LE PREMIER CHAPITRE DE LA THÉORIE ÉLÉMENTAIRE DES NOMBRES

Autor(en): **Aubry, A.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **17 (1915)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-16318

LE PREMIER CHAPITRE DE LA THÉORIE ÉLÉMENTAIRE DES NOMBRES

PAR

A. AUBRY (Dijon).

AVANT-PROPOS. — *Plusieurs jeunes correspondants m'ont si souvent demandé des renseignements sur les tout premiers éléments de la théorie élémentaire des nombres, que j'ai pensé qu'il serait utile d'en écrire un chapitre introductif faisant simplement pressentir l'esprit et les méthodes de cette théorie.*

J'ai donc écrit ce chapitre, — par lequel j'aurais dû commencer mes études, — en y définissant les idées et les procédés particuliers à cette science. J'ai ainsi rassemblé des formules, des théories et des problèmes épars un peu partout et dont le rapprochement fait mieux et plus rapidement pénétrer le sujet, en même temps qu'il suggère de nouveaux points de vue et de nouvelles démonstrations. J'ai complété par des problèmes célèbres ou utiles, que j'ai traités accessoirement et seulement à titre d'application : il est aisé de se proposer autant qu'on voudra de problèmes indéterminés, et souvent assez aisé d'en trouver une, plusieurs ou même une infinité de solutions ; — mais les cas sont rares où on peut trouver la solution générale, et cependant c'est dans ce seul cas que le problème peut être considéré comme résolu. — Car peut-on se déclarer entièrement satisfait de savoir uniquement que tel nombre répond à telle question ? *Ce nombre a-t-il une particularité qui le distingue ? Est-il seul ? le plus grand ? le plus petit ? le plus facile à découvrir ?*

Il semble d'ailleurs qu'il y aurait lieu de réagir contre cette marée montante des problèmes particuliers, menaçant de submersion la science elle-même, et qu'il faudrait se borner à des recueils d'exercices choisis : intéressants, comme énoncés ou démonstrations ; utiles, comme illustrations de théories ou sujets d'études ; enfin, et surtout, susceptibles d'une réponse complète et précise.

La théorie des nombres [1] *comporte trois degrés bien définis :*

---

[1] Ce mot, qui désigne si mal son objet, ne peut être remplacé par l'appellation exacte d'*arithmétique*, détournée de son sens. On a proposé la dénomination d'*arithmologie*, qui ne vaut pas mieux et peut-être même moins que théorie des nombres ; *arithmonomie* serait mieux mais est trop long ; l'abrégé *arithnomie* me conviendrait assez, mais je n'ai pas voulu créer un néologisme.

*l'*arithmétique élémentaire, *qui pourrait porter le nom d'Euclide, et dont le traité le plus récent est le recueil d'exercices, de Fitz-Patrick ;*

la théorie élémentaire des nombres, *ou arithmétique de Fermat, mise en lumière par Euler et Lagrange, et pour la vulgarisation de laquelle j'ai écrit mes articles de l'*Ens. Math. ;

enfin la théorie générale des nombres, *ou arithmétique de Gauss, que beaucoup ne peuvent ou ne veulent pas entreprendre : M. Cahen vient de publier le premier volume de cette dernière.*

Les domaines des deux premiers stades sont aujourd'hui bien délimités ; aussi, là, on peut entrer en matière tout de suite. C'est pourquoi j'estime suffisant le chapitre introductif tel que je l'ai conçu, sans qu'il y soit besoin de préliminaires plus étendus.

A. Aubry (Dijon).

1. *Définitions.* La *théorie élémentaire des nombres* traite des relations des nombres entiers entre eux, et particulièrement des *formes* sous lesquelles ils peuvent être mis, ainsi que leurs diviseurs et leurs multiples.

Dans tout ce qui suit, sauf indication contraire, toutes les lettres représentent des nombres entiers.

Les coefficients a, b, c, désignant des entiers donnés, on dit qu'un nombre n est de la *forme linéaire* $ax + b$, ou de la *forme quadratique* $ax^2 + bxy + cy^2$, quand on peut déterminer, — ou tout au moins prouver qu'il existe, — certaines valeurs entières de x, ou de x et de y, qui rendent la valeur de cette expression égale à n. On dit également qu'on peut, dans les mêmes cas, écrire $n = ax + b$ ou $n = ax^2 + bxy + cy^2$.

Ainsi 47 est des deux formes $4x + 3$ et $x^2 + 3xy + 7y^2$, car, faisant $x = 11$ dans la première, et $x = 5$, $y = 1$ dans la seconde, on trouve 47.

Le plus souvent, les coefficients a, b, c n'ont pas de facteur commun : la forme est alors dite *primitive*.

2. *Rappel des théorèmes fondamentaux.* Les recherches de ce genre empruntent à l'algèbre l'art du calcul littéral et celui de la transformation des formules ; elles s'appuient en outre sur quelques propositions arithmétiques élémentaires, qu'il suffira de rappeler et qu'on trouve déjà, au moins implicitement, chez Euclide.

Tout diviseur de a *et de* b *divise* ka + lb *et en particulier* a + b *et* a — b. Réciproquement, *si* c *divise* a *et non* b, *il ne divise pas* a ± b.

Tout nombre divisible par plusieurs entiers premiers entre eux, l'est par leur produit.

Si un nombre divise un produit de deux facteurs et qu'il soit premier avec l'un de ces facteurs, il divise l'autre.

Tout nombre premier qui divise un produit divise au moins un des facteurs de ce produit.

Un nombre premier avec plusieurs autres l'est avec leur produit. En particulier, *le produit de plusieurs entiers inférieurs à un nombre premier donné, ne peut être divisible par celui-ci.*

Un nombre est une puissance n^ième *si les exposants de ses facteurs sont tous des multiples de* n.

Si deux nombres sont premiers entre eux, il en est de même de leurs puissances.

Si un nombre premier divise a^n, *il divise également* a.

3. *Congruences.* Deux entiers a et b, qui ne diffèrent que d'un multiple de l'entier n, sont dits, d'après Gauss, *congrus* par rapport au *module* n[1], et cette relation s'indique par la notation

$$(\alpha) \qquad a \equiv b \ . \qquad (\mathrm{mod}\ n)$$

Par exemple, on a :

$$(1) \qquad (nx + a)(nx' + a') \equiv aa' \ . \qquad (\mathrm{id.})$$

De (α), on tire :

$$(2) \qquad a + c \equiv b + c \ , \qquad ka \equiv kb \ . \qquad (\mathrm{id.})$$

Si $A \equiv a$, $B \equiv b$, $C \equiv c$, ... (mod n), on peut écrire :

$$(3) \qquad \left.\begin{aligned} A + B &\equiv a + b \ , \\ fA + gB + hC + \ldots &\equiv fa + gb + hc + \ldots \end{aligned}\right\} \quad (\mathrm{mod}\ n)$$

$$(4) \qquad ABC \ldots \equiv abc \ldots \qquad (\mathrm{id.})$$

d'où

$$(5) \qquad A^k \equiv a^k \ . \qquad (\mathrm{id.})$$

---

[1] Le plus souvent, b représente le reste de la division de a par n; on écrit alors $b = R\,\frac{a}{n}$.

Si $ka \equiv kb \pmod{n}$ et que d soit le p. g. c. d. de k et de n, on a :

$$a \equiv b . \qquad \left(\mathrm{mod}\ \frac{n}{d}\right) \tag{6}$$

On appelle *congruence* une expression algébrique de la forme $Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots Lx + M \equiv 0 \pmod{n}$, où les coefficients A, B, ... L, M sont entiers ou nuls, et les valeurs de x astreintes à être également des nombres entiers.

Les valeurs de x inférieures à n qui satisfont à cette congruence sont les *racines* de celle-ci; les autres sont ses *non-racines*. Ainsi les nombres 1, 3, 4 sont les racines de $x^3 - 3x^2 - x + 3 \equiv 0 \pmod{5}$ et 0, 2, ses non-racines. La congruence $x^2 + 2x + 5 \equiv 0 \pmod{7}$ n'a aucune racine : elle a donc les non-racines 0, 1, 2, 3, 4, 5, 6.

4. *De quelques formes particulières.* Les formes linéaires s'indiquent d'une manière plus expressive au moyen de caractères gras : ainsi l'expression $4x + 1$, qui désigne un multiple de 4 augmenté de 1, s'écrira $\mathbf{4} + 1$. On remarquera que les formules $\mathbf{4} + 3$, $\mathbf{6} + 4$, par exemple, peuvent s'écrire aussi $\mathbf{4} - 1$, $\mathbf{6} - 2$; on peut souvent de la sorte condenser deux formules en une seule : ainsi on écrira « les formules $\mathbf{8} \pm 3$ » au lieu de « la formule $\mathbf{8} + 3$ ou la formule $\mathbf{8} + 5$ ».

Voici maintenant quelques propositions très simples, la plupart assez connues, et qu'on pourrait étendre indéfiniment.

Le produit de plusieurs entiers est pair si l'un d'eux est pair, et il est impair si tous sont impairs.

Tout entier est de l'une des deux formes $\mathbf{2}$, $\mathbf{2} + 1$; *ou de l'une des trois formes* $\mathbf{3}$, $\mathbf{3} \pm 1$; *ou de l'une des quatre formes* $\mathbf{4}$, $\mathbf{4} \pm 1$, $\mathbf{4} + 2$; *etc.*

Tout nombre premier, sauf 2, *est de l'une des formes* $\mathbf{4} \pm 1$.

Tout nombre premier, sauf 2 *et* 3, *est de l'une des formes* $\mathbf{6} \pm 1$.

De même, *tout nombre premier est de l'une des quatre formes* $\mathbf{10} \pm 1$, $\mathbf{10} \pm 3$; *ou de l'une des quatre suivantes* $\mathbf{12} \pm 1$, $\mathbf{12} \pm 5$; *etc.*

Le produit de nombres de la forme $ax + 1$ *est* isomorphe (de la même forme). Ainsi $(6.5 + 1)(6.9 + 1) = 6.284 + 1 = \mathbf{6} + 1$. Conséquence de (1).

Tout nombre impair est de l'une des formes 4 ± 1, *selon que le nombre de ses facteurs* $4 - 1$ *est pair ou impair.* Car le produit de deux nombres $4 + 1$ donne un produit $4 + 1$, ainsi que celui de deux nombres $4 - 1$, tandis que $(4f + 1)(4g - 1) = 4 - 1$. On conclut de là que *tout nombre* $4 - 1$ *a quelque diviseur isomorphe.* Id.

Tout nombre impair et non multiple de 3 *est de l'une des formes* 6 ± 1, *selon que le nombre de ses facteurs* $6 - 1$ *est pair ou impair.* Id.

Le carré d'un nombre entier est pair ou impair, selon que ce nombre est lui-même pair ou impair. Id.

Le carré de $2a \pm b$ *est de la forme* $4ax + b^2$. *Si* a *et* b *sont impairs, ce carré est de la forme* $8ax + b^2$. Ainsi *les carrés de nombres des formes* 2, $2 + 1$, 6 ± 1, 6 ± 2 *sont respectivement des formes* 4, $8 + 1$, $24 + 1$, $12 + 4$.

Aucun nombre 8 ± 2, 8 ± 3, ou $8 - 1$ *ne peut être un carré.* Ainsi $x^2 + 4y + 2$ ne peut représenter un carré, car, selon que x est pair ou impair, cette expression prend la forme $4 + 2$ ou la forme $4 + 3$, qui ne peuvent convenir à un carré. De même, pour x différent de zéro, aucune des expressions $x^2 \pm 1$, $x^2 \pm x + 1$, $x^2 \pm 2x$, ... ne peut représenter un carré; de même $x^2 + 4x + 5$, puisque cette expression peut s'écrire $(x + 2)^2 + 1$.

Tout carré est de l'une des formes 9 *ou* $3 + 1$; *ou de l'une des suivantes* 25 *ou* $5 + 1$; *etc. Tout bicarré est de l'une des formes* 625 *ou* 5 ± 1; *etc.* (Voir exercice n° 10.)

Soit k *impair, le nombre* $y^2 + kz^2$ *ne peut être premier si* y *et* z *sont de parités différentes.* 1° En particulier, soit $k = 1$; le nombre impair $y^2 + z^2$ n'est pas premier s'il n'est pas de la forme $4 + 1$.

2° Soit $k = \pm 2$; $y^2 \pm 2z^2$ n'est impair que si y est impair, et alors la formule linéaire de $y^2 + 2z^2$ est $8 + 1$ ou $8 + 3$; celle de $y^2 - 2z^2$ est $8 + 1$ ou $8 - 1$.

3° Soit $k = 3$; si y est impair et z pair, y ne peut être que 6 ± 1, son carré 24 ± 1 et celui de z, 4, de sorte que $y^2 + 3z^2 = 12 + 1$. Si y est pair et z impair, on a les deux cas

$$y = 6 \pm 2 \quad \text{et} \quad z = 6 \pm 1 \quad \text{ou} \quad 6 + 3 ,$$

d'où $y^2 + 3z^2 = 12 + 7$. Ainsi *si le nombre* $y^2 + 3z^2$ *est premier, il est de la forme* $6 + 1$.

5. *Analyse indéterminée.* On appelle *équations indéterminées* un système d'équations en nombre inférieur à celui des inconnues, lesquelles sont supposées entières; et *analyse indéterminée* l'art de les résoudre ou de démontrer leur insolubilité. On connaît seulement la résolution des équations indéterminées des deux premiers degrés; et encore les calculs qu'elles nécessitent la rendent-elle à peu près illusoire, tout au moins pour le second; aussi, le plus souvent, les résout-on par des tâtonnements méthodiques, qu'on cherche à rendre aussi rapides que possible.

Occupons-nous de l'importante équation $ax^2 + bx + c = y^2$. Comme il ne s'agit que de nombres entiers, la première idée qui se présente est d'essayer pour x, successivement les nombres 1, 2, 3, ..., soit directement, ou mieux à l'aide de la méthode des différences. Mais comme le plus souvent, le nombre des solutions, c'est-à-dire des valeurs satisfaisant au système, est peu considérable, il est préférable d'essayer de déterminer les régions où *peuvent* se trouver des solutions : par exemple, on localisera notablement les recherches si on arrive à fixer des limites inférieures ou supérieures des solutions. Ou bien, — ce qui sera à la fois plus facile et plus avantageux, — on essaiera de déterminer les régions, — en général bien plus vastes, — où il ne peut se trouver aucune solution; l'idée de ce procédé est due à Frénicle, qui lui a donné le nom d'*exclusion*.

Applications. Soit à résoudre $4x^2 + 5x + 7 = y^2$. On écrira :

pour $x = 0$, $4x^2 + 5x + 7 = 7$ 9

..... 1 ..... 16 8 17

..... 2 ..... 33 8 25

..... 3 ..... 58 8 33

..... 4 ..... 91 8 41

..... 5 ..... 132 8 49

. . . . . .

jusqu'à ce qu'on arrive à un carré. Ou bien on circonscrira les régions des nombres à essayer, en écartant de prime abord les valeurs inacceptables, à cause de leur forme linéaire, et essayant ensuite les nombres non exclus.

Ainsi les expressions $15x^2 + 30x + 17$ et $15x^2 + 30x + 14$ ne peuvent représenter un carré : la première, parce qu'elle est de la forme $\mathbf{3} - 1$; la deuxième, parce que, d'une part, une valeur paire de x la rendrait de la forme $\mathbf{4} + 2$, et qu'en posant $x = 2y + 1$, elle deviendrait $60y^2 + 120y + 59$, formule qui ne peut représenter un carré, que y soit pair ou qu'il soit impair, car elle ne donne que des résultats de forme $\mathbf{4} - 1$, ou, plus simplement, parce qu'elle est de la forme $3x^2 + 2$, qui ne convient point à un carré.

On peut utiliser la remarque suivante : posons $x = fy + g$, il viendra :

$$ax^2 + bx + c \equiv ag^2 + bg + c \pmod{f}.$$

Par exemple, pour $x = \mathbf{8} + 0, 1, 2, 3, 4, 5, 6, 7$ [1], on a :

$$4x^2 + 5x + 7 = \mathbf{8} + 7, 0, 1, 2, 7, 4, 5, 6 :$$

il y a donc lieu d'essayer seulement les valeurs $x = \mathbf{8} + 1, 2, 5$, c'est-à-dire les nombres 9, 10, 13, 17, 18, 21, ...

Soit $15x^2 + 13x + 11$. Le module 2 n'apprend rien, mais l'emploi du module 3 fait voir que cette expression ne peut représenter un carré si x est $\mathbf{3}$ ou $\mathbf{3} - 1$. Posons donc $x = 3y + 1$; on trouve $135y^2 + 129y + 39$, formule qui ne peut donner un carré que si $y = \mathbf{5}$, ou $\mathbf{5} - 1$, ou $\mathbf{5} - 2$, c'est-à-dire si $x = 2y + 1$ est de la forme $\mathbf{15} + 1$, ou $\mathbf{15} - 2$ ou $\mathbf{15} - 5$. On essaiera donc les nombres 10, 13, 16, 25, 28, 31, 40, 43, 46, 55, 58, 59, ... en écartant, sans autre examen, les valeurs de la forme non terminées par l'un des groupes suivants :

00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64,
69, 76, 81, 84, 89, 96,

par lesquels se terminent les carrés numériques.

On pourrait du reste examiner encore ce que produisent

[1] Abréviation de $8 + 0$, $8 + 1$, $8 + 2$, etc.

les suppositions $y = 7, 7+1, 7+2, \ldots 11, 11+1, \ldots$ etc., ce qui donnerait d'autres conditions réduisant encore le nombre des essais. Ainsi, avec les valeurs $x = 7+2, 3, 5, 6$, l'expression proposée ne peut être un carré : il n'y a donc pas lieu de faire les substitutions $x = 9, 10, 12, 13, 16, 17, 19, 20, 30, 31, 33, 34, 36, 37, 39, 40, 44, 45, 47, \ldots$; on substituera seulement les valeurs $x = 25, 28, 43, 46, 70, 85, 88, 91, 106, \ldots$ pouvant conduire à des carrés. S'il y a des solutions[1], on les trouvera ainsi avec beaucoup moins de peine. (Voir les exercices n^{os} **24** et suivants.)

6. *Identités.* Bien que les relations indiquées par des identités algébriques s'appliquent aussi bien aux nombres non entiers qu'aux nombres entiers, elles n'en sont pas moins importantes en arithmétique, comme fournissant souvent des conditions permettant d'éliminer de nombreuses classes de nombres dans certaines recherches, et par suite de les rendre plus accessibles, et les tâtonnements moins nombreux et mieux ordonnés. A ce titre, il convient de rappeler plusieurs identités, qu'on démontrera en les considérant comme résultant de transformations d'identités connues ou évidentes.

Ainsi la suivante

$$A - C = (A - B) + (B - C)$$

donne, en faisant

$$A = \frac{1}{\alpha - \beta}, \qquad B = \frac{1}{\alpha - \gamma}, \qquad C = \frac{1}{\alpha - \delta},$$

puis

$$\alpha = \frac{a}{a'}, \qquad \beta = \frac{b}{b'}, \qquad \gamma = \frac{c}{c'}, \qquad \delta = \frac{d}{d'},$$

l'*identité de Fontaine*[2]

$$(7) \qquad (ac' - a'c)(bd' - b'd) = (ad' - a'd)(bc' - b'c) + (ab' - a'b)(cd' - c'd),$$

[1] En réalité, il n'y en a pas. Voir l'exercice **24**, 6°.

[2] *Traité de calcul différentiel et intégral* (Paris, 1770). Cette identité lui sert à l'intégration de nombreuses classes de différentielles rationnelles.

laquelle, pour $d' = b$, $b' = -d$, $c' = \pm a$, $a' = \mp c$, se transforme en l'*identité de Fibonacci*

$$(8) \qquad (a^2 + c^2)(b^2 + d^2) = (ab \pm cd)^2 + (bc \mp ad)^2 ,$$

qui montre que *le produit de deux sommes de deux carrés est isomorphe, et cela de deux manières différentes, à moins qu'on ait* ad = bc. De là, en conséquence, le moyen de résoudre, d'une infinité de manières, l'équation indéterminée $x^2 + y^2 = z^2 + w^2$.

7. L'identité

$$(9) \qquad (\alpha + \beta)(\alpha - \beta) = \alpha^2 - \beta^2$$

est fréquemment utilisée. Ainsi : 1° faisant $\alpha = a^2 + b^2$ et $\beta = a^2 - b^2$, on trouve celle-ci

$$(10) \qquad (a^2 + b^2)^2 = (a^2 - b^2)^2 + (2ab)^2$$

entrevue par Pythagore et Platon et qui fournit une infinité de solutions de l'équation $x^2 + y^2 = z^2$ [1]. (Voir exercices n^{os} 6 et 58.)

2° Faisant $\alpha = a^2 + b^2$, $\beta = \sqrt{2}\,ab$, on trouve cette identité de Leibniz

$$(11) \qquad a^4 + b^4 = (a^2 + \sqrt{2}\,ab + b^2)(a^2 - \sqrt{2}\,ab + b^2) ,$$

laquelle devient, en changeant b en $\sqrt{2}\,b$, cette autre d'Euler

$$(12) \qquad a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2) ,$$

qui démontre ces trois propositions de Goldbach, de Sophie Germain et d'Aurifeuille : *aucun nombre* $4x^4 + 1$, $x^4 + 4$ *ou* $2^{4x+2} + 1$ *n'est premier, sauf le nombre* 5 [2]. On n'a qu'à faire $a = 1$, $b = x$; $a = x$, $b = 1$; $a = 1$, $b = 2^x$.

8. Cette identité d'Euler

$$(13) \qquad (1 + a)(1 + b)(1 + c)\ldots = 1 + a + b(1 + a) + c(1 + a)(1 + b) + \ldots$$

---

[1] Les nombres x, y, z sont dits alors former un *triangle* (rectangle), dont z est l'*hypoténuse*, et y, z, les *cathètes*. Les nombres a et b sont les *générateurs* du triangle.

[2] Landry n'avait pu arriver à décomposer en ses facteurs le nombre $2^{58} + 1$ qu'au prix de calculs des plus laborieux, et il pensait que si cette décomposition venait à se perdre, bien des siècles se passeraient avant qu'on la retrouvât. Or on voit immédiatement que ce nombre est le produit de deux facteurs $2^{29} + 2^{15} + 1$ et $2^{29} - 2^{15} + 1$.

en fournit beaucoup d'autres, la plupart fort intéressantes. Il suffira de mentionner les cas particuliers suivants.

1° Pour $a = b = c = \ldots = x - 1$, on a celle-ci d'Eudoxe

$$1 + x + x^2 + \ldots + x^{n-1} = \frac{x^n - 1}{x - 1}, \tag{14}$$

qui donne cette autre démonstration de (5) : posons $x = \frac{a}{b}$, $b = a + hn$; le nombre $(a + hn)^k - a^k$ est divisible par $(a + hn) - a$, donc, de $b \equiv a \pmod{n}$, on déduit $b^k \equiv a^k \pmod{n}$.

Ainsi $a^k - b^k$ *est divisible par* $a - b$; donc, en mettant $-b$, au lieu de b, $a^k - (-b)^k$ *est divisible par* $a + b$, ce qui revient à dire que *selon que* k *est pair ou impair,* $a^k \mp b^k$ *est divisible par* $a + b$.

2° Pour $a = \frac{n}{1}$, $b = \frac{n}{2}$, $c = \frac{n}{3}$, ... (13) donne la sommation de certaines expressions très importantes appelées *nombres figurés, nombres combinatoires* ou *coefficients binomiaux,* et qu'on représente par la notation

$$C_{n,a} = \frac{n(n-1)(n-2)\ldots(n-a+1)}{a!}.$$

L'identité ainsi obtenue

$$\left\{ \begin{array}{l} C_{n+k,k} = \dfrac{(n+1)(n+2)\ldots(n+k)}{k!} \\ = 1 + C_{n,1} + C_{n+1,2} + \ldots + C_{n+k+1,k}, \end{array} \right. \tag{15}$$

mise implicitement pour la première fois sous cette forme par Briggs, a été démontrée par Pascal, à l'aide de sa méthode *de proche en proche*[1]. Elle peut servir à faire voir que *le produit* $(n + 1) \ldots (n + k)$ *est divisible par le produit* k ! Mais on démontre plus aisément cette proposition, due également à Pascal, en changeant successivement n en $n - 1$, $n - 2$, ... dans la relation suivante, aisée à établir

$$C_{n,k} = C_{n-1,k} + C_{n-1,k-1}, \tag{16}$$

[1] Cette méthode, fréquemment employée, et dont on trouvera plus loin plusieurs exemples, consiste à s'assurer qu'une propriété supposée vraie pour le cas d'une expression $F(n)$, l'est encore pour $F(n + 1)$, d'où on conclut sa généralité, si elle se vérifie pour $F(1)$; car elle l'est par suite pour $F(2)$; l'étant pour $F(2)$, elle l'est pour $F(3)$; et ainsi de suite à l'infini.

ce qui conduit, de proche en proche, à des identités évidentes de la forme $C_{h,h} = 1$.

L'expression $C_{n,k}$ jouit d'ailleurs d'un grand nombre d'intéressantes propriétés, qui sont plutôt du domaine de l'analyse algébrique. Il suffira de faire remarquer, en premier lieu, qu'elle n'a de signification arithmétique que si n et k sont des entiers positifs, avec $n > k$, mais que cependant on admet par définition qu'on a :

$$C_{0,k} = 1 , \qquad C_{k,k} = 1 . \tag{17}$$

En second lieu, que *si* p *désigne un nombre premier* $>$ k, $C_{p,k}$ *est divisible par* p (Euler), ou bien qu'on a :

$$C_{p,k} \equiv 0 \pmod{p} \tag{18}$$

car on peut écrire

$$kC_{p,k} = pC_{p-1,k-1} ,$$

et p étant premier avec k, il divise $C_{p,k}$.

9. *Utilisation des irrationnelles.* Un grand nombre de formules se généralisent aisément par une substitution d'irrationnelles à des indéterminées rationnelles. Ainsi changeant dans (10) b en $b\sqrt{k}$, cette formule devient (voir exercice n° 7)

$$(a^2 + kb^2)^2 = (a^2 - kb^2)^2 + k(2ab)^2 . \tag{19}$$

Mais on arrive de la manière suivante à des résultats beaucoup plus intéressants.

Euler, le premier, a remarqué que *deux expressions telles que* $a + b\sqrt{k}$ (où k est positif ou négatif) *ne peuvent être égales que si les parties rationnelles le sont elles-mêmes, ainsi que les coefficients des parties irrationnelles.* Il en déduit, à l'aide de la formule du binome [1], cet important théo-

---

[1] On y arrive plus simplement ainsi : Soit $(a + \sqrt{b})^2 = A + B\sqrt{b}$, d'où $A = a^2 + b$, $B = 2a$; il viendra $(a - \sqrt{b})^2 = A - B\sqrt{b}$. Or si on a :

$$(a \pm \sqrt{b})^k = \alpha \pm \beta\sqrt{b} ,$$

on aura aussi :

$$(a \pm \sqrt{b})^{k+1} = (\alpha \pm \beta\sqrt{b})(a + \sqrt{b}) = (a\alpha + b\beta) \pm (\alpha b + a\beta)\sqrt{b} .$$

La proposition est donc vraie en général.

Autrement. Soient les relations

$$(a + \sqrt{b})^k = A + B\sqrt{b} , \qquad (a - \sqrt{b})^k = A' + B'\sqrt{b} .$$

rème : *la relation* $F(a+\sqrt{b}) = A + B\sqrt{b}$ *entraîne cette autre* $F(a-\sqrt{b}) = A - B\sqrt{b}$, F désignant une fonction entière.

Cor. I. Posons $(a + b\sqrt{k})(x + y\sqrt{k}) = A + B\sqrt{k}$; on en tirera

$$ax + kby = A\ , \qquad ay + bx = B\ , \qquad \text{d'où } x \text{ et } y.$$

II. *Trouver un cube qui soit en même temps de la forme* $u^2 + kv^2$. (Voir exercice **51**.)

III. Si $(a + b\sqrt{k})^n = A + B\sqrt{k}$, on aura aussi $(a - b\sqrt{k})^n = A - B\sqrt{k}$, d'où, en multipliant,

$$(a^2 - kb^2)^n = A^2 - kB^2\ .$$

Donc, si F désigne une fonction entière, les égalités

$$F(a + b\sqrt{k}) = \alpha + \beta\sqrt{k} \qquad \text{et} \qquad F(a^2 + kb^2) = \alpha^2 + k\beta^2$$

sont équivalentes. (Voir exercice n° **41**.)

IV. Soit

$$(\alpha) \qquad (a + b\sqrt{k})(\alpha + \beta\sqrt{k}) = A + B\sqrt{k}$$

on aura aussi

$$(a - b\sqrt{k})(\alpha - \beta\sqrt{k}) = A - B\sqrt{k}\ ,$$

d'où, en multipliant,

$$(20) \qquad (a^2 - kb^2)(\alpha^2 - k\beta^2) = A^2 - kB^2\ .$$

Donc *le produit des expressions de la forme* $x^2 + ky^2$ *est isomorphe* (Goldbach). Tenant compte de (α), (20) donne cette importante identité, due à Euler (voir exercice n° **46**)

$$(21) \qquad (a^2 + kb^2)(\alpha^2 + k\beta^2) = (a\alpha - kb\beta)^2 + k(a\beta + b\alpha)^2\ .$$

C'est une généralisation de (8), laquelle la comprend en même temps, comme cas particulier, en y changeant c en

---

L'expression $(a+\sqrt{b})^k - (a-\sqrt{b})^k$ est algébriquement divisible par $(a+\sqrt{b}) - (a-\sqrt{b}) = 2\sqrt{b}$, c'est-à-dire qu'elle contient $\sqrt{b}$ dans tous ses termes, ce qui demande qu'on ait $A - A' = 0$. D'ailleurs le produit

$$(A + B\sqrt{b})(A' + B'\sqrt{b}) = (a^2 - b)^k$$

est rationnel, ce qui conduit à écrire

$$(AB' + BA')\sqrt{b} = 0\ , \qquad \text{d'où} \qquad B' = -B\ .$$

$b\sqrt{k}$, b en α et d en $\beta\sqrt{k}$. Comme le premier membre ne varie pas en y changeant b en $-b$, il en est de même du second membre, et on a par suite :

$$(22)\quad (a\alpha - kb\beta)^2 + k(a\beta + b\alpha)^2 = (a\alpha + kb\beta)^2 + k(a\beta - b\alpha)^2 .$$

10. *Emploi des imaginaires.* La considération des imaginaires conduit à des résultats analogues. Une transformation très usitée consiste à remplacer $a^2 + b^2$ par le produit $(a + bi)(a - bi)$ et combiner plusieurs expressions de ce genre. Ainsi on a :

$$\begin{aligned}(a^2 + b^2)^2 &= (a + bi)^2(a - bi)^2 = (a^2 + 2abi - b^2)(a^2 - 2abi - b^2)\\ &= (a^2 - b^2)^2 - (2abi)^2\end{aligned}$$

d'où l'identité (10) (Euler).

Celle de Fibonacci (8) s'obtient de même, en remarquant que le premier membre peut s'écrire

$$\begin{aligned}&(a + bi)(c \pm di)(a - bi)(c \mp di)\\ &= (ac \mp bd \pm adi + cbi)(ac \mp bd - cbi \mp adi)\\ &= (ac \mp bd)^2 - (ab \mp cd)^2 i^2 .\end{aligned}$$ (Euler)

Enfin, si, avec Mathews Collins, on a fait dans (7)

$$\begin{aligned}&a = \alpha + \beta i , \quad a' = \gamma + \delta i , \quad c = -\gamma + \delta i , \quad c' = \alpha - \beta i ,\\ &b = \alpha' + \beta' i , \quad b' = \gamma' + \delta' i , \quad d = -\gamma' + \delta' i , \quad d' = \alpha' - \beta' i ,\end{aligned}$$

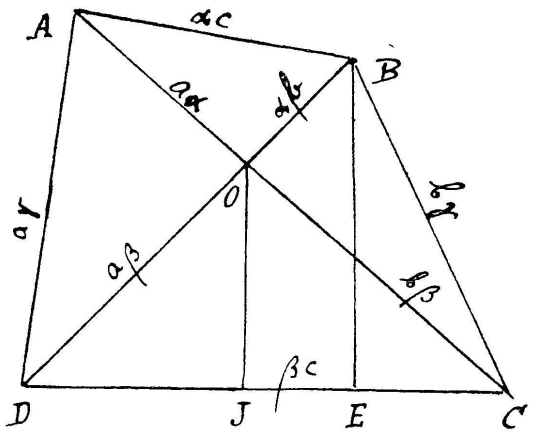
on trouve cette identité d'Euler

$$(23)\quad \left\{\begin{aligned}&(\alpha^2 + \beta^2 + \gamma^2 + \delta^2)(\alpha'^2 + \beta'^2 + \gamma'^2 + \delta'^2) = (\alpha\alpha' + \beta\beta' + \gamma\gamma' + \delta\delta')^2\\ &+ (\alpha\beta' - \beta\alpha' - \gamma\delta' + \delta\gamma')^2 + (\alpha\gamma' + \beta\delta' - \gamma\delta' - \delta\beta')^2\\ &\qquad + (\alpha\delta' - \beta\gamma' + \gamma\beta' - \delta\alpha')^2\end{aligned}\right.$$

qui montre que *le produit de deux sommes de quatre carrés est isomorphe.* (Voir exercice n° **15**.)

11. *Figurations arithmétiques.* La méthode arithmo-graphique a, — comme la méthode arithmo-algébrique, — cet inconvénient d'être indirecte et de se prêter encore moins que celle-ci, à la représentation des conditions arithmétiques. De plus elle utilise des figures dont on ne sait pas toujours lire les propriétés et dont il est souvent difficile

d'affirmer la généralité ou les limites d'emploi. Mais elle a cet avantage de représenter synoptiquement un ensemble de propriétés qui la rend quelquefois aussi suggestive dans les recherches que commode dans les exposés et dans les démonstrations. On comprend que les premiers arithméticiens l'aient employée dans ce but, préférablement à l'algèbre.



On traitera seulement ici du *quadrilatère de Brahmagupta :* on appelle ainsi celui qui est à la fois inscriptible et *orthodiagonal.* (Voir exercices n^{os} **1**, **2** et **3**.)

1° Soit O l'intersection des diagonales AC, BD d'un tel quadrilatère. Les côtés seront entiers si l'on prend :

$$\text{AO} = a\alpha\ , \qquad \text{BO} = \alpha b\ , \qquad \text{CO} = b\beta\ , \qquad \text{DO} = a\beta\ ,$$

a, b et α, β désignant les cathètes de deux triangles rectangles[1] dont les hypoténuses sont c et γ. On aura en effet

$$\text{AB} = \alpha c\ , \qquad \text{BC} = b\gamma\ , \qquad \text{DC} = \beta c\ , \qquad \text{AD} = a\gamma\ .$$

De plus, on aura, en abaissant les perpendiculaires OJ, BE sur DC,

$$\text{OJ} = \frac{\text{DO}\,.\,\text{OC}}{\text{DC}} = \frac{ab\beta}{c}\ , \quad \text{d'où} \quad \text{CE} = \frac{b}{c}(b\beta - a\alpha)\ , \quad \text{BE} = \frac{b}{c}(a\beta + b\alpha)\ .$$

2° La relation évidente $\text{OB}^2 + \text{OC}^2 = \text{BE}^2 + \text{CE}^2$ conduit immédiatement à l'identité de Fibonacci qui, très probablement, y est arrivé ainsi, si toutefois elle n'est pas de Brahmagupta lui-même.

3° Supposons que γ soit, non plus un entier, mais une irrationnelle $\sqrt{\text{C}}$; on tirera ainsi de ce qui précède, une nouvelle solution de l'équation $x^2 + y^2 = \text{C}$, connaissant

[1] Brahmagupta opère sur le quadrilatère correspondant aux données $a = 3$, $b = 4$, $\alpha = 5$, $\beta = 12$, ou bien

$\text{OA} = 15$, $\text{OB} = 20$, $\text{OC} = 48$, $\text{OD} = 36$, $\text{AB} = 25$, $\text{BC} = 52$, $\text{CD} = 30$, $\text{AD} = 39$.

une première solution $\alpha^2 + \beta^2 = C$: construire le triangle $OB = \alpha$, $OC = \beta$, $BC = \gamma$; prolonger OB, de $OD = \frac{a\beta}{b}$, a et b désignant les cathètes d'un triangle d'hypoténuse c ; on n'aura plus qu'à joindre DC et abaisser la perpendiculaire BE, ce qui donnera [1]

$$x = EC = \frac{b\beta - a\alpha}{C}, \qquad y = BE = \frac{a\beta + b\alpha}{C}.$$

4° Supposons $a^2 - kb^2 = 1$, $\alpha^2 - k\beta^2 = C$; on aura, avec Brahmagupta,

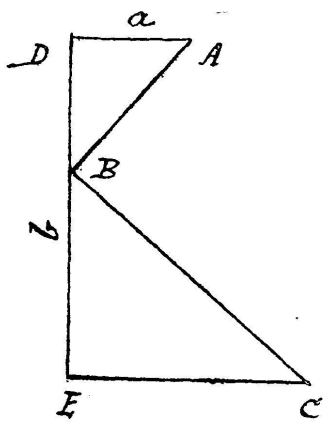
$$(kb\beta - a\alpha)^2 - k(a\beta + \alpha b)^2 = C.$$

Changeons en effet dans 3°, a, b, β et y en aC, $bC\sqrt{-k}$, $\beta\sqrt{-k}$ et $y\sqrt{-k}$; il viendra :

$$x = kb\beta - a\alpha, \qquad y = a\beta + b\alpha,$$

ce qui donne une autre solution de $x^2 - ky^2 = C$.

5° Voici une manière d'arriver plus aisément à l'identité de Fibonacci que par 2°. Soit l'angle droit ABC ; menons, par le sommet, la droite quelconque DE, sur laquelle on abaissera les perpendiculaires AD, CE. On a, $\frac{f}{g}$ désignant le rapport de AD à DB,



$$(AD^2 + DB^2) + (BE^2 + EC^2)$$
$$= BD + BE)^2 + (EC - AD)^2$$

ou bien

$$a^2 + \left(\frac{fa}{g}\right)^2 + b^2 + \left(\frac{fb}{g}\right)^2 = \left(b + \frac{fa}{g}\right)^2 + \left(\frac{fb}{g} - a\right)^2.$$

12. *Descente.* On appelle ainsi, d'après Fermat, une méthode de démonstration de l'impossibilité de certaines propositions, consistant à faire voir que ces propositions supposées vraies pour des nombres donnés, demandent, par cela même, qu'elles le soient pour des nombres plus petits ; ce qui fait que de ceux-ci on tirerait d'autres nombres encore

[1] Voir Chasles, *Ap. Hist.*, p. 441 et J. L. (1837), p. 37.

plus petits et jouissant des mêmes propriétés; et ainsi de suite, ce qui implique contradiction avec le nombre limité des entiers inférieurs à ceux donnés d'abord.

Exemple. *L'aire d'un triangle ne saurait être un carré* (Fermat). Démonstration rétablie par Euler. Les trois côtés étant f^2+g^2, $2fg$ et f^2-g^2, l'aire A est $fg(f^2-g^2)$; f et g sont premiers entre eux avec f^2-g^2. Pour que A soit un carré, il faut que f, g et f^2-g^2 soient également des carrés; posons en conséquence $f=\lambda^2$, $g=\mu^2$; $f^2-g^2=\lambda^4-\mu^4$ doit être un carré. Or λ et μ sont premiers entre eux, de même que $\lambda^2+\mu^2$ et $\lambda^2-\mu^2$; ces deux derniers sont donc des carrés. Ecrivons donc

$$\lambda^2+\mu^2=r^2\ ,\quad \lambda^2-\mu^2=s^2\ ,\quad \text{d'où}\quad \mu^2+s^2=\lambda^2\ ,\quad s^2+2\mu^2=r^2\ .$$

La dernière égalité donne, à cause de (19)

$$s=t^2-2u^2\ ,\quad \mu=2tu\ ,\quad r=t^2+2u^2\ ,\quad \text{d'où}\quad \lambda^2=\mu^2+s^2=t^4+4u^4\ ,$$

c'est-à-dire un triangle t^2, $2u^2$, λ dont l'aire $A'=t^2u^2$ serait également un carré et qui serait beaucoup plus petit que le premier, car on a :

$$A=\lambda^2\mu^2(\lambda^4-\mu^4)=4t^2u^2(t^4+4u^4)(t^2+2u^2)^2(t^2-2u^2)^2>A'\ .$$

On aurait ainsi la possibilité de trouver une suite indéfinie de triangles dans ce cas, ce qui est impossible puisqu'il s'agit de nombres entiers, qui ne peuvent indéfiniment décroître. (Voir *Ens. Math.*, 1909, p. 331, pour un autre exemple.)

Exercices.

1. *Trouver graphiquement les développements de* $(a+b)(c+d)$, *de* $(a\pm b)^2$, *de* $(a+b)(a-b)$, *de* $\left(\frac{a+b}{2}\right)^2-\left(\frac{a-b}{2}\right)^2$ [1] (Euclide), *ainsi que la sommation d'une progression arithmétique* (Archimède).

2. *La somme des* n *premiers impairs successifs est un carré.*

[1] C'est de cette dernière figuration qu'on a tiré l'idée de remplacer les multiplications par des soustractions, à l'aide de tables de quarts de carrés.

Il en est de même de deux triangulaires successifs[1]. *Tout carré impair est la différence de deux triangulaires, et en même temps, l'octuple d'un triangulaire augmenté de l'unité* (Pythagoriciens). Se démontrent par des configurations géométriques de points.

3. *Démontrer géométriquement que si* (a, b) *est une solution de* $x^2 - 2y^2 = n$, $(2b + a, a + b)$ *en est une de* $x^2 - 2y^2 = -n$. Construisons le triangle rectangle isoscèle ABC; abaissons sur l'hypoténuse AC, la hauteur BD et d'un point E de BC, la perpendiculaire EF. On aura :

$$AF^2 + EF^2 = AB^2 + BE^2 \quad \text{ou} \quad (2b + a)^2 + a^2 = 2(a + b)^2 + 2b^2 ,$$

en posant $DF = b$, $FC = a$. Cette proposition semble due aux Platoniciens, qui s'en servaient pour trouver des approximations de plus en plus serrées de l'irrationnelle $\sqrt{2}$, en partant des solutions $a = 3$, $b = 2$, de l'équation $x^2 - 2y^2 = 1$.

4. *Résoudre les équations*

$$1^\circ\ Ax = By ; \quad 2^\circ\ xy = Az ; \quad 3^\circ\ xy = uv ; \quad 4^\circ\ x^2 = yz ;$$
$$5^\circ\ x^2 = ay ; \quad 6^\circ\ xyz = tuv ; \quad 7^\circ\ x^3 = tuv ; \quad 8^\circ\ x^2y = u^2v .$$

1° Si A et B sont premiers entre eux, on pose $x = B\alpha$, $y = A\alpha$, α entier quelconque.

Si A et B ont h comme p. g. c. d., on écrit : $hx = B\alpha$, $hy = A\alpha$.

2° Soit $A = ab$; on écrira $z = \gamma\delta$, $x = a\gamma$, $y = b\gamma$; γ et δ quelconques. Il y a autant de solutions que de manières de décomposer A en deux facteurs.

3° On fera $x = \alpha\beta$, $y = \gamma\delta$, $u = \alpha\gamma$, $v = \beta\delta$; α, β, γ, δ, quelconques.

4° On fera $x = \alpha\beta\gamma$, $y = \alpha^2\beta$, $z = \beta\gamma^2$.

5° Soit $a = b^2c$; on fera $x = bc\alpha$, $y = c\alpha^2$.

6° On écrira : $x = \alpha\beta$, $y = \gamma\delta$, $z = \varepsilon\varphi$, $t = \alpha\gamma$, $u = \beta\varepsilon$, $v = \delta\varphi$.

7° On écrira : $x = \alpha\beta\gamma$, $t = \alpha^2\beta$, $u = \beta^2\gamma$, $v = \gamma^2\alpha$.

---

[1] On appelle *triangulaire* un nombre de la forme $\frac{x(x+1)}{2}$.

8° On écrira : $x = \alpha\beta$, $y = \gamma^2\delta^2$, $u = \alpha\gamma$, $v = \beta^2\delta^2$ [1].

5. *Résoudre* $xy + Ax + By = C$. On a :

$$y = \frac{AB + C}{x + B} - A .$$

Soit $AB + C = ab$; on posera : $x = a - B$ ou $b - B$, d'où deux solutions pour chaque décomposition de $AB + C$ en deux facteurs (Euler).

6. *Résoudre* $x^2 + y^2 = z^2$. Posons $z = y + z'$, ce qui nous fera éliminer un carré [2]. Il viendra $x^2 = z'(2y + z')$, ce qui conduit à poser :

$$x = tuv , \quad z' = t^2u , \quad 2y + z' = uv^2 , \quad \text{d'où} \quad 2y = u(v^2 - t^2) , \quad 2z = u(v^2 + t^2) .$$

On retrouve la formule (10) présentée un peu plus généralement, telle qu'Euclide l'a donnée.

7. *Résoudre* $x^2 - y^2 = az^2$. Soit $a = fg$; on peut écrire :

$$x + y = f\lambda^2 , \quad x - y = g\mu^2 \quad \text{d'où} \quad 2x = f\lambda^2 + g\mu^2 , \quad 2y = f\lambda^2 - g\mu^2 , \quad z = \lambda\mu .$$

Il y a autant de solutions que de manières de décomposer a en deux facteurs (Lagrange).

8. *Tout cube est égal à la différence de deux triangulaires successifs* (Ibn Almadjdi).

9. *Tout nombre de la forme* $x^2 \pm x + 1$ *est la somme de deux triangulaires* (de Roquigny). En général, *tout nombre* $x^2 \pm xy + y^2$ *est en même temps de la forme* $z^2 + 3w^2$ (Euler). Voir *Ens. Math.*, 1907, p. 441.

10. *Aucun nombre* $2(x^2 + y^2 + xy)$ *ne peut être un carré* (Fermat), *ni aucun des suivants* $2x^2 + 3y^2$, $2w^2 + y^2$, $3x^2 + 7y^2$, $5x^2 + 7y^2$, $6x^2 + 7y^2$, *ni le nombre* $2x^4 + 2$ (Euler).

Si a *et* b *ne sont pas tous les deux divisibles par* 3, *ou* 7, *ou* 11, *ou* 19, *ou* 23, ... *il en est de même de* $a^2 + b^2$.

---

[1] On multiplierait aisément ces exercices, et d'autres de genre analogue. En voici, par exemple, un dû à Cauchy : *les nombres* a, b, c *étant premiers entre eux, la solution générale de* $ax + by = cz$ *est donnée par les formules*

$$x = b\alpha - c\beta , \qquad y = c\gamma - a\alpha , \qquad z = b\gamma - a\beta .$$

[2] Ce procédé d'élimination d'un carré de l'énoncé est dû à Diophante, qui pour résoudre $x^2 + ax + b = y^2$, égale le premier membre à $(x + z)^2$, ce qui lui donne $x = \frac{z^2 - b}{a - 2z}$, d'où une infinité de valeurs fractionnaires de x, en faisant $z = 1, 2, 3, \ldots$

11. *Tout nombre* $2a^2 - b^2$ *est en même temps de la forme* $x^2 - 2y^2$. *Tout nombre* $5a^2 - b^2$ *est en même temps de la forme* $x^2 - 5y^2$ (Lagrange). En général, *on a cette identité de Mathews Collins*

$$(g^2 a)^2 - (f^2 + g^2) b^2 = (f^2 + g^2)(ga \pm fb)^2 - [(f^2 + g^2) b \pm fga]^2 .$$

12. *Le double d'un nombre de la forme* $x^2 + y^2 + xy$ *est une somme de trois carrés, et le double de son carré, la somme de trois bicarrés* (Catalan). *Il en est de même du nombre* $x^2 + y^2 + z^2 - xy - yz - zx$ (Ed. Lucas).

13. $a^{2n+1} \pm 1$ *n'est jamais divisible par* $a^2 - 1$. En effet, le quotient de $a^{2n} \pm 1$ par $a \pm 1$ peut s'écrire

$$a(a \mp 1)(a^{2n-2} + a^{2n-4} + \ldots + 1) + 1 .$$

14. *Posons* $F = ax^2 + 2bxy + y^2$, $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$; *on trouvera, en substituant, une nouvelle forme* $F' = a'x'^2 + 2b'x'y' + c'y'^2$ *telle que* $b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2$. *Tout nombre représentable par la forme* F *l'est par la forme* F', *et la réciproque a lieu également si* $\alpha\delta - \beta\gamma = \pm 1$ (Lagrange).

15. 1° Faisant dans (23) $d = \delta = 0$, on arrive à cette conclusion que *le produit de deux sommes de trois carrés est une somme de quatre carrés*[1] (Euler).

2° Chercher l'expression du produit de la somme de quatre carrés par $3 = 1^2 + 1^2 + 1^2 + 0$, par $4 = 1^2 + 1^2 + 1^2 + 1^2$, par $4 = (-1)^2 + 1^2 + 1^2 + 1^2$, par $5 = 4 + 1 + 0 + 0$, par $6 = 4 + 1 + 1 + 0$, par $7 = 4 + 1 + 1 + 1$, par $10 = 4 + 4 + 1 + 1$, etc.; on obtiendra ainsi diverses formules, dont les trois premières sont dues à Euler, Cauchy et Jacobi.

3° *On trouvera une généralisation de* (23), due à Lagrange, *en y changeant* $\beta, \gamma, \delta, \beta' \gamma' \delta'$ en $\beta\sqrt{k}$, $\gamma\sqrt{l}$, $\delta\sqrt{kl}$, $\beta'\sqrt{k}$, $\gamma'\sqrt{l}$, $\delta'\sqrt{kl}$.

16. *Soit* A *le produit de nombres impairs* a, a', a'', ... *les deux nombres*

$$\frac{A - 1}{2} \quad \text{et} \quad \frac{a - 1}{2} + \frac{a' - 1}{2} + \ldots$$

[1] Cauchy a fait voir que ce théorème résulte de la considération d'un triangle projeté sur trois plans rectangulaires.

sont respectivement de même parité que les suivants

$$\frac{A^2-1}{8} \quad \text{et} \quad \frac{a^2-1}{8}+\frac{a'^2-1}{8}+\ldots \qquad \text{(Gauss)}$$

17. *Toute sixième puissance est de l'une ces formes* $7+0, 1$; *toute dixième puissance, de l'une des formes* $11+0, 1$; *toute douzième, de l'une des formes* $13+0, 1$; *toute seizième, de l'une des formes* $17+0, 1$; *etc.* Par exemple, on a, pour les carrés, les formes $7+0, 1, 4, 2$; d'où, pour celles des bicarrés, $7+0, 1, 2, 4$; et pour les sixièmes puissances, $7+0, 1, 1, 1$.

18. Divers problèmes de Goldbach et d'Euler. Voir *Ens. Math.*, 1909, pp. 354 et 355.

19. *Le quadruple d'un triangulaire ne peut être un triangulaire* (de Rocquigny). On devrait avoir $x^2+x=4y^2+4y^2$, égalité qui revient à l'une quelconque des suivantes :

$$x^2+x+1=(2y+1)^2\ , \qquad 2x+1=\pm\sqrt{4(2y+1)^2-3}\ ,$$

$$(4y+2x-3)(4y-2x+1)=3\ , \qquad (x+2y+2)(x-2y)=x\ ,$$

dont l'impossibilité est aisée à démontrer, car le premier membre de la première ne peut être un carré; 3 ne peut être la différence d'autres carrés que 4 et 1; enfin les deux dernières ne peuvent avoir lieu que pour $x=y=0$. (*I. M.*, 1894, pp. 303 et 394.)

20. *Si* a *est premier avec* b, *les congruences* $n=h$ *(mod* a*)* *et* $n=h$ *(mod* b*) entraînent la suivante* $n=h$ *(mod* ab*)*. En effet le nombre $n-h$ étant divisible par a et b, l'est par ab. Cette question s'étend à un nombre quelconque d'entiers premiers entre eux : c'est un cas particulier de la suivante, qui remonte à l'antiquité : *trouver un nombre qui, divisé par* a, b, c, ... *donne les restes* $\alpha, \beta, \gamma, \ldots$

21. *Tout nombre impair est* $8+1$ *si ses facteurs de forme* $8+3, 5, 7$ *sont tous en nombre pair ou tous en nombre impair.* Zéro est compté pour un nombre pair.

22. a *et* b *étant premiers entre eux, si* $ax-by=1$, *les nombres*

$$x=\alpha c+\lambda b\ , \qquad y=\beta c+\lambda a$$

satisfont à l'équation $ax-by=c$.

23. *Des solutions des équations*

$$ax - by = c\ , \qquad ax' - b'y' = c\ , \qquad ax'' - b''y'' = c\ , \ \ldots$$

déduire celles de ax — bb'b''... y = c (Gauss).

24. Soit l'équation $a^2x^2 + bx + c = y^2$. Posons $y = ax + \frac{z}{u}$, on en tirera une expression de x, en z et u qui donnera les valeurs positives de x en donnant à z et u des valeurs telles que $\frac{b}{2a} \gtrless \frac{z}{u} \gtrless \sqrt{c}$.

2° Soit $ax^2 + bx + c^2 = y^2$. On posera $y = c + \frac{z}{u}x$, ce qui donnera pour x une formule analogue. On s'occupera seulement des valeurs de $\frac{z}{u}$ comprises entre $\sqrt{a}$ et $\frac{b}{2c}$.

3° Le cas général $ax^2 + bx + c = y^2$ est bien moins aisé à résoudre ; aussi il faut tout d'abord tâcher de voir s'il n'y a pas impossibilité, comme c'est le cas pour $13x^2 + 54x + 69 = y^2$, puisque le premier nombre peut s'écrire $7(x+3)^2 + 6(x+1)^2$.

4° On sait que si $b^2 - 4ac$ est un carré, le trinome $ax^2 + bx + c$ peut se décomposer en deux facteurs linéaires. On peut donc le supposer égal à $(ax + f)(x + g)$ ou à $\frac{u^2}{v^2}(x+g)^2$, d'où on tire x, qui sera entier si on fait $v^2a - u^2 = \pm 1$ (Euler).

Si $ax^2 + bx + c$ peut se mettre sous la forme $(fx+g)^2 + (hx+j)(kx+l)$, on égalera sa racine carrée à $(fx+g) + \frac{u}{v}(hx+j)$, ce qui donnera une valeur de x en u et v dont on essaiera d'égaler le dénominateur à ± 1 (Euler).

6° Résolvons algébriquement $ax^2 + bx + c = y^2$ par rapport à x ; on est ramené, en posant $X = 2y$, $b^2 - 4ac = B$, à résoudre $aX^2 + B = Y^2$, ce qu'on fait en donnant des valeurs convenables à Y. Inutile d'ailleurs de prendre $Y > \frac{a}{2}$, puisque $(Y \pm ka)^2 - B$ est divisible par a, en même temps que $Y^2 - B$. Si jusqu'à $Y = \frac{a}{2}$ on ne trouve aucune solution, l'équation est insoluble (Lagrange).

25. *Soit* $ax^2 + 2bcx + c^2 = y^2$ *et supposons* $x > b$ *et* $> c$; *la valeur de* y *est de la forme* $zx^2 - bx + c$.

26. *Déterminer les valeurs de* x *supérieures à* b *et à* c *données par l'équation* $a^2x^2 + bx + c = y^2$. On a :

$$\frac{b+1}{2a} > y - ax > \frac{b}{2a+1}.$$

y est de la forme $ax + d$ avec $d < x$, car $x > b > \frac{b+1}{2a} > d$. En écrivant $a^2x^2 + bx + c = (ax + d)^2$, il vient $(b - 2ad)x + c - d^2 = 0$. On essaie, dans cette expression, les valeurs de $d = y - ax$ comprises entre les limites données plus haut (*S. Œ.*, 1910, p. 146).

27. *On peut toujours former une puissance entière quelconque par l'addition de termes d'une progression arithmétique* (Rallier des Ourmes). Application à l'étude des suites formées :

1° par le premier entier 1 ; la somme, 2 + 3, des deux suivants ; celle, 4 + 5 + 6, des trois suivants ; etc.

2° par le premier entier 1 ; la somme, 2 + 3 + 4, des trois suivants ; celle des cinq suivants ; etc.

3° par le premier impair ; la somme des deux suivants ; etc.

4° par la somme des deux premiers impairs ; celle des quatre suivants ; etc.

5° par le premier impair ; la somme des quatre premiers ; celle des neuf premiers ; etc.

6° par le premier impair ; la somme des (1 + 4) suivants ; celle des (1 + 4 + 9) suivants ; etc.

7° par le premier impair ; la somme des (1 + 8) suivants ; celle des (1 + 8 + 27) suivants ; etc. (de Rocquigny).

28. *Combien de zéros dans les* n *premiers entiers ?* (Ed. Lucas).

29. *Le nombre* 1000 ! *se termine à droite par* 249 zéros (de Rocquigny).

30. *Quels sont les derniers chiffres à droite de* 2^{1000}, de 3^{1000} ? (id.)

31. *Il y a quinze nombres dans les* 1000^{1000} *premiers entiers qui sont à la fois carrés, cubes, bicarrés, ... dixièmes puissances* (de Laplanche) [1].

---

[1] On peut rappeler ici le *problème de Comiers*, jadis célèbre : *quel est le produit des deux nombres formés respectivement de* 666 *chiffres* 9 *et de* 666 *chiffres* 6 ?

32. *Dans quatre cents ans, combien de mois de février de cinq dimanches ?* (N. A.) *Combien de vendredis* 13 ? (Buray) *Il y a au plus trois de ces derniers et au moins un annuellement* (G. Tarry).

33. *La série de Fibonacci* 1, 2, 3, 5, 8, 13, 21, 34, ... $u_{n+1} = u_n + u_{n-1}$ *ne peut avoir que quatre ou cinq termes d'un nombre donné de chiffres* (Lamé). Cela vient de ce que si

$$u_k < 10u_{k-4} < u_{k+1} \qquad \text{et} \qquad u_{k+1} < 10u_{k-3} < u_{k+2} ,$$

il s'ensuit $u_{k+2} < 10u_{k-2} < u_{k+3}$.

34. *Disposer les douze premiers entiers sur trois lignes, qui donnent des sommes égales, et de telle manière que, dans chacune des quatre colonnes, le plus grand des trois nombres soit égal à la somme des deux autres.*

35. *Placer les neuf premiers nombres aux sommets et sur les côtés d'un triangle, de manière que la somme des nombres d'un côté quelconque soit constante, ainsi que celle de leurs carrés* (Proth). Appelons x, y, z les trois sommets ; les valeurs des deux expressions $x + y + z$ et $x^2 + y^2 + z^2$ sont toutes deux des multiples de 3, ce qui demande que x, y, et z soient ensemble **3** ou **3** + 1 ou **3** — 1. De là trois solutions, dont la seconde seule 2, 5, 8 est à conserver. Le reste s'achève facilement.

36. *Le carré d'un polynome de* 2^k *termes ayant autant de termes négatifs que de positifs contient* 2^{2k-2} *doubles produits négatifs et* $2^{k-1}(2^{2k-1} - 1)$ *doubles produits positifs* (Barbette).

Pour que le carré d'un polynome de n *termes présente autant de doubles produits positifs que de négatifs, il faut que* n *soit un carré, et alors il y a* $\frac{n + \sqrt{n}}{2}$ *termes positifs* (Id.)[1].

37. *Quel est le signe du* $n^{ième}$ *terme du développement du produit*

$$(1 - a)(1 - b)(1 - c) \ldots ? \qquad \text{(Catalan)}$$

Montrer l'identité de ce problème avec le suivant : *considérons les lettres* a, b, *que nous ferons suivre du groupe ren-*

[1] A rapprocher de la question suivante : *trouver le produit de deux expressions de la forme* $\sqrt{a} + \sqrt{b} + \ldots$ *qui ne diffèrent qu'en ce que, dans la deuxième, certains radicaux sont pris avec le signe* —. Voir Fitz-Patrick, *Exercices d'Arithmétique*, p. 575.

versé ba, *d'où le groupe* abba, *auquel nous accolerons le groupe inverse, ce qui nous donnera* abbabaab, *et ainsi de suite. Quelle est la* n^ième *lettre ?* (Laisant). Voir *A. F.*, 1881.

38. Soit a la base de numération ; $a^n - 1$ *est divisible par* $a - 1$; il s'ensuit que *tout nombre* $N = A^n + B^{n-1} + \ldots$ fournit la relation $N \equiv A + B + \ldots$ *(mod* $a - 1$*)* et que *l'un des nombres* $a^n \pm 1$ *est divisible par* $a + 1$ *selon que* n *est pair ou impair.* Donc si n est pair, on a : $N \equiv A - B + C - \ldots$ (mod $a + 1$) (Gauss).

39. *Soit* d *un diviseur de* $a10^b \pm c$. *Un nombre est divisible par* d *quand, ayant séparé* b *chiffres à la droite de ce nombre et divisé le nombre restant à gauche par* a, *la somme ou la différence entre* c *fois le quotient et le nombre formé en écrivant le nombre de droite à la droite du reste est divisible par* d (E. Gelin). Voir les *Caract. de div.* du même auteur, et les *Ex. d'Arith.* de Fitz-Patrick, pp. 24 et seq.

40. 1° L'expression $(a + 1)^n - a^n$ est la somme des n termes

$$(a + 1)^{n-1}, \quad (a + 1)^{n-2}a, \quad (a + 1)^{n-3}a^2, \ \ldots \ a^{n-1},$$

et par suite elle comprend visiblement n fois le terme a^{n-1}, plus des termes en a^{n-2}, en a^{n-3}, ... On peut donc écrire :

$$(\alpha) \qquad (a + 1)^n - a^n = na^{n-1} + Aa^{n-2} + \ldots + La + 1 \ [1].$$

2° Soit la suite de fonctions

$$\begin{aligned} F_1(x) &= F(x + 1) - F(x) \\ F_2(x) &= F_1(x + 1) - F_1(x) \\ F_3(x) &= F_2(x + 1) - F_2(x) \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

les fonctions F_1, F_2, F_3, ... sont appelées la *différence première,* la *différence seconde,* la *différence troisième,* ... de la fonction F. Posons maintenant

$$F(x) = Ax^n + Bx^{n-1} + Cx^{n-2} + \ldots + Lx + M ;$$

sa différence première $F(x + 1) - F(x) = F_1(x)$ contiendra

[1] Voir *Ens. Math.*, 1907, p. 297.

le terme nAx^{n-1}, plus des termes en x^{n-2}, ... On peut donc écrire $F_1(x) = nAx^{n-1} + B'x^{n-2} + \dots$ La différence seconde est donc de la forme

$$n(n-1)Ax^{n-2} + B''x^{n-3} + \dots$$

La différence troisième est de la forme $n(n-1)(n-2)Ax^{n-3} + B'''x^{n-4} + \dots$ On voit qu'on a :

$$F_n(x+1) + F_n(x) = n(n-1) \dots 2 . 1A .$$

Ainsi *la différence* n^ième *du polynome* $Ax^n + \dots$ *est égale à* An ! proposition connue des Anciens, mais laissée sans démonstration jusqu'à Mercator.

3° La fonction

$$F(x, k) = x - C^k(x-1)^n + C_{n,2}(x-2)^n - \dots$$

est du degré n, et par suite sa différence $n^{ième}$ a pour valeur n ! Or, à cause de (16), on trouve, pour l'expression de ses différences première, seconde, ... $n^{ième}$,

$$F(x+1, k) - F(x, k) = F(x+1, k+1) ,$$
$$F(x+2, k+1) - F(x+1, k+1) = F(x+3, k+2) ,$$
$$\dots\dots F(x+n, k+n) = n !$$

Faisant $x + n = a$, $k = 0$, il vient cette identité de Mercator

$$a^n C_{n,1}(a-1)^n + C_{n,2}(a-2)^n - \dots \pm 1 = n ! \qquad (a \geqq a) .$$

4° *Si* a *et* b *sont premiers entre eux, tout diviseur commun à* a — b *et à* $\frac{a^n - b^n}{a - b}$ *divise également* n (Lebesgue). Il suffit de changer dans (α) a en $\frac{b}{a-b}$.

Lebesgue démontre ce théorème à l'aide de la formule du binome. Malebranche, qui l'avait aussi rencontré (voir Ch. Henry, *Rech. sur les man. de Fermat*, p. 92), en donne une démonstration dont le principe pourrait être utilisé ailleurs : tout diviseur commun à $a - b$ et à $a^{n-1} + ba^{n-2} + b^2a^{n-3} + \dots$ divise $a^{n-2}(a-b) = a^{n-1} - ba^{n-2}$, et par suite $-2ba^{n-2} - b^2a^{n-3} - \dots$; or il divise $2ba^{n-3}(a-b)$

$= 2ba^{n-2} - 2b^2a^{n-3}$, il s'ensuit qu'il divise aussi $-3b^2a^{n-3} - b^3a^{n-4} - \ldots$; on voit qu'on arrivera à prouver qu'il divise nb^n.

41. *Les nombres* A_k *et* B_k *de la formule* $(a + \sqrt{b} = A_k + B_k\sqrt{b}$ *se calculent, de proche en proche, d'après les formules suivantes d'Euler*

$$A_{n+1} = aA_n + bB_n \ , \qquad B_{n+1} = A_n + aB_n \ ;$$

$$A_{n+1} = 2aA_n - (a^2 - b)A_{n-1} \ , \qquad B_{n+1} = 2aB_n - (a^2 - b)B_{n-1} \ .$$

42. *Les nombres* $y^2 - 3z^2$ *et* $3y^2 - z^2$ *ne peuvent être premiers qu'autant qu'ils sont respectivement des formes* $12 + 1$, et $12 - 1$.

Si le nombre $y^2 - 5z^2$ *est premier, il ne peut être que de l'une des quatre formes* 20 ± 1, ± 9.

43. *Tout nombre* $a^2 + 1$ *en divise une infinité d'autres isomorphes. En effet*

$$(a^2 + 1)[(ax + 1)^2 + x^2] = (a^2x + x + a)^2 + 1 \ .$$

Plus généralement, *le nombre* $n = ka^2 + lb^2$ *divise une infinité de nombres de la forme* $x^2 + kly^2$, *qui sont en même temps de la forme* $kx^2 + ly^2$ (Euler). En effet, on a :

$$n(1 + kl) = (ka \pm lb)^2 + kl(a \mp b)^2 = k(a \pm lb)^2 + l(b \mp ka)^2 \ .$$

44. *Tout diviseur commun aux nombres* $a^2 - kb^2$, $c^2 - ld^2$, ... *divise également un nombre de la forme* $x^2 - kl \ldots y^2$. En effet, il divise

$$a^2(c^2 - ld^2) + ld^2(a^2 - kb^2) = (ac)^2 - kl(bd)^2 \ . \qquad \text{(Lagrange)}$$

45. Posons $X = xx' - Qyy'$, $Y = xy' + yx' + Pyy'$, il viendra, si a et b sont les racines de l'équation $z^2 - Pz + Q = 0$,

$$(x + ay)(x' + ay') = X + aY \ .$$

Or on a : $(x + ay)(x + by) = x^2 + Pxy + Qy^2$; donc *le produit de deux nombres de la forme* $x^2 + Pxy + Qy^2$ *est isomorphe* (Lagrange).

46. Dans (21) changeons k en $\frac{k}{l}$, puis dans (8), a, c, b, d, respectivement en $a\sqrt{k}$, $b\sqrt{l}$, α, $\beta\sqrt{kl}$; il viendra deux

nouvelles formules, dues à Euler, lesquelles, avec (8), montrent que *le produit d'entiers des deux formes* $ax^2 + by^2$ *et* $x^2 + aby^2$ *est de la première ou de la seconde forme, selon que le nombre de ceux de la seconde est pair ou impair* (Euler).

47. 1° Faisant dans (9) $\alpha = a^2 + b^2$, $\beta = c^2$, on obtiendra une formule d'Euler permettant de décomposer le carré d'une somme de trois carrés en une somme de trois carrés.

2° Faisant $\alpha = a^2 + 1$, $\beta = a$, on trouvera une identité dont Euler s'est servi pour l'étude du produit $(1 + a + a^2)(1 + a^2 + a^4)(1 + a^4 + a^8) \ldots$

3° Faisant $\alpha = x^2 + Q$, $\beta = \sqrt{2(Q - P)}x$, on aura une extension de (11), qui en donne une de l'identité d'Aurifeuille, en posant $Q - P = a$, $x = (2a)^{\frac{2n+1}{2}}$. On peut trouver d'autres cas intéressants, par exemple en faisant $Q = 1$, $P = -\frac{1}{2}$, $x = 3^{\frac{2n+1}{2}}$; ces extensions sont dues à Catalan.

4° Faisant $\alpha = a^2 + b^2 + c^2 + d^2$ et $\beta = a^2 + b^2 + c^2 + d^2$, on aura un moyen, dû à Ed. Lucas, de décomposer le carré d'une somme de quatre carrés en une somme de quatre carrés.

5° Faisant $\alpha = Ax^3 + Cx$ et $\beta = Bx^2 + D$, il vient, en identifiant à $x^6 - 1$,

$$A = D = 1 , \quad 2C - B^2 = 0 , \quad C^2 - 2B = 0 , \quad B = C = 2 ,$$

d'où une remarquable identité, due à A. Boutin.

6° Faisant, de deux manières différentes, le produit de $2(a + b)(c - d)$ par $2(a - b)(c + d)$, à l'aide de cette transformation de (9)

$$2f \cdot sg = (f + g)^2 - (f - g)^2 ,$$

où on fait $f = a^2 - b^2$, $g = c^2 - d^2$, on obtiendra une identité de forme $x^2 + y^2 + z^2 = x'^2 + y'^2 + z'^2$, trouvée par B. af Genäs.

48. *Si* $ax - by = 1$, *les valeurs* $X = y^2(3ax - by)$ *et* $Y = x^2(3by - ax)$ *satisfont à l'équation* $b^2X - a^2Y = 1$ (Bouniakowsky)[1]. On n'a qu'à changer α et β en $\frac{a}{y}$ et $\frac{b}{x}$ dans l'identité $(\alpha - \beta)^3 = (3\alpha - \beta)\beta^2 - (3\beta - \alpha)\alpha^2$.

[1] Le savant russe est arrivé à cette conclusion, ainsi qu'à d'autres plus générales, à l'aide de la formule d'intégration par parties.

49. *Soit* $f^3 + ag^3 = bh^3$; *on aura une autre solution de* $x^3 + ay^3 = bz^3$ *en faisant*

$$x = f(f^3 + 2ag^3) , \quad y = -g(2f^3 + ag^3) , \quad z = h(f^3 - ag^3) . \quad \text{(Euler)}$$

Prestet avait trouvé, avant Euler, le cas particulier de $a = b = 1$.

50. Effectuant, de deux manières différentes, le produit

$$(f + g\sqrt{-k})^4 (f - g\sqrt{-k})^4 ,$$

on aura une identité de A. Boutin donnant une solution de $x^4 = y^2 + kz^2$.

51. Posant $k\sqrt{a} + l\sqrt{-b} = (x\sqrt{a} + y\sqrt{-b})^3$, puis égalant les coefficients de $\sqrt{a}$ et ceux de $\sqrt{-b}$, il vient

$$k = ax^3 - 3bxy^2 , \qquad l = 3ax^2y - by^3 ,$$

d'où

$$ak^2 + bl^2 = (ax^2 + by^2)^3 . \quad \text{(Euler)}$$

52. Développant l'expression $(a + bi)^3(a - bi)^3$ et l'identifiant à $(a^2 + b^2)^3$, on trouvera un cas particulier de l'identité précédente, qui montre à déterminer un cube qui soit la somme de deux carrés (Euler).

53. *Théorème de Binet.* Voir *Ens. Math.*, 1907, p. 303, ex. 11.

54. *Egalités multiples.* Voir *Ens. Math.*, 1914, p. 18.

55. *Factorisation.* Voir *Ens. Math.*, 1913, p. 202 et seq. passim.

56. *Fractions continues.* Voir *Ens. Math.*, 1912, p. 184 et seq. passim.

57. *Carrelages.* On obtient de remarquables carrelages en considérant comme axes de coordonnées deux droites rectangulaires d'une feuille *quadrillée* et mettant la case (x, y) en gris ou en noir, selon que le reste de la division de $\alpha(x^2 + y^2)$ par n est de la forme $\mathbf{3} + 1$ ou de la forme $\mathbf{3} - 1$. Voir *S. Œ.*, 1912.

58. *Triangles.* 1° *L'une des cathètes du triangle* $x^2 + y^2 = z^2$ *est toujours paire* (Frénicle). On la désignera par $2fg$.

2° *Tous les triangles sont donnés par la formule d'Euclide* (ex. n° 6). Conséquence de 1°. Les deux générateurs sont, dans ce qui suit, désignés par f et g.

3° *L'hypoténuse est de l'une des formes* $12 + 1$, 5 (anonyme arabe). Le triangle étant primitif, $z = f^2 + g^2$ est impair, et z^2, de la forme $4 + 1$.

4° *Une cathète est multiple de* 3 *et une autre, multiple de* 4 (Frénicle).

5° *L'un des côtés est multiple de* 5 (Id.). On examine les formes linéaires de f et de g relativement au module 5.

6° *La somme et la différence de deux cathètes sont de l'une des formes* 8 ± 1 (Id.).

7° *Le seul triangle* 3, 4, 5 *a ses côtés en progression arithmétique. Il n'y en a aucun les ayant en progression géométrique* (Ozanam).

8° *Si les générateurs* f, g *sont deux triangulaires consécutifs, le côté* $f^2 - g^2$ *est cube* (Id.).

9° *Si* $f = g + 1$, *l'hypoténuse surpasse de* 1 *la cathète paire* (Id.).

10° *Si les deux cathètes diffèrent de* 1, *le triangle ayant pour générateurs* $(2f + g)$ *et* f *sera dans le même cas* (Fermat).

11° *Si l'on prend pour générateurs deux termes successifs de la série* 1, 2, 5, 12, 29, 70, ... *les deux cathètes diffèrent de* 1 (Ozanam). C'est le théorème précédent de Fermat[1].

12° *Trouver un triangle dont la bissectrice soit rationnelle* (Diophante). Il faut rendre rationnelle l'expression $2f\sqrt{f^2+g^2}$, ce qui se fait en posant $f = k(\varphi^2 - \gamma^2)$, $g = k(2\varphi\gamma)$.

13° *Trouver un triangle dont le périmètre soit un carré* (Id.). Il s'agit d'égaler à un carré le nombre $2f(f+g)$, ce qu'on fait en écrivant $f = 2u^2$, $g = v^2 - 2u^2$.

14° *Trouver un triangle dont la somme des cathètes soit un carré* (Teilhet). La question se ramène à rendre carré le nombre $f^2 + 2fg - g^2$; on y arrive en faisant

$$f = u^2 - 2uv + v^2 , \qquad g = 2uv ,$$

15° *Trouver trois carrés en progression arithmétique* (Fibo-

---

[1] En général si les deux premiers termes sont 1, a, les cathètes successives diffèrent de $a^2 - 2a - 1$. On peut d'ailleurs continuer la série en remontant : ainsi, pour $a = 4$, on a : ... — 19, 8, — 3, 2, 1, 4, 9, 22, ... C'est vraisemblablement ainsi qu'Ozanam a trouvé la liste des triangles dont les cathètes diffèrent de 7 (*Dict. math.*). On voit qu'il pratiquait virtuellement la théorie des séries récurrentes.

nacci). Comme on a :

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

le problème est ramené à faire $a = f^2 - g^2$, $b = 2fg$, ce qui donne l'identité

$$(f^2 - g^2 - 2fg)^2 + (f^2 - g^2 + 2fg)^2 = 2(f^2 + g^2) .$$

Cette solution paraît due aux Arabes[1]. Fibonacci a fait remarquer que la raison $4fg(f^2 - g^2)$ est divisible par 24; il en déduit la solution du système $x^2 + y^2 = u^2$, $x^2 - y = v^2$.

On est ramené à ce même problème en cherchant un *triangle dont la seconde bissectrice soit rationnelle,* ou encore, en cherchant avec A. Boutin *trois triangulaires en progression arithmétique.*

16° *Trouver deux triangles tels que la différence des deux plus grands côtés de chacun soit égale à celle des deux plus petits de l'autre* (Frénicle). Voir *Œuvres de Fermat,* t. IV, p. 253.

17° *Trouver trois triangles dont les aires soient égales* (Diophante). Les valeurs

$$x = k^2 - 1 , \qquad y = 2k + 1 , \qquad z = k^2 + k + 1$$

satisfont à l'équation $x^2 + xy + y^2 = z^2$; de là la solution de Diophante

$$2xz(z^2 - x^2) = 2zy(z^2 - y^2) = 2z(x + y)[(x + y)^2 - z^2] .$$

18° *Il est impossible de trouver deux triangles tels que les deux plus grands côtés diffèrent également de même que les plus petits.*

19° *Trouver un triangle dont l'hypoténuse soit un carré, ainsi que la somme de ses cathètes* (Fermat). Ces dernières étant $x = u^2 - v^2$ et $y = 2uv$, on pose $u = \lambda^2 - \mu^2$ et $v = 2\lambda\mu$. Il faut que $x + y = \lambda^4 + 4\lambda^3\mu - 6\lambda^2\mu^2 - 4\lambda\mu^3 + \mu^4$ soit un carré, qu'on supposera [2] égal à celui de $\lambda^2 - 2\lambda\mu + \mu^2$,

[1] On la voit, pour la première fois, dans S'Gravesande, *Math. univ. elem.* (Leyde, 1727).

[2] Ce procédé porte le nom de Fermat. Si $a = \alpha^2$, ou si $e = \varepsilon^2$, on résoudra $a + bx + cx^2 + dx^3 + ex^4 = y^2$ en l'assimilant au carré de $\alpha + ux + vx^2$, ou de $u + vx + \varepsilon x^2$, et on disposera de u et de v de manière à obtenir une égalité de la forme $Ax = B$. Connaissant une solution $x = n$, on en aura une nouvelle en changeant x en $x' + n$, et ainsi de suite. Euler a traité des cas analogues de l'équation $a + bx + cx^2 + dx^3 = y^2$.

ce qui donnera $\lambda = \frac{3\mu}{2}$ et $\mu = -119$, solution à rejeter. Posons, en conséquence, $\lambda = \frac{3\mu}{2} + \nu$, il viendra une expression en μ et ν qu'on assimilera au carré de $\mu^2 + 148\mu\nu - 4\nu^2$; on trouvera ainsi $\mu = 84$, $\nu = 1343$, $\lambda = 1469$, d'où

$$x = 4565486027761 , \qquad y = 106165229352 .$$

Lagrange a montré que ces nombres sont bien les plus petits qui répondent à la question, ainsi que l'avait affirmé Fermat.

20° *Si* (x, y, z) *définit un triangle, les nombres* (2x + y + 2z, x + 2y + 2z, 2x + 2y + 3z) *en définissent un autre dont les cathètes diffèrent autant que celles du premier.* De là, le moyen de *trouver une série infinie de triangles dont les cathètes diffèrent de la même quantité* (Wilkinson). *Les séries ainsi obtenues, en partant de* 0, n, n, *et faisant varier* n, *donnent tous les triangles possibles* (Monck). Voir *M.*, 1906, p. 113.

21° En outre du triangle possédant un angle droit, on pourrait étudier le triangle possédant un angle de 60°. *La formule qui relie les côtés d'un tel triangle est* $x^2 - xy + y^2 = z^2$, *et les formules générales des côtés sont :* [1]

$$x = 3f^2 - g^2 - 2fg , \qquad y = 3f^2 - g^2 + 2fg , \qquad z = 3f^2 + g^2 .$$

59. *Si* (a, b, c; d) *désigne une solution de l'équation* $x^2 + y^2 + z^2 = w^2$ *donnant, en nombres entiers, les côtés et la diagonale d'un parallélipipède rectangle, l'expression*

$$(a + b + d , \quad a + c + d , \quad b + c + d ; \quad a + b + c + 2d)$$

en désigne un autre dans le même cas (Monck). De là une infinité de semblables solides, en partant de (1, 2, 2; 3) [2].

---

[1] Elles se tirent des formules de l'exercice 7, en remarquant que $(2z)^2 = (x + y)^2 + 3(x - y)^2$.
Les triangles quelconques fournissent également d'intéressantes questions. Ainsi *considérons la série des triangles tels que les côtés de chacun soient les demi-sommes de ceux du précédent, ces triangles tendront vers le triangle équilatéral isopérimètre* (Mackay). Voir aussi *S. Œ.*, 1913, p. 182.

[2] On a étudié de même, à la suite d'Euler, le parallélipipède rectangle dont les côtés et les diagonales superficielles sont des nombres entiers, ainsi que le trièdre tri-rectangle à côtés entiers. Mais on ne connaît pas de solutions générales de ces deux problèmes.

60. 1° *Désignons par* $\mathrm{E}\omega$ *la partie entière du nombre non entier* ω, *on a :*

(α) $0 < \omega - \mathrm{E}\omega < 1$,

(β) $-1 < \mathrm{E}\omega - \omega < 0$

(γ) $\mathrm{E}\omega < \omega < 1 + \mathrm{E}\omega$,

(δ) $\mathrm{E}(\omega \pm a) = \mathrm{E}\omega \pm a$

(ε) $\mathrm{E}(\omega + \omega') - \mathrm{E}(\omega + \omega'') = \mathrm{E}(\omega' - \omega'')$

(φ) $\mathrm{E}(a - \omega) = a - 1 - \mathrm{E}\omega$

2° *Entre* ω *et* ω' *il y a* $(\mathrm{E}\omega - \mathrm{E}\omega')$ *entiers.*

3° *Dans les* b *premiers entiers, il y a* $\mathrm{E}\frac{b}{a}$ *multiples de* a.

4° *Le plus grand multiple de* a *inférieur à* b *est* $a\mathrm{E}\frac{b}{a}$. On peut le désigner aussi par l'expression $b - \mathrm{R}\frac{b}{a}$.

5° *Déterminer* x *tel que le quotient* q *de* a *divisé par* b *ne change pas quand on ajoute* x *à chacun de ces deux nombres.* On a

$$0 \leq a + x + q(b + x) \leq b + x$$

d'où deux limites de x.

6° *Si* $\omega - \mathrm{E}\omega < \frac{1}{n}$, *on a :* $\mathrm{E}(n\omega) = n\mathrm{E}\omega$. On multiplie la relation donnée par n et on lui ajoute, membre à membre, la relation (β) après qu'on y a changé ω en $n\omega$.

7° *On a :* $0 \leq \mathrm{E}(n\omega) - n\mathrm{E}\omega < n$. On multiplie (α) par n et on ajoute la transformée de (β) du n° précédent.

8° On a :

$$\frac{a}{\mathrm{E}\omega} - \frac{a}{\omega} < \frac{a}{(\mathrm{E}\omega)^2} \; ; \qquad \sqrt{\omega} - \sqrt{\mathrm{E}\omega} < \frac{1}{2\sqrt{\mathrm{E}\omega}} \; ;$$

$$\mathrm{E}\omega + \sqrt{\omega - \mathrm{E}\omega} - \omega < \frac{1}{4} \; ; \quad a\mathrm{E}\omega - \mathrm{E}(\omega\omega') - \mathrm{E}[(a - \omega')\omega] = 0 \text{ ou } 1 \; ;$$

$$\mathrm{E}\sqrt{a(a+1)} = \mathrm{E}\sqrt{a(a+2)} = \mathrm{E}\sqrt[3]{a(a+1)(\ +2)} = a \; ;$$

$$\mathrm{E}\sqrt{a(a+1)(a+2)(a+3)} = a(a+3)\,[1] \; ;$$

$$\mathrm{E}\sqrt[3]{a(a+1)\ldots(a+5)} = a^2 + 5a + 3 \; ; \qquad \text{(Goulard)}$$

$$\mathrm{E}(e\sqrt[n]{n!}) = n + 1 \; . \qquad (\textit{Ens. Math.}, 1906, \text{p. } 354)$$

9° *On a :* $\mathrm{E}\frac{\mathrm{E}\frac{a}{b}}{c} = \mathrm{E}\frac{\mathrm{E}\frac{a}{c}}{b} = \mathrm{E}\frac{a}{bc}$. On fait $\omega = \frac{a}{b}$ dans (α) et

[1] On n'a ainsi d'ailleurs que des approximations assez grossières, car, augmentant de 1 la partie sous le radical, on obtient le carré de $a(a+3)$.

on divise par c; on ajoute ensuite, membre à membre, avec la relation (β) où on a fait $\omega = \frac{a}{bc}$.

10° Faisons, dans la relation de 7°, $n = 2$, $\omega = \frac{a}{b}$, puis dans (β), $\omega = \frac{2a}{b}$, et additionnons ; on conclura que $\left(\mathrm{E}\frac{2a}{b} - 2\mathrm{E}\frac{a}{b}\right)$ *est égal à* 0 *ou à* 1, *selon que* $\mathrm{E}\frac{2a}{b}$ *est pair ou impair* (Catalan). Généraliser.

11° *Pour* $a < b$, *on a :*

$$\mathrm{E}\left(\frac{a}{b}\mathrm{E}\frac{cb}{a}\right) = c - 1 \qquad \text{et} \qquad \mathrm{E}\left[\frac{a}{b}\left(1 + \mathrm{E}\frac{cb}{a}\right)\right] = c .$$

Par exemple, pour la première relation, on fait d'abord dans (α), $\omega = \frac{cb}{a}$ et on multiplie par $\frac{a}{b}$; puis $\omega = \frac{a}{b}\mathrm{E}\frac{cb}{a}$, et on additionne, membre à membre.

12° *Soit* $(3 + \sqrt{5})^n = a + b\sqrt{5}$, *on a :* $a = \mathrm{E}(b\sqrt{5}) + 1$. Voir Fitz-Patrick, op. cit. 569.

13° Voir *Ens. Math.*, 1910, pp. 458 et 472, plusieurs utilisations et figurations de la fonction $\mathrm{E}\omega$.

14° De la relation $\mathrm{E}(\omega + 1) = 1 + \mathrm{E}\omega$, on conclut que, quel que soit l'entier n, il y a un nombre non entier ξ positif et plus petit que n, tel que $\omega + \frac{\xi}{n} = 1 + \mathrm{E}\omega$; ce qui donne $\xi = n\mathrm{E}\omega - n\omega + n$, d'où, à cause de (δ)

$$\mathrm{E}\xi = n\mathrm{E}\omega - \mathrm{E}(n\omega) + n ;$$

à cause de 7°. On peut donc dire, avec Hermite, que *dans la suite*

$$\mathrm{E}\omega , \qquad \mathrm{E}\left(\omega + \frac{1}{n}\right) , \qquad \mathrm{E}\left(\omega + \frac{2}{n}\right) , \ \ldots$$

chacun des $(n\mathrm{E}\omega - \mathrm{E}(n\omega) + n)$ *premiers termes est égal au premier.*

15° *Soit* $\mathrm{E}\omega = a$, l'expression

$$\frac{\omega^n + \mathrm{C}_{2n,2}\,\omega^{n-1}a^2 + \mathrm{C}_{2n,4}\,\omega^{n-2}a^4 + \ldots}{\mathrm{C}_{2n,1}\,\omega^{n-1}a + \mathrm{C}_{2n,3}\,\omega^{n-2}a^3 + \mathrm{C}_{2n,5}\,\omega^{n-3}a^5 + \ldots}$$

tend vers la limite $\sqrt{\omega}$, *à mesure que* n *augmente.*

16° *Le nombre de fois que le nombre premier* p *est facteur dans* n ! *s'exprime par*

$$\mathrm{E}\frac{n}{p} + \mathrm{E}\frac{n}{p^2} + \mathrm{E}\frac{n}{p^3} + \ldots \qquad \text{(Legendre)}$$

17° *Si* $a < b$, *les* $\left(\mathrm{E}\dfrac{b}{\mathrm{E}\dfrac{b}{a+1}} - a\right)$ *premiers termes de la série*

$$\mathrm{E}\frac{b}{a+1}, \quad \mathrm{E}\frac{b}{a+2}, \ldots$$

sont égaux au premier (Berger).

18° *Démontrer les relations suivantes :*

$$\mathrm{E}\frac{a+1}{2} + \mathrm{E}\frac{a+2}{4} + \mathrm{E}\frac{a+4}{8} + \ldots = a, \qquad \text{(Cesaro)}$$

$$\Sigma\mathrm{E}\frac{a-bx}{c} = \Sigma\mathrm{E}\frac{a-cx}{b}^{1} \qquad \text{(Hermite)}$$

$$\Sigma\mathrm{E}\frac{a+x}{2x} = \Sigma\mathrm{E}\frac{a}{2x-1}, \qquad \Sigma\mathrm{E}\frac{a-bx}{x} = \Sigma\mathrm{E}\frac{a}{b+x}, \qquad \text{(Cesaro)}$$

19° On pourra s'exercer sur d'autres fonctions analogues. Ainsi, appelons $\mathrm{I}(\omega) = \mathrm{E}(2\omega) - \mathrm{E}(\omega)$ l'expression de l'entier le plus voisin du nombre ω, non entier ni moitié d'un entier ; on a :

$$\mathrm{I}\frac{\omega}{2} + \mathrm{I}\frac{\omega}{4} + \mathrm{I}\frac{\omega}{8} + \ldots = \mathrm{E}\omega. \qquad \text{(Cesaro)}$$

61. Soit n un nombre non carré, et désignons respectivement par a, b, c, d, ... l'excès de n, de na, de nb, de nc, ... sur le plus grand carré inférieur au nombre considéré n, na, nb, nc, ... ; les nombres 1, a, b, c, d forment une *suite de Brocard. Une telle suite est périodique, et le nombre des*

[1] Chacun des deux membres de cette égalité représente le nombre de solutions du problème figuré par la relation $cy + bz \leq a$ (Cesaro).

termes de la période est inférieur à 4n. Soient en effet k et l deux termes successifs, et $kn = r^2 + s$; on a :

$$l = s\ , \qquad s \leqq 2r\ , \qquad 4kn = 4r^2 + 4s \geqq s^2 + 4s > s^2\ ,$$

d'où $l^2 < 4nk$. Si h désigne une certaine puissance de 2, on a :

$$l^2 < (4n)(2\sqrt{n})(\sqrt{2\sqrt{n}})(\sqrt[4]{2\sqrt{n}}) \ldots \sqrt[h]{a} < 16n^2 \sqrt[h]{a}\ , \quad \text{d'où} \quad l \leqq 4n\ .$$

62. Posons $k\pi = n\varphi$; *l'expression* $\frac{\sin(2n-1)\varphi + \sin\varphi}{2\sin\varphi}$ *a pour valeur* n *ou* 0, *selon que* k *est ou n'est pas multiple de* n (Libri).

Les fonctions $0^{0^x}\,0^{0^{a-x}}$ *et* $(1 - 0^{0^{-x}})(1 - 0^{0^{a-x}})$ *ont la valeur* 1 *pour* $0 \leqq x \leqq a$, *et la valeur* 0 *pour toute autre valeur de* x (Id.).

Libri tire de là de curieuses formules sur le nombre des solutions des congruences $ax - bx = c$ et $ax^2 - by^2 \equiv c$, sur la représentation des nombres premiers, la somme des nombres premiers compris entre deux limites données, la détermination d'un nombre premier supérieur à une limite donnée, enfin la somme des diviseurs de divers groupes de nombres. Ces formules n'ont du reste aucun intérêt pratique.