Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 37 (1938)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SUR QUELQUES PROPRIÉTÉS DES NOMBRES DE LA FORME $a^m + b^m$
Autor: KULAKOFF, A.
DOI: https://doi.org/10.5169/seals-28589

SUR QUELQUES PROPRIÉTÉS DES NOMBRES DE LA FORME $a^m + b^m$

PAR

A. KULAKOFF (Moscou).

Dans mon travail: *Sur quelques propriétés des groupes finis* [1] j'ai démontré le théorème suivant: *soit* p *un nombre premier impair, et* α *un nombre entier tel que* $\alpha^p \equiv 1 \pmod{k}$. *Alors une congruence linéaire de la forme:*

$$(\alpha^{i+1} - 1)x \equiv \alpha^i - 1 \pmod{k}, \qquad (1 \leq i \leq p-2)$$

admet nécessairement une solution.

C'est en essayant de généraliser ce théorème que je suis arrivé aux résultats du présent article.

§ 1. — Soient a et b deux nombres entiers positifs, premiers entre eux, et tels que $ab \neq 1$. Nous allons démontrer que le plus grand commun diviseur d des nombres $a^m + b^m$ et $a^n + b^n$ divise l'un au moins des nombres $a^\delta + b^\delta$ et $a^\delta - b^\delta$, où $\delta = (m, n)$.

Soit $m \geq n$. Si m est divisible par n, le théorème est évidemment vrai.

Supposons maintenant que

$$m = \nu n + \sigma_1 \qquad (1 \leq \sigma_1 < n)$$
$$n = \sigma_1 n_1 + \sigma_2 \qquad (0 \leq \sigma_2 < \sigma_1)$$
$$\cdots\cdots\cdots\cdots$$

[1] *Recueil mathématique* (nouvelle série), t. 1, fasc. 2, p. 253 (1936).

Il est clair que d divise le nombre

$$a^m + b^m - b^{m-n}(a^n + b^n) = a^n(a^{m-n} - b^{m-n}) .$$

Or d est premier à a^n, puisque d est un diviseur de $a^n + b^n$, donc d divise $a^{m-n} - b^{m-n}$.

Il en résulte que d divise aussi le nombre

$$a^{m-n} - b^{m-n} + b^{m-2n}(a^n + b^n) = a^n(a^{m-2n} + b^{m-2n}) ,$$

et par suite le nombre $a^{m-2n} + b^{m-2n}$.

En continuant ainsi, nous démontrerons que d divise l'un au moins des nombres $a^{\sigma_1} + b^{\sigma_1}$ et $a^{\sigma_1} - b^{\sigma_1}$. Si donc $\sigma_2 = 0$, le théorème est démontré. Si $\sigma_2 > 0$, d divise l'un des nombres $a^{\sigma_2} + b^{\sigma_2}$ et $a^{\sigma_2} - b^{\sigma_2}$.

En répétant au besoin ces raisonnements, nous établirons complètement notre théorème.

On obtient des résultats analogues pour les nombres $a^m + b^m$ et $a^n - b^n$, ainsi que pour les nombres $a^m - b^m$ et $a^n + b^n$.

Considérons à présent le cas des nombres $a^m - b^m$ et $a^n - b^n$. En suivant la marche qui a été indiquée plus haut, on démontrera que d divise $a^\delta - b^\delta$. Mais d est en même temps divisible par $a^\delta - b^\delta$, puisque δ divise chacun des nombres m et n, donc $d = a^\delta - b^\delta$.

Etudions encore le cas où m est un nombre impair, et $(m, n) = 1$. Alors $d = (a^m - b^m, a^n + b^n)$ divise 2.

En effet, dans ce cas d divise l'un au moins des nombres $a + b$ et $a - b$. Mais $(a^m - b^m, a + b)$ divise 2. On déduit cela de ce fait que même $d' = (a^m - b^m, a^m + b^m)$ divise 2, puisque d' divise

$$(a^m + b^m) + (a^m - b^m) = 2a^m ,$$

et $(a^m - b^m, 2a^m)$ divise 2.

On démontrera de même que $(a^n + b^n, a - b)$ divise 2. Notre théorème est donc établi.

En particulier, si l'un des nombres a et b est pair et l'autre impair, alors $(a^m - b^m, a^n + b^n) = 1$.

Admettons à présent que $m = p$ soit un nombre premier impair. Alors chacun des nombres

$$\left(\frac{a^p - b^p}{a - b},\ a^{p-i} - b^{p-i}\right), \qquad (i = 1, 2, \ldots, p-1)$$

divise p.

En effet, comme $(p, p - i) = 1$, on a

$$(a^p - b^p,\ a^{p-i} - b^{p-i}) = a - b,$$

d'où il suit, en vertu d'un théorème connu [1], que

$$\left(\frac{a^p - b^p}{a - b},\ a^{p-i} - b^{p-i}\right) = \left(\frac{a^p - b^p}{a - b},\ a - b\right)$$

divise p.

En se servant des résultats précédents, on obtiendra sans peine le théorème suivant: *Si* $(a, b) = 1$, $a - b \not\equiv 0 \pmod 2$ *et d'ailleurs* $\left(\frac{a^p - b^p}{a - b}, a - b\right) = 1$, *alors* $\frac{a^p - b^p}{a - b}$ *est premier à chacun des nombres.*

$$a^{p-1} - b^{p-1},\ a^{p-2} - b^{p-2},\ \ldots,\ a^2 - b^2,$$

ainsi qu'à chacun des nombres

$$a^p + b^p,\ a^{p-1} + b^{p-1},\ \ldots,\ a^2 + b^2.$$

§ 2. — Nous allons indiquer maintenant quelques applications des théorèmes précédents.

Soit $(a, b) = 1$ et $ab \not\equiv 1$. Alors on peut démontrer le théorème suivant. *Pour qu'un nombre* p *soit premier, il faut et il suffit que le plus grand commun diviseur des nombres* $a^p - b^p$ *et* $a^i - b^i$ $(i = 1, 2, \ldots, p - 1)$ *soit égal à* $a - b$.

Cette condition est nécessaire, d'après le théorème sur le plus grand commun diviseur des nombres $a^m - b^m$ et $a^n - b^n$ établi dans le § 1.

Elle est aussi suffisante. En effet, si $p = tu$ $(t > 1,\ u > 1)$, alors $(a^p - b^p,\ a^u - b^u) \not\equiv a - b$, puisque

$$a^p - b^p = a^{tu} - b^{tu} = (a^u - b^u)(a^{u(t-1)} + a^{u(t-2)} b^u + \ldots)$$

est divisible par $a^u - b^u > a - b$.

---

[1] Voir par exemple E. LUCAS, *Théorie des nombres*, t. 1, p. 341.

Considérons à présent une congruence linéaire de la forme:

$$(a^i - b^i)x \equiv a^j - b^j \pmod{k}, \qquad [(i, \mu) = (j, \mu) = 1], \quad (1)$$

où $(a, b) = 1$, $ab \neq 1$ et d'ailleurs $a^\mu \equiv b^\mu \pmod{k}$.

Cette congruence admet une solution.

En effet, comme $(i, \mu) = (j, \mu) = 1$, nous avons:

$$(a^\mu - b^\mu, \quad a^i - b^i) = (a^\mu - b^\mu, \quad a^j - b^j) = a - b .$$

Si donc $(k, a - b) = \delta$, on a aussi $(k, a^i - b^i) = (k, a^j - b^j) = \delta$.

Par conséquent, la congruence (1) est équivalente à la suivante:

$$Ax \equiv B \pmod{k'},$$

où

$$A = \frac{a^i - b^i}{\delta}, \qquad B = \frac{a^j - b^j}{\delta} \qquad \text{et} \qquad k' = \frac{k}{\delta} .$$

Comme A et k' sont premiers entre eux, notre théorème est démontré.

En posant $b = 1$, $j = i - 1$ et $\mu = p$, nous retrouvons le théorème qui a été établi par l'auteur dans l'article cité plus haut.

Mais ce dernier résultat n'est pas nouveau [1], puisqu'il découle immédiatement de ce fait connu que les nombres $\frac{x^m - 1}{x - 1}$ et $\frac{x^n - 1}{x - 1}$, où x est un nombre entier positif distinct de 1, sont premiers entre eux, toutes les fois que m et n le sont [2].

A son tour, ce théorème se laisse généraliser de la manière suivante: *Les nombres* $\frac{a^m - b^m}{a - b}$ *et* $\frac{a^n - b^n}{a - b}$, *où* $(a, b) = (m, n) = 1$ *et* $ab \neq 1$, *sont premiers entre eux.* Ce résultat paraît être nouveau.

---

[1] J'ai appris cela quelque temps après la publication de mon travail.

[2] Voir: H. C. POCKLINGTON, The divisors of certain arithmetical forms, etc. *Proceedings. Cambr. Philosoph. Soc.*, v. 16, p. 7 (1911).