Sur le dernier théorème de Fermat.

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

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.07.2024**

avec les côtés fixes AC, AB. Mais comme la droite AI est fixe quelle que soit la position de la droite BC, les points Q et R sont aussi fixes et le cercle PQR qui touche en ces points aux deux droites fixes AC et AB est bien déterminé et ne dépend nullement de la position de la droite BC.

Ainsi donc, tout cercle circonscrit au triangle ABC est bien tangent au cercle déterminé PQR, quelle que soit la position du côté BC.

Y. SAWAYAMA (Tokio).

Sur le dernier théorème de Fermat.

(A propos d'un article de M. Cailler sur les congruences du troisième degré).

Il est facile, comme on sait, de rattacher la théorie de l'équation de Fermat

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

à celle des équations et des congruences du troisième degré.

Soient, en effet, s_1, s_2, s_3 les fonctions symétriques élémentaires $x + y + z$, $xy + xz + yz$, xyz. La somme $x^l + y^l + z^l$ est une fonction rationnelle entière à coefficients entiers de s_1, s_2, s_3. En l'égalant à zéro, on obtient une relation de la forme

$$\varphi(s_1, s_2, s_3) = 0 ,$$

φ étant un polynôme de degré l à coefficients entiers.

Or x, y, z sont racines de l'équation

$$t^3 - s_1 t^2 + s_2 t - s_3 = 0 . \tag{1}$$

On voit donc que l'étude de l'équation de Fermat se ramène à celle de l'équation (1) *caractérisée* par la relation $\varphi = 0$.

Au lieu de l'équation (1) on peut envisager la congruence correspondante mod n, n étant un nombre entier quelconque. L'étude se simplifie, mais la portée de la méthode diminue.

Il m'a paru intéressant d'appliquer à ces congruences les propositions établies par M. Cailler dans son article « Sur les congruences du troisième degré » (*Ens. math.*, novembre 1908, p. 474-487).

Bornons-nous au cas où les nombres x, y, z sont supposés premiers à l, et posons $n = l$. Dans ce cas s_3 n'est pas divisible par l; d'autre part on a toujours

$$x^l + y^l + z^l \equiv x + y + z .$$

Donc $s_1 \equiv 0$ et la congruence du troisième degré s'écrit

$$(1') \qquad t^3 + s_2 t - s_3 \equiv 0 \pmod{l}.$$

Or Legendre (*Mém. Acad. Sc. Institut France*, 1823) a déjà fait cette remarque que la différence

$$s_1^l - (x^l + y^l + z^l) = s_1^l - \varphi$$

est divisible par $(x+y)(x+z)(y+z) = s_1 s_2 - s_3$ et par l. Posons

$$\frac{s_1^l - \varphi}{l(s_1 s_2 - s_3)} = \mathrm{P}(s_1, s_2, s_3).$$

Comme s_1^l est divisible par l^l et que d'autre part $s_1 s_2 - s_3$ est premier à l, on aura en faisant $\varphi = 0$,

$$\mathrm{P}(s_1, s_2, s_3) \equiv 0$$

et par conséquent

$$\mathrm{P}(0, s_2, s_3) \equiv 0,$$

puisque $s_1 \equiv 0$.

On en conclut ceci : si l'équation de Fermat admet une solution première à l, la congruence $(1')$ caractérisée par la relation $\mathrm{P} \equiv 0$ a trois racines. Or les polynômes P se calculent très simplement à l'aide de la formule de Waring (E. Lucas, *Théorie des nombres*, p. 274).

Pour $l = 3$, $\mathrm{P} = 1$; donc $\mathrm{P} \not\equiv 0 \pmod{3}$ et l'équation de Fermat est impossible en nombres entiers premiers à l pour $l = 3$.

Pour $l = 5$, $\mathrm{P} = -s_2$. La condition $\mathrm{P} \equiv 0$ donne $s_2 \equiv 0$, mais alors le discriminant $-4s_2^3 - 27s_3^2$ de $(1')$ se réduit à $-27s_3^2 =$ non-résidu (puisque -3 est non-résidu pour tous les l de la forme $3m-1$). La congruence $(1')$ ne saurait donc avoir trois racines.

Pour $l = 11$, $\mathrm{P} = s_2(s_2^3 - s_3^2)$. Le module l étant un nombre de la forme $3m-1$, nous pouvons écarter l'hypothèse $s_2 \equiv 0$. Reste l'hypothèse $s_2^3 \equiv s_3^2$; le discriminant de $(1')$ se réduit à $-31s_3^2 \equiv 2s_3^2$ $=$ non-résidu.

Soit encore $l = 17$. Le polynôme P s'écrit $-s_2(s_2^6 - 5s_2^3 s_3^2 + s_3^4)$. En écartant l'hypothèse $s_2 \equiv 0$ et en posant $s_2^3 = u$, $s_3^2 = v$, on est conduit à la congruence

$$u^2 - 5uv + v^2 \equiv 0 \qquad \text{ou} \qquad (u - 12v)(u - 10v) \equiv 0.$$

Mais pour $u \equiv 12v$ le discriminant devient $-75s_3^2 \equiv 10s_3^2 =$ non-résidu. Reste l'hypothèse $u \equiv 10v$; le discriminant devient $-67s_3^2 \equiv s_3^2 \mp$ résidu.

Le nombre des racines de (1′) est donc égal à 0 ou à 3. Mais est-il égal à 0, est-il égal à 3 ? Pour répondre à cette question nous allons appliquer à la congruence (1′) le criterium donné par M. Cailler à la p. 486 (quatrième cas). Soient a, b deux nombres définis par les relations

$$ab \equiv -\frac{s_2}{3}\,, \quad a + b \equiv \frac{3s_3}{s_2}\,.$$

Pour que la congruence (1′) ait trois racines, il faut et il suffit que

$$\frac{a^6 - b^6}{a - b} \equiv 0 \pmod{17}$$

ou

$$\left\{ (a+b)^2 - ab \right\} \left\{ (a+b)^3 - 3ab(a+b) \right\} \equiv 0$$

et comme $a + b$ n'est pas divisible par 17, cette relation s'écrit

$$(u + 27v)(u + 9v) \equiv 0\,.$$

Or pour $u \equiv 10v$ le premier membre n'est pas divisible par 17. Les propositions établies par M. Cailler permettent donc de démontrer l'impossibilité de l'équation de Fermat en nombres entiers premiers à l pour $l = 17$.

Lorsque le module l est un nombre de la forme $3m + 1$, nous n'avons plus le droit de rejeter l'hypothèse $s_2 \equiv 0$, car le discriminant de (1′), qui se réduit à $-27s_3^2$, est résidu quadratique et la congruence (1′) peut avoir trois racines. C'est par l'étude directe de la relation $\varphi = 0$ et non des congruences que Lamé et Lebesgue ont réussi, comme on sait, à démontrer l'impossibilité de l'équation de Fermat pour $l = 7$ (*J. de Mathém.* 1840).

D. Mirimanoff (Genève).

Règle à calculs pour les écoles.

Au moment où la règle à calculs tend à pénétrer de plus en plus dans la pratique, il est indispensable de pouvoir en montrer le maniement dans les gymnases et écoles techniques.

Jusqu'ici son introduction dans l'enseignement était rendue difficile par suite du prix élevé de cet instrument. La maison Wichmann (Berlin, NW 6, Karlstrasse, 13), vient d'éditer une règle à calculs en carton blanc, dont le prix très modique (1 mark 25)