} F_x + (-1)^x F_x \} \\ &\quad - t^{p-1} \{ p^x \mathcal{G}^x - \dots + (-1)^{x-1} x(x-1) \dots 2p \mathcal{G} F_{x-1} \\ &\quad + (-1)^x x(x-1) \dots 2 \cdot 1 F_x \} \\ &= (-1)^{x-1} x! \{ \mathcal{G} - 1 + t^{p-1} \} F_x \\ &\quad - t^{p-1} \{ p^x \mathcal{G}^x - \dots + (-1)^{x-1} x(x-1) \dots 2p \mathcal{G} F_{x-1} \}. \end{aligned}$$

Es werde nun vorausgesetzt, daß

$$t \text{ weder } \equiv 0 \text{ noch } \equiv -1 \pmod{p}$$

ist. Weiterhin ist leicht zu sehen, daß F_i für $i < p$ nie die Zahl p im Nenner haben kann. Demnach wird, da $t^{p-1} \equiv 1 \pmod{p}$ ist,

$$(9.) \quad A_{x+1} \equiv (-1)^{x-1} x! \mathcal{G} F_x \pmod{p}$$

für $x = 1, 2, \dots, p-1$.

Aus (5.) und (9.) ergibt sich endlich

$$(10.) \quad \varphi_{x+1} \equiv \frac{(-1)^{x-1} x! F_x}{\mathcal{G}^x} \pmod{p}.$$

§ 2.

Es sei

$$(11.) \quad G_i = \begin{vmatrix} \binom{x}{1} & \binom{x}{2} & \dots & \binom{x}{i-1} & \binom{x}{i} \\ \mathcal{G} & \binom{x-1}{1} & \dots & \binom{x-1}{i-2} & \binom{x-1}{i-1} \\ 0 & \mathcal{G} & \dots & \binom{x-2}{i-3} & \binom{x-2}{i-2} \\ . & . & & . & . \\ . & . & & . & . \\ 0 & 0 & \dots & \binom{x-i+2}{1} & \binom{x-i+2}{2} \\ 0 & 0 & \dots & \mathcal{G} & \binom{x-i+1}{1} \end{vmatrix}.$$

Dann finde ich leicht, indem ich wie in § 1 verfare, daß

$$G_i = \frac{x!}{(x-i)!} F_i$$

ist, d. h. daß

$$(12.) \quad G_i \equiv (-1)^{i-1} \binom{x}{i} \mathcal{G}^i \varphi_{i+1} \pmod{p}$$

ist.

Speziell für $i = x$ ergibt sich

$$(11a.) \quad G_x = \begin{vmatrix} \binom{x}{1} & \binom{x}{2} & \dots & \binom{x}{x-1} & \binom{x}{x} \\ \vartheta & \binom{x-1}{1} & \dots & \binom{x-1}{x-2} & \binom{x-1}{x-1} \\ 0 & \vartheta & \dots & \binom{x-2}{x-3} & \binom{x-2}{x-2} \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \dots & \binom{2}{1} & \binom{2}{2} \\ 0 & 0 & \dots & \vartheta & \binom{1}{1} \end{vmatrix}$$

und

$$(12a.) \quad G_x \equiv (-1)^{x-1} \vartheta^x \varphi_{x+1} \pmod{p}.$$

Addiere ich jetzt in (11a.) die resp. mit λ^{x-1} , $\lambda^{x-2} \dots \lambda^2$, λ multiplizierten Kolonnen zur letzten Kolonne, so erhalte ich

$$G_x = \begin{vmatrix} \binom{x}{1} & \binom{x}{2} & \dots & \binom{x}{x-1} & (1+\lambda)^x - \lambda^x \\ \vartheta & \binom{x-1}{1} & \dots & \binom{x-1}{x-2} & (1+\lambda)^{x-1} - \lambda^{x-1} + \vartheta \lambda^{x-1} \\ 0 & \vartheta & \dots & \binom{x-2}{x-3} & (1+\lambda)^{x-2} - \lambda^{x-2} + \vartheta \lambda^{x-2} \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \dots & \binom{2}{1} & (1+\lambda)^2 - \lambda^2 + \vartheta \lambda^2 \\ 0 & 0 & \dots & \vartheta & (1+\lambda) - \lambda + \vartheta \lambda \end{vmatrix},$$

wobei λ eine beliebige Zahl ist.

Setze ich noch

$$(13.) \quad (1+\lambda)^i - \lambda^i + \vartheta \lambda^i = (1+\lambda)^i + (\vartheta-1)\lambda^i = H_{i+1},$$

so wird

$$\begin{aligned} G_x &= (-1)^{x-1} \vartheta^{x-1} (H_{x+1} - \vartheta \lambda^x) + (-1)^{x-2} \vartheta^{x-2} H_x G_1 + \dots \\ &\quad + \vartheta^2 H_4 G_{x-3} - \vartheta H_3 G_{x-2} + H_2 G_{x-1}, \end{aligned}$$

d. h. nach (12.) und (12^a.)

$$(14.) \quad \begin{aligned} -\vartheta \varphi_{x+1} \equiv & -H_{x+1} + \vartheta \lambda^x + \binom{x}{1} H_x \varphi_2 + \binom{x}{2} H_{x-1} \varphi_3 + \dots \\ & + \binom{x}{x-3} H_4 \varphi_{x-2} + \binom{x}{x-2} H_3 \varphi_{x-1} + \binom{x}{x-1} H_2 \varphi_x \pmod{p}. \end{aligned}$$

§ 3.

Ich summiere jetzt die Kongruenzen (14.) über

$$\lambda = 0, -1, 2, -3, \dots, p-1, -p.$$

Setze ich zur Abkürzung

$$(15.) \quad \begin{cases} 1^{2j-1} - 2^{2j-1} + 3^{2j-1} - \dots - (p-1)^{2j-1} + p^{2j-1} = \mathfrak{B}_{2j}, \\ 1^{2j} + 2^{2j} + 3^{2j} + \dots + (p-1)^{2j} + p^{2j} = S_{2j+1}, \end{cases}$$

so erhalte ich leicht

$$(16.) \quad \begin{cases} \sum_{\lambda=0, -1, 2, \dots, -p} H_{2j} = (2 - \vartheta) \mathfrak{B}_{2j}, \\ \sum_{\lambda=0, -1, 2, \dots, -p} H_{2j+1} = \vartheta S_{2j+1}, \\ \sum_{\lambda=0, -1, 2, \dots, -p} \lambda^x = \begin{cases} S_{x+1} \\ -\mathfrak{B}_{x+1} \end{cases} \end{cases}, \text{ je nachdem } x \begin{cases} \text{gerade} \\ \text{ungerade} \end{cases} \text{ ist.}$$

Ersetze ich noch x durch $2x-1$, so erhalte ich endlich

$$(17.) \quad \begin{aligned} -\vartheta \varphi_{2x} \equiv & -2 \mathfrak{B}_{2x} + \binom{2x-1}{1} \vartheta S_{2x-1} \varphi_2 + \binom{2x-1}{2} (2 - \vartheta) \mathfrak{B}_{2x-2} \varphi_3 \\ & + \dots + \binom{2x-1}{2x-3} \vartheta S_3 \varphi_{2x-2} + \binom{2x-1}{2x-2} (2 - \vartheta) \mathfrak{B}_2 \varphi_{2x-1}. \end{aligned}$$

Es ist nun

$$S_{2j+1} \equiv 0 \pmod{p},$$

ferner bekanntlich

$$\mathfrak{B}_{2j} \equiv (-1)^{j-1} B_j \frac{2^{2j}-1}{j} \pmod{p},$$

wo B_j die j -te Bernoullische Zahl bedeutet.

Die Kongruenz (17.) geht demnach über in

$$\begin{aligned} -\vartheta \varphi_{2k} &\equiv -2 \mathfrak{B}_{2k} + \binom{2k-1}{2} (2-\vartheta) B_{k-1} \varphi_3 \frac{2^{2k-2}-1}{k-1} + \dots \\ &\quad + \binom{2k-1}{2k-2} (2-\vartheta) B_1 \varphi_{2k-1} \frac{2^2-1}{1}, \end{aligned}$$

oder, wenn ich noch $k = \frac{p-1}{2}$ setze,

$$\begin{aligned} (18.) \quad -\vartheta \varphi_{p-1} &\equiv -2 \mathfrak{B}_{\frac{p-1}{2}} + (2-\vartheta) \left\{ \binom{p-2}{2} B_{\frac{p-3}{2}} \frac{2^{p-3}-1}{\frac{p-3}{2}} \varphi_3 + \dots \right. \\ &\quad \left. + \binom{p-2}{p-3} B_1 \frac{2^2-1}{1} \varphi_{p-2} \right\}. \end{aligned}$$

Wir wollen nunmehr annehmen, daß die Kongruenzen (1.)

$$\varphi_i B_{\frac{p-i}{2}} \equiv 0 \pmod{p}$$

sämtlich erfüllt seien, daß also

$$\varphi_3 B_{\frac{p-3}{2}} \equiv 0,$$

$$\varphi_5 B_{\frac{p-5}{2}} \equiv 0,$$

.

.

$$\varphi_{p-4} B_2 \equiv 0,$$

$$\varphi_{p-2} B_1 \equiv 0$$

sei. Dann liefert also (18.) die Kongruenz

$$(19.) \quad \vartheta \varphi_{p-1} \equiv 2 \mathfrak{B}_{p-1} \pmod{p}.$$

Es ist nun nach (2.)

$$\varphi_{p-1} = \sum_{j=1}^{p-1} (-1)^{j-1} t^j j^{p-2},$$

d. h.

$$\begin{aligned} \varphi_{p-1} &\equiv t - \frac{1}{2}t^2 + \frac{1}{3}t^3 - \dots - \frac{1}{p-1}t^{p-1} \\ &\equiv \frac{1}{p} \{ \binom{p}{1}t + \binom{p}{2}t^2 + \binom{p}{3}t^3 + \dots + \binom{p}{p-1}t^{p-1} \} \\ &\equiv \frac{(1+t)^p - 1 - t^p}{p} \pmod{p}. \end{aligned}$$

Es läßt sich nun leicht zeigen, daß $\varphi_{p-1} \equiv 0$ sein muß modulo p , daß also $(1+t)^p - 1 - t^p$ durch p^2 teilbar sein muß. Es ist nämlich t das Verhältnis zweier der Größen x, y, z , etwa $t = \frac{y}{x}$.

Dann wird

$$\varphi_{p-1} \equiv \frac{(x+y)^p - x^p - y^p}{p x^p},$$

d. h. da $x+y+z \equiv 0 \pmod{p}$, gleich Ap ist,

$$\varphi_{p-1} \equiv \frac{(Ap-z)^p - x^p - y^p}{p x^p} \equiv 0 \pmod{p}.$$

Es muß daher auch

$$(20.) \quad \mathfrak{B}_{p-1} \equiv 0 \pmod{p}$$

sein. Es ist aber

$$\begin{aligned}\mathfrak{B}_{p-1} &\equiv 1 - \frac{1}{2} + \frac{1}{3} - \dots - \frac{1}{p-1} \\ &\equiv \frac{1}{p} \{ \binom{p}{1} + \binom{p}{2} + \binom{p}{3} + \dots + \binom{p}{p-1} \} \\ &\equiv \frac{2^p - 2}{p} \pmod{p}.\end{aligned}$$

Da die Werte $t \equiv 0$ und $t \equiv -1$ nicht in Betracht kommen wegen der Annahme, daß x, y, z prim zu p sind, so ergibt sich also ganz allgemein, daß das Bestehen der Kongruenzen (1.) die Kongruenz

$$2^{p-1} \equiv 1 \pmod{p^2}$$

bedingt.
