Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 9 (1907)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LE LEMME FONDAMENTAL DE LA THÉORIE DES NOMBRES
Autor: Aubry, A.
Kapitel: Exercices.
DOI: https://doi.org/10.5169/seals-10154

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 13.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

division par b seront les nombres α, α', ... ; de là, en multipliant, la congruence

$$\Pi^{\varphi(b)-1} \equiv \Pi \,, \qquad \text{d'où} \qquad \Pi^{\varphi(b)} \equiv \Pi^2 \qquad (\text{mod. } b)$$

Autre démonstration. Joignons, de α en α, les sommets d'un polygone P, de b côtés, et, de x en x, ceux du deuxième polygone P′ ainsi obtenu, x étant choisi tel que le troisième polygone coïncide avec le premier P. On a ainsi pris les sommets de αx en αx, ce qui produit le même résultat que si on les avait pris de 1 en 1. Ainsi si α est premier avec b, il y aura toujours un nombre x tel que $\alpha x \equiv 1$ (mod. b)[1].

Si $x = \alpha$, et qu'on prenne les sommets de P′ de $b - \alpha$ en $b - \alpha$, on retombera sur le polygone P renversé ; donc $\alpha(b - \alpha)$ revient à -1 ou bien $\alpha(b - \alpha) \equiv -1$ (mod. b).

Ainsi, dans tous les cas, les nombres 1, α, α', ... $b - 1$ peuvent s'associer de manière que leur produit soit de la forme ± 1 (mod. b) : on peut donc écrire

$$\Pi \equiv \pm 1 \qquad (\text{mod. } b).$$

selon que le nombre des produits de la forme -1 (mod. b), est pair ou impair[2].

Exercices.

1. La somme des quotients provenant de la division par b des nombres a, $2a$, $3a$, ... $(b - 1)\,a$, est égale à $\frac{1}{2}(a - 1)(b - 1)$. (Gauss).

---

[1] De là, une solution graphique de la congruence $\alpha x - by = 1$. (Poinsot).

[2] Si b est un nombre premier p, la démonstration se simplifie ainsi, d'après Cayley.

D'après ce qui a été dit, *Cor. XIII*, 2°, premier alinéa, b points disposés régulièrement sur une circonférence sont les sommets de $\frac{\varphi(b) + 1}{2}$ polygones réguliers de b côtés ; d'où, si q est premier et égal à p, $\frac{1}{2}(p - 1)$ polygones.

Or le nombre total des polygones, tant réguliers qu'irréguliers, est évidemment la moitié du nombre des permutations de $p - 1$ objets, puisque ces polygones se reproduisent deux à deux. D'un autre côté, si nous faisons tourner autour de son centre, et successivement des angles $\frac{2\pi}{p}$, $\frac{4\pi}{p}$, $\frac{6\pi}{p}$, ... $\frac{2(p-1)\pi}{p}$, un polygone irrégulier quelconque, nous obtiendrons $p - 1$ autres polygones irréguliers : le nombre des polygones irréguliers possibles est donc un multiple de p. De là, la relation

$$\frac{1}{2}(p - 1)! - \frac{1}{2}(p - 1) \equiv 0 \,.$$

2. Si $x = \alpha$, $y = \beta$ est une solution de $ax - by = 1$; $x = c\alpha$, $y = c\beta$ en est une de $ax - by = c$.

3. Trouver x tel que $x \equiv \alpha$ (mod. a) et $x \equiv \beta$ (mod. b).

On cherche $b\mathrm{A} \equiv 1$ (mod. a) et $a\mathrm{B} \equiv 1$ (mod. b), ce qui donne

$$x \equiv \mathrm{A}b\alpha + \mathrm{B}a\beta \qquad (\text{mod. } ab)$$

4. Soit g celui des $b - 1$ premiers entiers positifs qui rend $c - ag$ multiple de b, l'équation $ax + by = c$ a un nombre de solution représenté par la *formule de Paoli,*

$$\mathrm{E}\left(\frac{c - ag}{ab}\right) + 1 .$$

5. La solution de $ax - by = c$ est donnée par la *formule de Libri,*

$$x = \frac{c-1}{2} + \frac{1}{2} \sum_{k=1}^{k=b} \frac{\sin \dfrac{(2c - a)\, k\pi}{b}}{\sin \dfrac{ak\pi}{b}} .$$

6. Soit μ le plus grand commun diviseur des nombres donnés α, β, γ, ... On peut toujours déterminer les nombres A, B, C, ... de manière qu'on ait

$$\frac{\mathrm{A}}{\alpha} + \frac{\mathrm{B}}{\beta} + \ldots = \mu \qquad \text{(Gauss).}$$

7. Résoudre les équations

$$x'y'' - x''y' = a\,,\ x''y - xy'' = a'\,,\ xy' - x'y = a''. \qquad \text{(Gauss)}$$

8. Soit à résoudre les équations

$$x = ay + \alpha = bz + \beta = cw + \gamma = \ldots$$

a, b, c, ... étant premiers deux à deux. On pose $\mathrm{P} = abc \ldots$ et on calcule a', b', c', ... de manière qu'on ait

$$\frac{\mathrm{P}}{a}\, a' \equiv 1 \ (\text{mod. } a)\ , \qquad \frac{\mathrm{P}}{b}\, b' \equiv 1 \ (\text{mod. } b)\ , \ldots$$

d'où

$$x = \mathrm{P}\left(\frac{a'\alpha}{a} + \frac{b'\beta}{b} + \ldots\right)$$

Le problème est ramené au calcul des associés de $\frac{P}{a}$, ... (Voir exercices n°s 10, 11 et 22).

9. *Regula cœci.* Partager A en n parties telles que a fois la première, b fois la deuxième, ... fassent ensemble une somme B.

Supposons que a est le plus petit des nombres $a, b, c, \ldots$ On a :

$$(b - a)\, y + (c - a)\, z + \ldots = \mathrm{B} - a\mathrm{A}\,,$$

équation de la forme $\alpha y + \beta z + \ldots = \mathrm{C}$, qu'on résout en remarquant qu'il y a au moins deux coefficients, α et β par exemple, qui sont premiers entre eux, ce qui permet de poser

$$\alpha\alpha' + \beta\beta' = 1\,, \quad \text{d'où} \quad x = \alpha'(\mathrm{C} - \gamma\alpha - \ldots) + \beta\lambda\,,$$
$$y = \beta'(\mathrm{C} - \gamma\alpha - \ldots) + \alpha\mu\,, \ldots$$

λ, μ, ... désignant des quantités indéterminées.

10. Divisons a par b, b par le reste, ce reste par le second reste, et ainsi de suite, de sorte qu'on ait

$$a = \alpha b + c\,, \quad b = \beta c + d\,, \quad c = \gamma d + e\,, \ldots$$

α, β, ... sont entiers et b, c, ... diminuent jusqu'à ce qu'on parvienne à $m = \mu n + 1$.

Formons les expressions

$$[\alpha] = \alpha = \mathrm{A}$$
$$[\alpha, \beta] = \beta\mathrm{A} + 1 = \mathrm{B}\,,$$
$$[\alpha, \beta, \gamma] = \gamma\mathrm{B} + 1 = \mathrm{C}\,,$$
$$\ldots\ldots\ldots\ldots$$

on aura

$$[\alpha, \beta, \ldots \mu]\,[\beta, \ldots \lambda] - [\alpha, \ldots \lambda]\,[\beta, \ldots \mu] = \pm 1\,.$$

De là le moyen de résoudre $ax - by = \pm 1$[1].

11. Soient r_1, r_2, r_3, ... et q_1, q_2, q_3, ... les restes et les quotients obtenus successivement en divisant p par a, r_1, r_2, r_3, ... Les restes sont tous différents de zéro et décroissent jusqu'à $r_n = 1$. On a :

$$a q_1 q_2 \cdots q_{n-1} \equiv -(-1)^n$$

[1] Les théories que contiennent les exercices 2, 3, 8, 9 et 10 étaient connues des Indiens, comme on le voit chez Brahmegupta et Bhaskara. Mais c'est seulement Bachet qui a commencé à les exposer avec méthode et en détail.

De là, la solution de $ax \equiv \pm 1$. (Binet).

12. a et b étant premiers entre eux, le produit

$$\frac{x^a - 1}{x - 1} \frac{x^b - 1}{x - 1}$$

est divisible par $\frac{x^{ab} - 1}{x - 1}$ (Gauss).

13. Si on peut écrire $a^2 \equiv r$ et $b^2 \equiv -r$, on a : $x^2 \equiv -1$ (Euler). En effet posons $ax \equiv b$, il viendra $a^2x^2 \equiv b^2 \equiv -a^2$. (Gauss).

14. Soient $a^2 \equiv r$, $b^2 \equiv rs$, on peut écrire $x^2 = s$ (Euler). En effet posons $ax \equiv b$, il viendra $rs \equiv b^2 \equiv a^2x^2 \equiv rx^2$. (Gauss).

15. Soit $a^g \equiv a^h \equiv r$, g et h étant premiers entre eux, on peut écrire $r^z \equiv a$. En effet posons $gx - hy = 1$, il viendra

$$r^x \equiv a^{gx} = a^{hy+1} \equiv ar^y \ . \qquad \text{(Legendre).}$$

16. Aucun nombre non décomposable en deux carrés entier ne l'est pas non plus en deux carrés fractionnaires (Fermat).

17. L'égalité $ax^2 - y^2 = 1$ ne peut avoir lieu si a n'est pas la somme de deux carrés. (Brahmegupta).

18. Les diviseurs du nombre $a^2 - 3b^2$ sont de l'une des formes quadratiques $\pm x^2 \mp 3y^2$, ou de l'une des formes linéaires $\mathbf{12} \pm 1$. (Lagrange).

19. Les nombres $a^4 + 1$ et $a^4 - a^2 + 1$ sont respectivement des deux formes linéaires $\mathbf{8} + 1$ et $\mathbf{12} + 1$. En effet on peut les écrire

$$(a^2 - 1)^2 + 1 \quad \text{et} \quad (a^2 - 1)^2 + a^2 = (a^2 + 1)^2 - 3a^2. \quad \text{(Serret).}$$

20. Si l'un des coefficients A, B, est multiple de p, la congruence $Ax^n + Bx^{n-1} + \ldots + M \equiv 0$ ne saurait avoir n racines.

Il en est de même si $M \equiv 0$.

Si elle a n racines, a, b, ... on peut l'écrire $A(x - a)(x - b) \ldots \equiv 0$ et l'on a :

$$A(a + b + \ldots) + B \equiv 0 \ , \quad ab \ldots \equiv \pm M \ .$$

21. Du *Cor. XI,* déduire la relation

$$s_{p-1,\,p-1} \equiv (p-1)\,!$$

ainsi que le *Cor. IX.*

22. Posons $a^{\varphi(b)} = kb + 1$, on aura

$$a\,(ca^{\varphi(b)-1}) - b\,(ck) = c$$

d'où une solution de $ax - by = c$ (Poinsot). Ainsi l'associé de a relativement à b est

$$x = a^{\varphi(b)-1}$$

23. Trouver x tel que $x \equiv \alpha$ (mod. a) et $\equiv \beta$ (mod. b). On a :

$$x = b^{\varphi(a)}\,\alpha + a^{\varphi(b)}\,\beta \qquad \text{(mod. } ab\text{)}.$$

Ainsi les nombres à la fois des deux formes $3 + 1$ et $4 - 1$ sont de la forme $12 + 7$; ceux des formes $3 - 1$ et $4 + 1$, de la forme $12 + 5$; ceux des formes 3 ± 1 et 4 ± 1, de la forme 12 ± 1.

24. Changeons successivement x et y en $1, \alpha, \alpha', \ldots b - 1$ dans la relation $a \equiv xy$ (mod. b) et multiplions, il viendra

$$a^{\varphi(b)} \equiv -\Pi^2 \quad \text{(mod. } b\text{)} \qquad \text{d'où} \qquad \Pi^2 \equiv 1 \quad \text{(mod. } b^2\text{)}$$

25. Démontrer les relations

$$\frac{(p-1)\,(p-2)\,\ldots\,m}{\left(\frac{p+1}{2}\right)\,!} \equiv (-1)^m\,. \qquad \text{(Lebesgue).}$$

$$(a-1)\,!\,(p-a)\,! \equiv (-1)^a\,. \qquad \text{(Lagrange).}$$

A. Aubry (Beaugency, Loiret).