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

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 *Fermat*schen Theorem.

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

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

Wenn die *Fermat*sche 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

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

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

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

ist und B_i die i-te *Bernoulli*sche 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

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

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

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

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

$$(4.)\qquad \begin{aligned}
\vartheta\varphi_{\varkappa+1} + \tbinom{\varkappa}{1}\varphi_\varkappa + \tbinom{\varkappa}{2}\varphi_{\varkappa-1} + \cdots + \tbinom{\varkappa}{\varkappa-1}\varphi_2 + \tbinom{\varkappa}{\varkappa}\varphi_1 &= 1 - t^{p-1}p^\varkappa,\\
\vartheta\varphi_\varkappa + \tbinom{\varkappa-1}{1}\varphi_{\varkappa-1} + \cdots + \tbinom{\varkappa-1}{\varkappa-2}\varphi_2 + \tbinom{\varkappa-1}{\varkappa-1}\varphi_1 &= 1 - t^{p-1}p^{\varkappa-1},\\
\vartheta\varphi_{\varkappa-1} + \cdots + \tbinom{\varkappa-2}{\varkappa-3}\varphi_2 + \tbinom{\varkappa-2}{\varkappa-2}\varphi_1 &= 1 - t^{p-1}p^{\varkappa-2},\\
\cdot\qquad\cdot\qquad\cdot\qquad & \cdot\\
\cdot\qquad\cdot\qquad\cdot\qquad & \cdot\\
\cdots + \tbinom{3}{2}\varphi_2 + \tbinom{3}{3}\varphi_1 &= 1 - t^{p-1}p^3,\\
\cdots + \tbinom{2}{1}\varphi_2 + \tbinom{2}{2}\varphi_1 &= 1 - t^{p-1}p^2,\\
\vartheta\varphi_2 + \tbinom{1}{1}\varphi_1 &= 1 - t^{p-1}p,\\
\vartheta\varphi_1 &= 1 - t^{p-1}.
\end{aligned}$$

Aus (4.) will ich nunmehr $\varphi_{\varkappa+1} = \frac{\Delta_{\varkappa+1}}{\Delta}$ bestimmen. Es ergibt sich sofort

$$(5.)\qquad \Delta = \vartheta^{\varkappa+1}.$$

Ferner ist

$$\Delta_{\varkappa+1} = \begin{vmatrix}
1-t^{p-1}p^\varkappa & \binom{\varkappa}{1} & \binom{\varkappa}{2} & \ldots & \binom{\varkappa}{\varkappa-2} & \binom{\varkappa}{\varkappa-1} & \binom{\varkappa}{\varkappa}\\
1-t^{p-1}p^{\varkappa-1} & \vartheta & \binom{\varkappa-1}{1} & \ldots & \binom{\varkappa-1}{\varkappa-3} & \binom{\varkappa-1}{\varkappa-2} & \binom{\varkappa-1}{\varkappa-1}\\
\cdot & \cdot & \cdot & & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & & \cdot & \cdot & \cdot\\
1-t^{p-1}p^2 & 0 & 0 & \ldots & \vartheta & \binom{2}{1} & \binom{2}{2}\\
1-t^{p-1}p & 0 & 0 & \ldots & 0 & \vartheta & \binom{1}{1}\\
1-t^{p-1} & 0 & 0 & \ldots & 0 & 0 & \vartheta
\end{vmatrix}.$$

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

$$\Delta_{x+1} x^x (x-1)^{x-1}\cdots 2^2\cdot 1 = \begin{vmatrix} 1-t^{p-1}p^x & \binom{x}{1} & \binom{x}{2} & \cdots & \binom{x}{x} \\ (1-t^{p-1}p^{x-1})x & \vartheta x & \binom{x-1}{1}x & \cdots & \binom{x-1}{x-1}x \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ (1-t^{p-1}p^2)x(x-1)\cdots 3 & 0 & 0 & \cdots & \binom{2}{2}x(x-1)\cdots 3 \\ (1-t^{p-1}p)\,x(x-1)\cdots 2 & 0 & 0 & \cdots & \binom{1}{1}x(x-1)\cdots 2 \\ (1-t^{p-1}) \quad x(x-1)\cdots 1 & 0 & 0 & \cdots & \vartheta x(x-1)\cdots 1 \end{vmatrix}.$$

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

$$\frac{1}{\tau!} = \alpha_\tau$$

setze,

$$\Delta_{x+1} = \begin{vmatrix} 1-t^{p-1}p^x & \alpha_1 & \alpha_2 & \cdots & \alpha_{x-1} & \alpha_x \\ (1-t^{p-1}p^{x-1})x & \vartheta & \alpha_1 & \cdots & \alpha_{x-2} & \alpha_{x-1} \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ (1-t^{p-1}p^2)x(x-1)\cdots 3 & 0 & 0 & \cdots & \alpha_1 & \alpha_2 \\ (1-t^{p-1}p)x(x-1)\cdots 2 & 0 & 0 & \cdots & \vartheta & \alpha_1 \\ (1-t^{p-1})x(x-1)\cdots 1 & 0 & 0 & \cdots & 0 & \vartheta \end{vmatrix}.$$

Es sei nun

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

gesetzt. Dann wird

$$\begin{aligned}\Delta_{x+1} &= (1-t^{p-1}p^x)\,\vartheta^x - x(1-t^{p-1}p^{x-1})\,\vartheta^{x-1}F_1 + \cdots \\ &\quad + (-1)^{x-1}x(x-1)\cdots 3\cdot 2\,(1-t^{p-1}p)\,\vartheta F_{x-1} \\ &\quad + (-1)^x x(x-1)\cdots 2\cdot 1\,(1-t^{p-1})\,F_x,\end{aligned}$$

oder auch

$$\begin{aligned}\Delta_{x+1} &= x!\,\{\alpha_x\vartheta^x - \alpha_{x-1}\vartheta^{x-1}F_1 + \alpha_{x-2}\vartheta^{x-2}F_2 + \cdots + (-1)^{x-2}\alpha_2\vartheta^2 F_{x-2} \\ &\qquad + (-1)^{x-1}\alpha_1\vartheta F_{x-1} + (-1)^x F_x\} \\ &\quad - t^{p-1}\{p^x\vartheta^x - xp^{x-1}\vartheta^{x-1}F_1 + x(x-1)p^{x-2}\vartheta^{x-2}F_2 - \cdots \\ &\qquad + (-1)^{x-1}x(x-1)\cdots 3\cdot 2p\,\vartheta F_{x-1} + (-1)^x x(x-1)\cdots 2\cdot 1\,F_x\}.\end{aligned} \tag{7.}$$

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

$$\begin{aligned}F_i &= \alpha_1 F_{i-1} - \alpha_2\vartheta F_{i-2} + \alpha_3\vartheta^2 F_{i-3} - \cdots + (-1)^{i-2}\alpha_{i-1}\vartheta^{i-2}F_1 \\ &\qquad + (-1)^{i-1}\alpha_i\vartheta^{i-1}\end{aligned} \tag{8.}$$

ist. Es ist also

$$\begin{aligned}&\alpha_x\vartheta^x - \alpha_{x-1}\vartheta^{x-1}F_1 + \cdots + (-1)^{x-2}\alpha_2\vartheta^2 F_{x-2} + (-1)^{x-1}\alpha_1\vartheta F_{x-1} \\ &\qquad = (-1)^{x-1}\vartheta F_x.\end{aligned}$$

Folglich wird

$$\begin{aligned}\Delta_{x+1} &= x!\,\{(-1)^{x-1}\vartheta F_x + (-1)^x F_x\} \\ &\quad - t^{p-1}\{p^x\vartheta^x - \cdots + (-1)^{x-1}x(x-1)\cdots 2p\,\vartheta F_{x-1} \\ &\qquad + (-1)^x x(x-1)\cdots 2\cdot 1\,F_x\} \\ &= (-1)^{x-1}x!\,\{\vartheta - 1 + t^{p-1}\}\,F_x \\ &\quad - t^{p-1}\{p^x\vartheta^x - \cdots + (-1)^{x-1}x(x-1)\cdots 2p\,\vartheta F_{x-1}\}.\end{aligned}$$

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,

$$\Delta_{\varkappa+1} \equiv (-1)^{\varkappa-1}\varkappa!\,\vartheta F_\varkappa \pmod{p} \tag{9.}$$

für $\varkappa = 1, 2, \ldots p-1$.

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

$$\varphi_{\varkappa+1} \equiv \frac{(-1)^{\varkappa-1}\varkappa!\,F_\varkappa}{\vartheta^\varkappa} \pmod{p}. \tag{10.}$$

§ 2.

Es sei

$$G_i = \begin{vmatrix} \binom{\varkappa}{1} & \binom{\varkappa}{2} & \ldots & \binom{\varkappa}{i-1} & \binom{\varkappa}{i} \\ \vartheta & \binom{\varkappa-1}{1} & \ldots & \binom{\varkappa-1}{i-2} & \binom{\varkappa-1}{i-1} \\ 0 & \vartheta & \ldots & \binom{\varkappa-2}{i-3} & \binom{\varkappa-2}{i-2} \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \ldots & \binom{\varkappa-i+2}{1} & \binom{\varkappa-i+2}{2} \\ 0 & 0 & \ldots & \vartheta & \binom{\varkappa-i+1}{1} \end{vmatrix}. \tag{11.}$$

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

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

ist, d. h. daß

$$G_i \equiv (-1)^{i-1}\binom{\varkappa}{i}\vartheta^i \varphi_{i+1} \pmod{p} \tag{12.}$$

ist.

Speziell für $i = \varkappa$ ergibt sich

$$(11^{a}.) \qquad G_{\varkappa} = \begin{vmatrix} \binom{\varkappa}{1} & \binom{\varkappa}{2} & \dots & \binom{\varkappa}{\varkappa-1} & \binom{\varkappa}{\varkappa} \\ \vartheta & \binom{\varkappa-1}{1} & \dots & \binom{\varkappa-1}{\varkappa-2} & \binom{\varkappa-1}{\varkappa-1} \\ 0 & \vartheta & \dots & \binom{\varkappa-2}{\varkappa-3} & \binom{\varkappa-2}{\varkappa-2} \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & \dots & \binom{2}{1} & \binom{2}{2} \\ 0 & 0 & \dots & \vartheta & \binom{1}{1} \end{vmatrix}$$

und

$$(12^{a}.) \qquad G_{\varkappa} \equiv (-1)^{\varkappa-1} \vartheta^{\varkappa} \varphi_{\varkappa+1} \pmod{p}.$$

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

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

wobei λ eine beliebige Zahl ist.

Setze ich noch

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

so wird

$$G_{\varkappa} = (-1)^{\varkappa-1}\vartheta^{\varkappa-1}(H_{\varkappa+1} - \vartheta\lambda^{\varkappa}) + (-1)^{\varkappa-2}\vartheta^{\varkappa-2}H_{\varkappa}G_{1} + \cdots$$
$$+ \vartheta^{2}H_{4}G_{\varkappa-3} - \vartheta H_{3}G_{\varkappa-2} + H_{2}G_{\varkappa-1},$$

d. h. nach (12.) und (12ª.)

$$(14.)\qquad \begin{aligned} -\vartheta\varphi_{\varkappa+1} \equiv & -H_{\varkappa+1} + \vartheta\lambda^{\varkappa} + \binom{\varkappa}{1} H_{\varkappa}\varphi_2 + \binom{\varkappa}{2} H_{\varkappa-1}\varphi_3 + \cdots \\ & + \binom{\varkappa}{\varkappa-3} H_4\varphi_{\varkappa-2} + \binom{\varkappa}{\varkappa-2} H_3\varphi_{\varkappa-1} + \binom{\varkappa}{\varkappa-1} H_2\varphi_{\varkappa} \pmod{p}. \end{aligned}$$

§ 3.

Ich summiere jetzt die Kongruenzen (14.) über

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

Setze ich zur Abkürzung

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

so erhalte ich leicht

$$(16.)\qquad \begin{cases} \sum\limits_{\lambda=0,-1,2,\ldots-p} H_{2j} = (2-\vartheta)\,\mathfrak{B}_{2j}, \\ \\ \sum\limits_{\lambda=0,-1,2,\ldots-p} H_{2j+1} = \vartheta S_{2j+1}, \\ \\ \sum\limits_{\lambda=0,-1,2,\ldots-p} \lambda^{\varkappa} = \begin{matrix} S_{\varkappa+1} \\ -\mathfrak{B}_{\varkappa+1} \end{matrix}, \text{ je nachdem } \varkappa \begin{cases} \text{gerade} \\ \text{ungerade} \end{cases} \text{ ist.} \end{cases}$$

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

$$(17.)\qquad \begin{aligned} -\vartheta\varphi_{2\varkappa} \equiv & -2\mathfrak{B}_{2k} + \binom{2\varkappa-1}{1} \vartheta S_{2\varkappa-1}\varphi_2 + \binom{2\varkappa-1}{2} (2-\vartheta)\,\mathfrak{B}_{2\varkappa-2}\varphi_3 \\ & + \cdots + \binom{2\varkappa-1}{2\varkappa-3} \vartheta S_3\varphi_{2\varkappa-2} + \binom{2\varkappa-1}{2\varkappa-2} (2-\vartheta)\,\mathfrak{B}_2\varphi_{2\varkappa-1}. \end{aligned}$$

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 *Bernoulli*sche Zahl bedeutet.

Die Kongruenz (17.) geht demnach über in

$$-\vartheta \varphi_{2k} \equiv -2\mathfrak{B}_{2\varkappa} + \binom{2\varkappa-1}{2}(2-\vartheta) B_{\varkappa-1} \varphi_3 \frac{2^{2\varkappa-2}-1}{\varkappa-1} + \cdots + \binom{2\varkappa-1}{2\varkappa-2}(2-\vartheta) B_1 \varphi_{2\varkappa-1} \frac{2^2-1}{1},$$

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

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

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

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

sämtlich erfüllt seien, daß also

$$\varphi_3 B_{\frac{p-3}{2}} \equiv 0,$$
$$\varphi_5 B_{\frac{p-5}{2}} \equiv 0,$$
$$\cdot$$
$$\cdot$$
$$\varphi_{p-4} B_2 \equiv 0,$$
$$\varphi_{p-2} B_1 \equiv 0$$

sei. Dann liefert also (18.) die Kongruenz

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

Es ist nun nach (2.)

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

d. h.

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

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

$$\mathfrak{B}_{p-1} \equiv 0 \pmod{p} \tag{20.}$$

sein. Es ist aber

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

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.