L'ÉQUATION DE FERMAT $a^{p-1} = pk_p(a) + 1$.

Autor(en): **Hansen, H. E.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **19 (1917)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-17328

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

L'ÉQUATION DE FERMAT

$$a^{p-1} = pk_p(a) + 1 \ .$$

PAR

H. E. HANSEN (Copenhague).

FERMAT a donné cette équation, d'où il résulte que, si pour p on choisit un nombre premier et pour a un nombre entier non divisible par p, on aura toujours un nombre entier comme valeur de $k_p(a)$. Jusqu'ici on n'a pas su déterminer ce nombre comme fonction entière et rationnelle de a et de p [1].

C'est d'une telle détermination qu'il s'agit ici.

Pour $a > p$, on peut poser $a = pn + x$, en admettant $n = 1, 2, 3 \ldots$, $x = 1, 2, 3 \ldots (p-1)$.

Alors on a

$$k_p(a) = \frac{(pn)^{p-1} + \frac{p-1}{1}(pn)^{p-2}.x + \frac{(p-1)(p-2)}{1.2}(pn)^{p-3}.x^2 + \ldots + \frac{p-1}{1}(pn)x^{p-2}}{p} + \frac{x^{p-1}-1}{p} \ . \qquad (A)$$

Le *premier* terme du second membre de cette équation sera entier et la valeur ainsi que la forme en sont déterminées pour les données p, n et x; il s'ensuit que seulement il importe de déterminer le *second* terme, c'est-à-dire d'examiner de plus près l'équation

$$a^{p-1} = pk_p(a) + 1$$

pour $a = 1, 2, 3 \ldots (p-1)$.

---

[1] Ceci n'est pas tout à fait exact : PLANA (*Mém. de l'Ac. des Sc. de Turin*, 1859) a donné la formule suivante, où s_n est mis pour $1^n + 2^n + 3^n + \ldots + (a-1)^n$,

$$\frac{a^{p-1}-1}{p} = \frac{1}{pa}(s_1 + C_{p-1,2}\,s_2 + C_{p-1,3}\,s_3 + \ldots) \ ;$$

en outre, LAGRANGE, dans son calcul des développements de $(x+1)(x+2)\ldots(x+n-1)$; et JACOBI, dans sa recherche des valeurs de p qui donnent $a^{p-1} - 1 \equiv 0 \pmod{p^2}$, se sont occupés de sujets analogues. N. D. L. R.

Quand p est un nombre premier — et seulement dans ce cas[1] — de $a^{p-1} = pk + 1$, par une division $p - 1$ fois réitérée avec a, on peut former les équations :

$$\begin{aligned}
a^{p-2} &= pk_1 + r_1 \\
a^{p-3} &= pk_2 + r_2 \\
&\cdots\cdots \\
a^{p-\alpha-1} &= pk_\alpha + r_\alpha \\
a^{p-\alpha-2} &= pk_{\alpha+1} + r_{\alpha+1} \\
&\cdots\cdots \\
a^2 &= pk_{p-3} + r_{p-3} \\
a &= pk_{p-2} + r_{p-2} \\
1 &= pk_{p-1} + 1
\end{aligned}$$

où l'on a k_α égal à $ak_{\alpha+1}$ plus un nombre ω, déterminé par le *plus petit* multiple ωp qui, additionné à r_α, donne une somme qui — à son tour — divisée par a, donne le quotient entier $r_{\alpha+1}$.

Il est ainsi évident que si dans

$$a^{p-\alpha-1} = pk_\alpha + r_\alpha$$

on met $k_\alpha = ak_{\alpha+1} + \omega$, on aura

$$a^{p-\alpha-1} = pak_{\alpha+1} + \omega p + r_\alpha ,$$

ou, après division par a,

$$a^{p-\alpha-2} = pk_{\alpha+1} + \frac{\omega p + r_\alpha}{a} = pk_{\alpha+1} + r_{\alpha+1} .$$

Dans tout cela nous n'avons encore rien dit sur les valeurs des $k, \ldots k_\alpha, k_{\alpha+1} \ldots k_{p-1}$; celles-ci pourraient bien être des fractions, et au surplus négatives, et telles seraient justement leurs valeurs, si, dans la dernière équation de la précédente suite, on ne trouvait pas $r_{p-1} = 1$.

Comme cela se trouvera toujours, on peut exprimer ce fait dans une : *loi pour les nombres premiers* — comme suit :

Partant de l'unité et d'un nombre premier, p, *on peut, en ajou-*

[1] Même observation. Ainsi $2^{37.73-1} \equiv 1 \pmod{37.73}$. Voir Ed. Lucas (*Th. des* n, p. 422). N. D. L. R.

tant à 1 *un multiple de* $p(\omega p)$, *obtenir un nombre divisible par* $a < p$. *Au quotient ainsi produit, il faut additionner un nouveau multiple de* $p(\omega_1 p)$, — ω_1 *éventuellement étant* 0 —, *puis diviser la somme par* a *pour avoir un nouveau quotient. Avec celui-ci, on agit comme avec le précédent, etc. Ayant ainsi fait* $p - 1$ *divisions, le dernier quotient obtenu sera toujours* 1.

La dernière équation de la suite donnée plus haut ayant ainsi la forme décrite, il est aisé de voir qu'il faut qu'on ait $k_{p-1} = 0$; et, à l'aide de nos substitutions, pour k_x, on trouvera successivement les valeurs de k_{p-2}, k_{p-3} ... et enfin celle de $k(\mathfrak{o} : k_p(a))$ comme fonctions entières et rationnelles de a.

A proprement dire, le problème posé ainsi peut être regardé comme résolu, mais nous ne manquerons pas de donner plusieurs exemples afin d'illustrer ce que nous avons dit.

Premièrement nous allons montrer en détail le traitement du cas $p = 7$, $a = 3$. Les résultats peuvent être rangés en quatre colonnes, dont (I) indique les $p - 1$ divisions par a, récemment décrite; (II) la suite des équations qui, pour le cas spécial, correspond avec la suite commune donnée au commencement; (III) indique les substitutions pour k, k_1 ... k_{p-1}, de même adaptées au cas spécial; et (IV), enfin, de bas en haut, successivement les valeurs trouvées pour k_6, k_5 ... k_1, la dernière donnant finalement $k(\mathfrak{o} : k_7(3))$.

(I)	(II)	(III)	(IV)
$\frac{1 + 2.7}{3} = 5$	$3^5 = 7k_1 + 5$	$k = 3k_1 + 2$	$k = 3^4.1 + 3^2.2 + 3 + 2$
$\frac{5 + 1.7}{3} = 4$	$3^4 = 7k_2 + 4$	$k_1 = 3k_2 + 1$	$k_1 = 3^3.1 + 3.2 + 1$
$\frac{4 + 2.7}{3} = 6$	$3^3 = 7k_3 + 6$	$k_2 = 3k_3 + 2$	$k_2 = 3^2.1 + 2$
$\frac{6 + 0.7}{3} = 2$	$3^2 = 7k_4 + 2$	$k_3 = 3k_4$	$k_3 = 3.1$
$\frac{2 + 1.7}{3} = 3$	$3 = 7k_5 + 3$	$k_4 = 3k_5 + 1$	$k_4 = 1$
$\frac{3 + 0.7}{3} = 1$	$1 = 7k_6 + 1$	$k_5 = 3k_6$	$k_5 = 0$

(donc $k_6 = 0$).

Cependant, comme ce n'est que l'expression pour $k(k_p(a))$ qu'on cherche, le résultat peut être trouvé bien plus simplement en

cherchant seulement les nombres qui dans (I) paraissent comme facteurs de 7 et dans (III) comme les quantités qu'il faut additionner à $3k_x\,(ak_x)$. En fin de compte, on peut garder la désignation a pour 3. La détermination de $k_7(3)$ alors peut être réglée ainsi :

1	5	4	6	2	3	1
2.7	1.7	2.7	0.7	1.7	0.7	—

On commence par écrire 1 en tête de la ligne supérieure, puis on cherche le *plus petit* multiple de 7 qui, additionné à 1, donne une somme divisible par 3. On écrit ce multiple sous 1, dans la seconde ligne, pendant que le quotient trouvé, 5, sera écrit à droite de 1 dans la première ligne. Maintenant on se comporte avec 5 comme auparavant avec 1, etc. — Le petit trait horizontal à la fin de la seconde ligne fait rappeler qu'on a $k_{p-1} = 0$.

A l'aide des facteurs de 7, de la seconde ligne, qui — comme il a été dit — seraient additionnés au produit $a \times$ le k précédent, on a successivement :

$$k_5 = a.0 + 0 = 0\ ,\quad k_4 = a.0 + 1 = 1\ ,\quad k_3 = a.1 + 0 = a\ ,$$
$$k_2 = a.a + 2\ ,\quad k_1 = a^3 + 2a + 1\ ,\quad k = a^4 + 2a^2 + a + 2\ .$$

Nous donnerons encore les résultats pour toutes les équations $a^{p-1} = pk_p(a) + 1$ correspondant aux nombres premiers 5, 7, 1 et 13, $(a < p)$.

$$p = 5\ .$$

$a = 2$,

1	3	4	2	1
1.5	1.5	0.5	0.5	—

$$k_3 = 0\ ,\quad k_2 = 0\ ,\quad k_1 = 1\ ,\quad k = k_p(a) = a + 1\ .$$

$a = 3$,

1	2	4	3	1
1.5	2.5	1.5	0.5	—

$$k_3 = 0\ ,\quad k_2 = 1\ ,\quad k_1 = a + 2\ ,\quad k = k_p(a) = a^2 + 2a + 1\ .$$

$a = 4$,

1	$\overline{4}$	1	4	1
3.5	0.5	3.5	0.5	—

$$k_3 = 0\ ,\quad k_2 = 3\ ,\quad k_1 = 3a\ ,\quad k = k_p(a) = 3a^2 + 3\ .$$

Le trait au-dessus de 4 et 1 désigne une *période* des quotients obtenus.

$$p = 7 .$$

$$a = 2 , \quad \begin{array}{c|cccccc|} 1 & \overline{4 & 2 & 1} & 4 & 2 & 1 \\ 1.7 & 0.7 & 0.7 & 1.7 & 0.7 & 0.7 & - \end{array}$$

$$k_5 = 0_1 , \quad k_4 = 0 , \quad k_3 = 1 , \quad k_2 = a , \quad k_1 = a^2 , \quad k = k_p(a) = a^3 + 1 .$$

$$a = 3 , \quad \begin{array}{c|cccccc|} 1 & 5 & 4 & 6 & 2 & 3 & 1 \\ 2.7 & 1.7 & 2.7 & 0.7 & 1.7 & 0.7 & - \end{array} .$$

$$k_5 = 0 , \quad k_4 = 1 , \quad k_3 = a , \quad k_2 = a^2 + 2 , \quad k_1 = a^3 + 2a + 1 ,$$
$$k_p(a) = a^4 + 2a^2 + a + 2 .$$

$$a = 4 , \quad \begin{array}{c|cccccc|} 1 & \overline{2 & 4 & 1} & 2 & 4 & 1 \\ 1.7 & 2.7 & 0.7 & 1.7 & 2.7 & 0.7 & - \end{array}$$

$$k_p(a) = 2a^4 + a^3 + 2a + 1 .$$

$$a = 5 , \quad \begin{array}{c|cccccc|} 1 & 3 & 2 & 6 & 4 & 5 & 1 \\ 2.7 & 1.7 & 4.7 & 2.7 & 3.7 & 0.7 & - \end{array}$$

$$k_p(a) = 3a^4 + 2a^3 + 4a^2 + a + 2 .$$

$$a = 6 , \quad \begin{array}{c|cccccc|} 1 & \overline{6 & 1} & 6 & 1 & 6 & 1 \\ 5.7 & 0.7 & 5.7 & 0.7 & 5.7 & 0\ 7 & - \end{array}$$

$$k_p(a) = 5a^4 + 5a^2 + 5 .$$

Par avance il était à présumer que les facteurs premiers de $p - 1$ allaient jouer un rôle considérable à l'égard de la forme des fonctions $k_p(a)$. En effet, il en est ainsi, car, de ce qui précède, on voit que de la solution de $p - 1$ se déduit l'apparition des *périodes* qui, à leur tour, donnent leur empreinte particulière à la forme du $k_p(a)$. Ainsi on voit, par exemple, dans ce qui précède, que pour $p - 1 = 6$ on peut avoir 2 périodes à 3 quotients ou 3 périodes à 2 quotients. Mais, d'un autre côté, on voit que la solubilité de $p - 1$ n'a aucune importance réelle. Ainsi pour $p - 1 = 6$ les valeurs 3 et 5 pour a n'admettent pas de périodes.

Pour $p = 11$ et 13 nous donnerons seulement les expressions pour $k_p(a)$:

$$p = 11 .$$

$$\begin{aligned}
a = 2 , \quad & k_p(a) = a^6 + a^4 + a^3 + a^2 + 1 , \\
a = 3 , \quad & \text{»} \quad = 2a^7 + a^6 + a^5 + 2a^2 + a + 1 , \\
a = 4 , \quad & \text{»} \quad = a^8 + a^7 + 3a^6 + a^5 + a^3 + a^2 + 3a + 1 , \\
a = 5 , \quad & \text{»} \quad = 2a^8 + a^7 + a^6 + 4a^5 + 2a^3 + a^2 + a + 4 , \\
a = 6 , \quad & \text{»} \quad = 3a^8 + a^7 + 3a^6 + 4a^5 + 5a^4 + 2a^3 + 4a^2 + 2a + 1 , \\
a = 7 , \quad & \text{»} \quad = 4a^8 + 3a^7 + a^6 + a^5 + 6a^4 + 2a^3 + 3a^2 + 5a + 5 , \\
a = 8 , \quad & \text{»} \quad = 5a^8 + 6a^7 + 4a^6 + 2a^5 + 7a^4 + 2a^3 + a^2 + 3a + 5 , \\
a = 9 , \quad & \text{»} \quad = 7a^8 + 3a^7 + 2a^6 + 4a^5 + 7a^3 + 3a^2 + 2a + 4 , \\
a = 10 , \quad & \text{»} \quad = 9a^8 + 9a^6 + 9a^4 + 9a^2 + 9 .
\end{aligned}$$

$$p = 13 .$$

$$\begin{aligned}
a = 2 , \quad & k_p(a) = a^8 + a^5 + a^4 + a^3 + a + 1 , \\
a = 3 , \quad & \text{»} \quad = 2a^9 + 2a^6 + 2a^3 + 2 , \\
a = 4 , \quad & \text{»} \quad = a^{10} + 3a^8 + 2a^7 + 3a^6 + a^4 + 3a^2 + 2a + 3 , \\
a = 5 , \quad & \text{»} \quad = a^{10} + 4a^9 + 3a^8 + a^6 + 4a^5 + 3a^4 + a^2 + 4a + 3 , \\
a = 6 , \quad & \text{»} \quad = 2a^{10} + 4a^9 + 3a^8 + 4a^7 + 5a^5 + 3a^4 + a^3 + 2a^2 + a + 5 , \\
a = 7 , \quad & \text{»} \quad = 3a^{10} + 5a^9 + 2a^8 + 4a^7 + 5a^6 + 6a^5 + 3a^4 + a^3 + 4a^2 \\
& \qquad + 2a + 1 , \\
a = 8 , \quad & \text{»} \quad = 4a^{10} + 7a^9 + 3a^8 + 4a^6 + 7a^5 + 3a^4 + 4a^2 + 7a + 3 , \\
a = 9 , \quad & \text{»} \quad = 6a^{10} + 2a^9 + 6a^7 + 2a^6 + 6a^4 + 2a^3 + 6a + 2 , \\
a = 10 , \quad & \text{»} \quad = 7a^{10} + 6a^9 + 9a^8 + 2a^7 + 3a^6 + 7a^4 + 6a^3 + 9a^2 + 2a + 3 , \\
a = 11 , \quad & \text{»} \quad = 9a^{10} + 3a^9 + 4a^8 + 2a^7 + 5a^6 + 10a^5 + a^4 + 7a^3 + 6a^2 \\
& \qquad + 8a + 5 , \\
a = 12 , \quad & \text{»} \quad = 11a^{10} + 11a^8 + 11a^6 + 11a^4 + 11a^2 + 11 .
\end{aligned}$$

En fin de compte, il faut donner une couple d'exemples correspondant au cas $a > p$. Nous choisissons $p = 5$, $a = 5.1 + 3$, $5.2 + 3$ et $5.3 + 3$. Dans la précédente équation (A) nous aurons $x = 3$, $p = 5$ et n égal à 1, 2 ou 3, ce qui nous donne :

$$\begin{aligned}
k_5(8) &= 5^3 + 4.5^2.3 + 6.5.3^2 + 4.3^3 + 3^2 + 2.3 + 1 , \\
k_5(13) &= 5^3.2^4 + 4.5^2.2^3.3 + 6.5.2^2.3^2 + 4.2.3^3 + 3^2 + 2.3 + 1 , \\
k_5(18) &= 5^3.3^4 + 4.5^2.3^4 + 6.5.3^4 + 4.3^4 + 3^2 + 2.3 + 1 .
\end{aligned}$$

Pour peu qu'on ait pensé trouver quelque relation entre le problème traité ici et celui d'*Abel*, il sera à supposer que le précédent renseignement exclura cette idée.

Finalement, il faut observer qu'en ce qui précède on ne trouvera pas le problème résolu généralement, c'est-à-dire pour des

valeurs quelconques de p et a. Aussi n'avons-nous pas démontré par induction que ce qui a lieu pour quelques valeurs de p et a serait aussi le cas pour des valeurs plus considérables.

A mon avis le cas traité est exceptionnel, et ne permet pas ces preuves ordinaires. En vérité, il me semble suffire que nous soyons à même d'éprouver l'exactitude de la loi que nous venons d'énoncer pour autant de nombres premiers que nous voulons, et de savoir que, dans autant de cas, notre exposition sera juste.

Copenhague, le 1er juillet 1916.

SUR UNE TRANSFORMATION PROJECTIVE CONDUISANT A QUELQUES PROPRIÉTÉS MÉTRIQUES

PAR

F. GONSETH (Zurich).

I

1. — Dans un plan non-euclidien, nous allons supposer que la conique absolue soit réciproque de celle du plan euclidien, c'est-à-dire qu'elle se réduise à deux droites. Nous examinerons ensuite la métrique de ce plan avec un œil euclidien.

Aux notions *d'angle de deux droites,* de *distance d'un point à une droite,* et *de distance de deux points* vont correspondre les notions au sens non-euclidien de distance de deux points, de distance d'une droite à un point, et d'angle de deux droites.

2. — Supposons que la conique absolue de ce plan soit formée des deux droites isotropes de l'origine

$$x^2 + y^2 = 0 \ .$$

Pour passer des premières notions précitées aux secondes, il suffit de remplacer dans les formules usuelles les coordonnées (x, y) d'un point, par celles (u, v) d'une droite; et l'équation des points cycliques

$$u^2 + v^2 = 0$$

par celle des droites isotropes de l'origine

$$x^2 + y^2 = 0 \ .$$