SUR LE DERNIER THÉORÈME DE FERMAT ET LE CRITÉRIUM DE M. A. WIEFERICH

Autor(en): **Mirimanoff, D.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **11 (1909)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **29.03.2024**

Persistenter Link: https://doi.org/10.5169/seals-11873

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Il doit d'ailleurs exister un triangle particulier tel que si sur chacun de ses côtés on construit un carré ou un des autres quadrilatères semi-réguliers, leurs aires satisfassent à la formule

$$S = S' + S'' .$$

Il serait facile, au moyen des considérations qui précèdent, de calculer la relation qui doit exister entre les côtés de ce triangle, selon la nature du quadrilatère choisi.

P. Barbarin (Bordeaux).

SUR LE DERNIER THÉORÈME DE FERMAT

ET LE

CRITÉRIUM DE M. A. WIEFERICH

Dans un article intitulé *Zum letzten Fermatschen Theorem* (Journal f. reine u. angew. Mathematik, t. 136, p. 293-302), M. A. Wieferich vient de démontrer un théorème important sur lequel je désirerais attirer l'attention des lecteurs de l'*Enseignement mathématique*. En voici l'énoncé :

Si l'équation $x^p + y^p + z^p = 0$ *est possible en nombres entiers premiers à* p, *le quotient de* $2^{p-1} - 1$ *par* p *est divisible par* p.

L'impossibilité de l'équation de Fermat en nombres entiers premiers à p est donc établie par tous les nombres premiers p tels que $2^{p-1} - 1$ ne soit pas divisible par p^2. Elle est établie en particulier pour tous les nombres premiers de la forme $2^n \pm 1$, c'est-à-dire pour les nombres de Mersenne et leurs analogues et pour tous les nombres premiers p pour lesquels la division du cercle en p parties égales peut être faite avec la règle et le compas. L'importance de ce résultat n'échappera à personne.

M. Wieferich a déduit son critérium des congruences gé-

nérales qui ont été données dans un article du *J. f. reine u. angew. Math.* (t. 128, p. 45) et qui découlent du reste assez simplement des célèbres recherches de Kummer.

L'importance du résultat obtenu par M. Wieferich m'a déterminé à reprendre l'étude de ces congruences. Je me suis demandé s'il était possible de simplifier sa démonstration. Or, en examinant de plus près la congruence finale de laquelle M. Wieferich a déduit son théorème, on ne peut ne pas être frappé de l'analogie qu'elle présente avec la formule connue d'Euler donnant la somme alternée des puissances des premiers nombres entiers. Il était donc naturel de prendre cette formule d'Euler comme point de départ.

Je montrerai que la congruence de M. Wieferich est une conséquence de la formule d'Euler.

Congruences fondamentales. Rappelons d'abord le critérium qui découle des recherches de Kummer.

Désignons par $\varphi_i(t)$ ou φ_i le polynôme

$$t - 2^{i-1}t^2 + 3^{i-1}t^3 - \ldots - (p-1)^{i-1}t^{p-1} .$$

En faisant $i = 1, 2, 3 \ldots p-1$, on aura $p-1$ polynômes, mais nous n'aurons à considérer que les polynômes φ_i à indices impairs et le polynôme φ_{p-1}.

Supposons maintenant que l'équation de Fermat

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

admette une solution x, y, z première à p. Soit t l'un des rapports $\frac{x}{y}$, $\frac{y}{x}$, $\frac{x}{z}$, $\frac{z}{x}$, $\frac{y}{z}$, $\frac{z}{y}$ ou, ce qui revient au même, son reste (mod p). Puisque, par hypothèse, x, y, z sont premiers à p, le nombre t n'est congru ni à 0, ni à -1 (mod p). Voici alors comment s'énonce le critérium que je voulais rappeler :

Chacun des six rapports t vérifie le système des congruences

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

$$(i = 3, 5, \ldots p-2)$$

$B_{\frac{p-i}{2}}$ étant le $\frac{p-i}{2}$e nombre de Bernoulli.

A ces $\frac{p-3}{2}$ congruences nous pouvons adjoindre la suivante

$$\varphi_{p-1}(t) \equiv 0 \ , \tag{2}$$

qui résulte des congruences (1) et qu'on peut aussi établir d'une manière directe (cf. *J. f. Math.*, t. 128, p. 64).

Nous avons donc en tout $\frac{p-1}{2}$ congruences (1), (2). Appelons-les congruences fondamentales.

Congruence de M. Wieferich. Nous allons établir maintenant la congruence nouvelle de laquelle M. Wieferich a déduit son critérium. Je partirai, comme je l'ai dit, de la formule d'Euler

$$\begin{aligned} 1^{2n+1} - 2^{2n+1} + 3^{2n+1} - \ldots + (-1)^{y+1} y^{2n+1} \\ = (-1)^{y+1} \left\{ \frac{1}{2} y^{2n+1} + \binom{2n+1}{1} \frac{2^2-1}{2} B_1 y^{2n} - \binom{2n+1}{3} \frac{2^4-1}{4} B_2 y^{2n-2} + \ldots \right. \\ \left. + (-1)^{n-1} \binom{2n+1}{2n-1} \frac{2^{2n}-1}{2n} B_n y^2 + (-1)^n \frac{2^{2n+2}-1}{2n+2} B_{n+1} \right\} \\ + (-1)^n \frac{2^{2n+2}-1}{2n+2} B_{n+1} \ . \end{aligned} \tag{3}$$

(Cf. L. Saalschütz, *Vorlesungen über die Bernoullischen Zahlen*, p. 53).

Posons $2n+1 = p-2$, faisons $y = 1, 2, 3, \ldots p-1$, multiplions les égalités ainsi obtenues respectivement par $t, t^2, t^3, \ldots t^{p-1}$ et ajoutons.

Il viendra

$$\begin{aligned} 1^{p-2} t + (1^{p-2} - 2^{p-2}) t^2 + \ldots + (1^{p-2} - 2^{p-2} + \ldots - (p-1)^{p-2}) t^{p-1} \\ = \frac{1}{2} \varphi_{p-1} + \binom{p-2}{1} \frac{2^2-1}{2} B_1 \varphi_{p-2} - \binom{p-2}{3} \frac{2^4-1}{4} B_2 \varphi_{p-4} + \ldots \\ + (-1)^{\nu-2} \binom{p-2}{p-4} \frac{2^{p-3}-1}{p-3} B_{\nu-1} \varphi_3 \\ + (-1)^{\nu-1} \frac{2^{p-1}-1}{p-1} B_\nu 2 (t + t^3 + \ldots + t^{p-2}) \ , \end{aligned}$$

en posant $\nu = \frac{p-1}{2}$.

Multiplions cette égalité par $t-1$; son premier membre devient

$$-\varphi_{p-1}+(1^{p-2}-2^{p-2}+\ldots-(p-1)^{p-2})\,t^p\ .$$

Nous obtenons ainsi la formule

$$(4)\qquad (1^{p-2}-2^{p-2}+\ldots-(p-1)^{p-2})\,t^p-\frac{1}{2}(t+1)\,\varphi_{p-1}$$

$$=(t-1)\left\{\binom{p-2}{1}\frac{2^2-1}{2}B_1\varphi_{p-2}-\binom{p-2}{3}\frac{2^4-1}{4}B_2\varphi_{p-4}+\ldots\right.$$

$$\left.+(-1)^{\nu-2}\binom{p-2}{p-4}\frac{2^{p-3}-1}{p-3}B_{\nu-1}\varphi_3\right\}+(-1)^{\nu-1}\frac{2^p-2}{p-1}B_\nu\frac{t^p-t}{t+1}\ ,$$

qui est une *identité* en t.

Si maintenant on l'envisage comme une congruence (mod p), on a le droit de supprimer le dernier terme, à la condition que t soit différent de -1 (mod p). En effet, le facteur p qui figure au dénominateur de B_ν disparaît en multipliant par 2^p-2 et d'autre part t^p-t s'annule pour toutes les valeurs entières de t (mod p).

Mais en supprimant le dernier terme de (4) on obtient précisément la congruence finale de laquelle M. Wieferich a tiré son critérium (l. c., n° 3, form. (18)).

On voit donc que la congruence de M. Wieferich résulte de l'identité (4), qui est une conséquence de la formule d'Euler. Mais la réciproque n'est pas vraie, et c'est là un point sur lequel je voudrais attirer l'attention : il ne serait pas facile de déduire l'identité (4) de la congruence de M. Wieferich.

Supposons maintenant que l'équation de Fermat soit possible en nombres entiers premiers à p. Il existera alors une, et même plusieurs racines t différentes de 0 et de -1 qui annuleront les premiers membres des congruences (1) et (2). L'égalité (4) se réduira à son premier terme et nous aurons la condition

$$1^{p-2}-2^{p-2}+\ldots-(p-1)^{p-2}\equiv 0\pmod p$$

Or le premier membre de cette congruence est congru à $\frac{2^p - 2}{p} \pmod{p}$ (cf. P. BACHMANN, *Niedere Zahlentheorie*, p. 163).

D'où

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

C. Q. F. D. D. MIRIMANOFF (Genève).

MÉLANGES ET CORRESPONDANCE

Notations rationnelles pour le système vectoriel[1].

8. — *Réponse de* MM. BURALI-FORTI et MARCOLONGO *à MM. Timerding et Wilson.*

Nous remercions vivement M. FEHR d'avoir ouvert, dans l'*Enseignement mathématique*, une discussion sur les notations rationnelles pour le système vectoriel minimum que nous avons proposées en 1908; nous remercions aussi MM. TIMERDING, WILSON et PEANO, qui ont accepté l'invitation de M. Fehr, et ont bien voulu faire connaître leurs observations.

Le tableau qui contient nos propositions a été publié dans les *Rendiconti del Circolo matematico di Palermo*, t. XXV, 1908, à la fin de notre *Nota IV, Per l'unificazione delle notazioni vettoriali.* L'un de nous le présenta au IV^me^ Congrès international des mathématiciens à Rome; il a été ensuite imprimé à part et reproduit par plusieurs journaux scientifiques et par l'*Enseignement* (15 janvier 1909).

Il semble, malheureusement, que nos notations soient connues surtout par notre tableau; mais ce tableau est le résumé de toutes les études que nous avons faites sur la question de l'unification et que nous avons publiées dans les *Rendiconti del Circolo mate-*

[1] Voir l'*Ens. math.*, XI^e^ année, n° du 15 janvier 1909, p. 41-45; n° du 15 mars, p. 124-134; n° du 15 mai, p. 211-217; n° du 15 juillet, p. 341.