LES FRACTIONS CONTINUES DANS LA THÉORIE ÉLÉMENTAIRE DES NOMBRES

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

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **14 (1912)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-14285

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

LES FRACTIONS CONTINUES DANS LA THÉORIE ÉLÉMENTAIRE DES NOMBRES[1]

1. — Désignons par $E\omega$ la partie entière du nombre positif non entier ω; la quantité $\omega - E\omega$ est < 1 et peut être mise sous la forme $\frac{1}{\omega'}$, ω' étant > 1; de même, $\omega' - E\omega' = \frac{1}{\omega''}$, ω'' étant > 1. En continuant ainsi jusqu'à un terme quelconque Ω, qui sera commensurable ou non en même temps que ω, — on aura le développement de ω en *fraction continue,*

$$\omega = E\omega + \frac{1}{E\omega'} + \frac{1}{E\omega''} + \ldots + \frac{1}{\Omega}$$

qu'on représente plus simplement ainsi :

$$\omega = | E\omega , E\omega', E\omega'' \ldots \Omega | .$$

Il ne s'agira ici que des valeurs de ω fractionnaires ou irrationnelles du deuxième degré.

2. — *Algorithme d'Euclide. Continuants.* — Soient deux nombres positifs N, A, et le premier plus grand que le second. Posons :

$$N = aA + B , \quad A = bB + C , \quad B = cC + D , \ldots$$
$$F = gG + H , \quad G = hH + I , \ldots$$

a, b, c, ... désignant la partie entière des quotients successifs de

[1] Les fractions continues fournissent bien des démonstrations d'importants théorèmes de la théorie des nombres; mais ces démonstrations, indirectes et souvent compliquées, ne peuvent être présentées que comme vérification. Par suite, il faudrait éviter de les mettre en tête d'un traité des nombres, car elles ne permettent pas d'entrer assez rapidement dans le sujet. Au contraire, leur rôle d'application des théories élémentaires paraît tout indiqué.

C'est dans cette idée qu'a été écrit le présent article : ce n'est donc pas une théorie spéciale des fractions continues, avec, comme corollaires, des applications aux propriétés des nombres ; mais, au contraire, la suite d'une étude des nombres où il est fait appel à cette théorie, ce qui a permis de simplifier plusieurs démonstrations. Cette étude, — amenée d'ailleurs par l'exposé des solutions des équations $ax - by = 1$ et $x^2 - ay^2 = 1$, auxquelles se réduisent celles des congruences des deux premiers degrés, — est complétée par l'énoncé des questions élémentaires les plus importantes relatives aux fractions continues, de manière qu'on trouvera réuni ici ce qu'il est le plus indispensable de connaître sur ce sujet.

N par A, de A par B, de B par C, ... et B, C, D, ... les restes correspondants : l'ensemble de ces opérations constitue ce qu'on appelle l'*algorithme d'Euclide*.

On a :

$$(1) \qquad \frac{N}{A} = \left| a, b \ldots h, \frac{H}{I} \right| = \left| a, b \ldots h + \frac{I}{H} \right|$$

et cette décomposition ne peut se faire que d'une seule manière.

Les nombres N, A, B, C, ... décroissent de plus en plus. En outre, ils sont entiers et premiers entre eux si N et A sont eux-mêmes des nombres entiers premiers entre eux.

Ecrivons

$$(0) = 1 , \qquad (a) = a , \qquad (a, b) = (a)b + (0) = ab + 1 ,$$
$$(a, b, c) = (a, b)c + (a) , \quad \ldots$$

et en général,

$$(\alpha) \qquad (a \ldots f, g, h) = (a \ldots f, g)h + (a \ldots f) ;$$

Ces expressions sont appelées les *médiateurs* (Kramp), les *cumulants* (Sylvester), les *objectifs* (Dormoy), ou les *continuants* (Muir) des nombres a, $b \ldots f$, g, h. On les voit définies pour la première fois dans l'*Alg.* de Saunderson.

On peut écrire :

$$(a \ldots f, g)G + (a \ldots f)H = (a \ldots f, g, h)H + (a \ldots f, g)I .$$

Les binômes analogues au premier membre ont donc une valeur constante, égale par conséquent à

$$(a, b)B + (a)C = (ab + 1)B + a(A - bB) = N .$$

Ainsi en général,

$$(2) \qquad (a \ldots g, h)H + (a \ldots g)I = N .$$

De même on a :

$$(b \ldots f, g, h)H + (b \ldots f, g)I = A \quad \text{et} \quad (c \ldots f, g, h)H + (c \ldots f, g)I = B ,$$

d'où

$$(3) \qquad \frac{N}{A} = \left| a, b \ldots f, g, h \right| = \frac{(a \ldots h)H + (a \ldots g)I}{(b \ldots h)H + (b \ldots g)I}$$

$$N = aA + B = [a(b \ldots h) + (c \ldots h)]H + [a(b \ldots g) + (c \ldots g)]I .$$

Comparant cette dernière relation avec (2), il vient

$$(\beta) \qquad a(b \ldots h) + (c \ldots h) = (a \ldots f, g, h) .$$

Or, de (α) on tire, en changeant $a, b, \ldots g, h$, en $h, g, \ldots b, a$,

$$(\gamma) \qquad (h \ldots a) = a(h \ldots b) + (h \ldots c) .$$

Mais on a :

$$(c, b) = cb + 1 = (b, c)$$

$$(d, c, b) = (d, c)b + (d) = (d\,c + 1)b + d = (b\,c + 1)d + b$$

$$= (b, c)d + (b) = (b, c, d) .$$

Donc

$$(d, c, b, a) = a(d, c, b) + (d, c) = a(b, c, d) + (c, d) = (a, b, c, d) .$$

En général, on a cette importante relation, due à Euler,

$$(4) \qquad (a \ldots h) = (h \ldots a) .$$

3. — La somme des deux expressions analogues

$$(b \ldots h)(a \ldots g) - (a \ldots h)(b \ldots g) \quad \text{et} \quad (b \ldots g)(a \ldots f) - (a \ldots g)(b \ldots f)$$

est identiquement nulle, ce qu'on voit en remplaçant les expressions $(a \ldots h)$ et $(b \ldots h)$ par leurs valeurs

$$(a \ldots g)h + (a \ldots f) \qquad \text{et} \qquad (b \ldots g)h + (b \ldots f) .$$

Ces deux expressions ont donc des valeurs égales et de signes contraires, que de proche en proche, on arrivera à représenter ainsi :

$$\pm (b, c)(a, b) \mp (a, b, c)b = \pm (bc + 1)(ab + 1) \mp (abc + a + c)b = \pm 1 .$$

On a donc :

$$(5) \qquad (b \ldots g, h)(a, b \ldots g) - (a, b \ldots g, h)(b \ldots g) = (-1)^t$$

t désignant le nombre des quantités $a, b \ldots g, h$ (Saunderson).

Or on a :

$$(\delta) \qquad A = (b \ldots g)G + (b \ldots f)H , \qquad N = (a \ldots g)G + (a \ldots f)H ,$$

d'où

$$(b \ldots g)N - (a, b \ldots g)A = \pm H .$$

Si A et N sont deux entiers premiers entre eux, on finira par trouver $H = 1$ et $I = 0$, ce qui donnera

$$(6) \qquad (b \ldots g)N - (a \ldots g)A = \pm 1$$

$$(7) \qquad (b \ldots h)N - (a \ldots h)A = 0 .$$

Euler a encore donné la relation suivante

$$(8)\quad (a \dots b, c, d, e \dots f) = (a \dots b, c)(d, e \dots f) + (a \dots b)(e \dots f) ;$$

qui se déduit de la comparaison des coefficients de H dans la seconde relation (δ) et dans celle qu'on trouve en remplaçant C et D dans cette autre

$$N = (a \dots b, c)C + (a \dots b)D$$

par les valeurs

$$C = (d, e \dots f, g)G + (d, e \dots f)H$$

$$D = (e \dots f, g)G + (e \dots f)H .$$

4. — La formule (6) fait voir que A *et* N *étant des entiers premiers entre eux, on peut toujours écrire* $Nx - Ay = \pm 1$, *ainsi que* $Nx' - Ay' = \mp 1$, *les signes étant convenablement choisis,* en faisant dans le dernier cas, $x' = A - x$, $y' = N - y$. De là, la démonstration du *lemme fondamental* (*Ens. Math.*, 1907, p. 287) et le moyen de résoudre l'équation du premier degré à deux inconnues $Nx - Ay = M$ [1].

Les formules (7) et (α) donnent

$$(9)\qquad \frac{N}{A} = \frac{(a \dots f, g, h)}{(b \dots f, g, h)} = \frac{(a \dots f, g)h + (a \dots f)}{(b \dots f, g)h + (b \dots f)}$$

h désignant le quotient correspondant à $H = 1$. Comme d'ailleurs en général d'après (5), les continuants $(a \dots g)$ et $(b \dots g)$ n'ont aucun facteur commun, on peut dire que de (8) on déduit les égalités

$$(10)\qquad (a \dots h) = N , \qquad (b \dots h) = A .$$

Les expressions

$$\frac{(a)}{1} , \qquad \frac{(a, b)}{(b)} , \qquad \frac{(a, b, c)}{(b, c)} , \qquad \frac{(a, b, c, d)}{(b, c, d)} , \qquad \dots$$

sont dites les *réduites* de $\frac{N}{A}$. De la sorte, si une quantité quelconque est définie par une fraction continue $|a, b, c \dots|$, on en

---

[1] On a des tables de solutions toutes faites, par exemple le *Canon mathematicus* de JACOBI (Berlin, 1839), qui donne les solutions *primitives* (inférieures à p) des deux congruences $g^x \equiv a$ et $g^a \equiv x$, g désignant une *racine primitive* de p pour $p < 1000$.

Soit à résoudre $\alpha x - py = \beta$, on cherchera les nombres A et B tels que $g^A \equiv \alpha$ et $g^B \equiv \beta$; on aura : $x \equiv g^{B-A}$.

A défaut des tables de Jacobi, on se servira de celle de GAUSS (*Disq. Arith.*), auteur de cette application des racines primitives; ou de celles d'Ostrogradski, insérées dans les traités de TCHEBICHEF et de CAHEN; ou celles de LEBESGUE (*Tables numériques*, Paris, 1866). Celles de Gauss s'arrêtent à $p = 97$; les secondes à $p = 197$.

trouvera les réduites à l'aide des formules qui précèdent. Dans le cas de N et A entiers, on a vu que leur nombre est limité ; si N et A sont incommensurables, le nombre des réduites est indéfini et on peut s'arrêter à un terme quelconque, qui est alors lui-même incommensurable ; si on a, par exemple,

$$\omega = | a, b, c \ldots e, f, g, \Omega |$$

on peut écrire

$$(11) \qquad \omega = \frac{(a \ldots f, g, \Omega)}{(b \ldots g, \Omega)} = \frac{(a \ldots f, g)\Omega + (a \ldots f)}{(b \ldots f, g)\Omega + (b \ldots f)} \ ^{1}$$

(voir exercices nos 1 à 11).

5. — Supposons que les entiers $a, \ldots b, c \ldots$ soient en nombre impair et leurs valeurs, symétriques, de sorte qu'on puisse les écrire $a \ldots b, c, d, c, b, \ldots a$; (8) deviendra

$$(12) \quad (a \ldots b, c, d, c, b \ldots a) = (a \ldots b, c)\,[(a \ldots b, c, d) + (a \ldots b, c)] \ ;$$

on peut encore affirmer que $(a \ldots b, c, d, c, b \ldots a)$ est un nombre composé, à moins que $(a \ldots c)$ ne soit égal à 1, ce qui ne peut avoir lieu si $a > 1$.

Si ces mêmes entiers sont en nombre pair et leurs valeurs également symétriques, on aura :

$$(13) \qquad (a \ldots c, d, d, c \ldots a) = (a \ldots c, d)^2 + (a \ldots c)^2 \ .$$

Soient A, A′, A″, ... les entiers premiers avec N et inférieurs à la moitié de ce dernier ; les quotients de N par ces mêmes nombres auront leur partie entière plus grande que 1. Soit $\frac{(a, b \ldots e, f)}{(b \ldots e, f)}$ la dernière réduite de $\frac{N}{A}$; on aura

$$N = (a, b \ldots e, f) \qquad \text{et} \qquad A = (b \ldots e, f) \ .$$

De même la fraction $\frac{(a, b \ldots e, f)}{(a, b \ldots e)}$, après calcul des continuants et réduction en fraction continue, donnera $(a, b \ldots e)$ égal à un des nombres A, A′, ... Ainsi, à chacun des nombres A, A′, ... correspond un autre nombre qui donne un continuant semblable, sauf qu'il a un terme de plus à droite et un de moins à gauche.

---

[1] La formule (11) se déduit directement de (α) en remarquant que la supposition

$$| b, c \ldots \Omega | = \frac{(b, c \ldots \Omega)}{(c \ldots \Omega)} \text{ entraîne la relation } | a, b, c \ldots \Omega | = a + \frac{1}{| b, c \ldots \Omega |} = \frac{a(b, c \ldots \Omega) + (c \ldots \Omega)}{(b, c \ldots \Omega)} \ .$$

Dans le cas particulier où N est un nombre premier $4 + 1$, les nombres A, A′, ... ne sont autres que les entiers 2, 3, 4, ... $\frac{N-1}{2}$ qui sont en nombre impair : il faut donc qu'un de ces nombres, par exemple A‴, se corresponde à lui-même. Si $a, b, \ldots g, h$ sont les quotients qui résultent du développement de $\frac{N}{A'''}$ en fraction continue, on a évidemment $(a, b \ldots g) = (h, g \ldots b)$; le continuant $(a, b \ldots g, h)$ est donc symétrique, et il ne peut être formé d'un nombre impair de termes, puisqu'on a : $a > 1$, et que, d'autre part, N est premier.

On a ainsi la démonstration de ce célèbre théorème de Fermat : *tout nombre premier* $4 + 1$ *est une somme de deux carrés*, et un moyen facile d'en déterminer la composition (Smith). (Voir exercices nos 12 et 13.)

6. — *Lemme.* L'entier y variant de 0 à k, et ω désignant un nombre irrationnel, appelons x l'entier $1 + E(y\omega)$ immédiatement supérieur à $y\omega$; on aura $0 < x - y\omega < 1$. La valeur de $x - y\omega$ est comprise entre deux des fractions $\frac{0}{k}, \frac{1}{k}, \frac{2}{k}, \ldots \frac{k}{k}$. Comme il n'y a que k intervalles et que y, et par suite $x - y\omega$, peuvent prendre $k + 1$ valeurs, il y a au moins un intervalle comprenant deux valeurs de $x - y\omega$, et on peut écrire :

$$0 < (x' - y'\omega) - (x'' - y''\omega) < \frac{1}{k} \quad \text{ou} \quad 0 < (x' - x'') - (y' - y'')\omega < \frac{1}{k} ;$$

$y' - y''$ est une des valeurs de y ; donc, en écrivant $x' - x'' = x$, il vient

$$(\varepsilon) \qquad 0 < x - y\omega < \frac{1}{k} < \frac{1}{y} .$$

Prenons k' assez grand pour que la plus petite valeur de $x - y\omega$ soit $> \frac{1}{k'}$; on obtiendra, de la même manière que tout à l'heure, un autre couple ξ, η, qui donnera une nouvelle solution de (ε), et ainsi de suite.

Par conséquent, *on peut toujours trouver une infinité de couples de valeurs de* x *et de* y *satisfaisant à la relation* $x - y\omega < \frac{1}{k}$ (Lejeune-Dirichlet).

Cor. Posons $\omega = \sqrt{n}$; on peut trouver une infinité de solutions de l'inégalité

$$(\zeta) \qquad 0 < x - y\sqrt{n} < \frac{1}{y} ,$$

ce qui permet d'écrire

$$0 < x + y\sqrt{n} < \frac{1}{y} + 2y\sqrt{n} ,$$

et, en multipliant,

$$0 < x^2 - ny^2 < \frac{1}{y^2} + 2\sqrt{n} < 1 + 2\sqrt{n} .$$

Ainsi, θ *désignant un certain entier compris entre* 0 *et* $1 + 2\sqrt{n}$, *l'équation* $x^2 - ny^2 = \theta$ *a une infinité de racines* (id.).

(Voir exercices nos 14 et 15.)

7. — *Problème de Fermat.* — *Si* n *désigne un nombre non carré, l'équation* $t^2 - nu^2 = 1$ *a une infinité de solutions.* (Fermat). Démonstration de Lejeune-Dirichlet. Parmi l'infinité de couples de solutions de $x^2 - ny^2 = \theta$, il ne peut se trouver plus de θ^2 couples tels que x et y divisés par θ donnent pour restes toutes les combinaisons des nombres inférieurs à θ. Il existe donc une infinité de couples qui donnent les mêmes restes, et on peut écrire :

$$x'^2 - ny'^2 = x''^2 - ny''^2 = \theta , \qquad x'' = x' + \alpha\theta , \qquad y'' = y' + \beta\theta ,$$

d'où, en posant $1 + \alpha x' - n\beta y' = t$, $\alpha y' - \beta x' = u$,

$$(x' \mp y'\sqrt{n})(x'' \pm y''\sqrt{n}) = \theta(t \mp u\sqrt{n}) ,$$

ce qui conduit facilement à l'équation $t^2 - nu^2 = 1$, où u est différent de zéro, car autrement on aurait

$$t = \pm 1 \qquad \text{et} \qquad x' - y'\sqrt{n} = \pm (x'' - y''\sqrt{n}) ,$$

ou bien

$$x' = \pm x'' \qquad \text{et} \qquad y' = \pm y'' ;$$

or x' et x'' peuvent être supposés positifs et inégaux, de même que y' et y''.

Cor. 1. *Soit* $x = a$, $y = b$ *une solution de* $x^2 - ny^2 = 1$; *les expressions*

$$(14) \qquad \begin{cases} x_k = a^k + C_{k,2}\, a^{k-2} b^2 n + C_{k,4}\, a^{k-4} b^4 n^2 + \dots \\ y_k = k a^{k-1} b + C_{k,3}\, a^{k-3} b^3 n + C_{k,5}\, a^{k-5} b^5 n^2 + \dots \end{cases}$$

en donneront une infinité d'autres, en faisant $k = 2, 3, 4, \dots$ (Euler). En effet

$$x_k \pm y_k\sqrt{n} = (a \pm b\sqrt{n})^k \qquad \text{d'où} \qquad x_k^2 - ny_k^2 = 1 .$$

Les formules (14) peuvent s'écrire

$$(15)\qquad \begin{cases} 2x_k = (a + b\sqrt{n})^k + (a - b\sqrt{n})^k , \\ 2y_k\sqrt{n} = (a + b\sqrt{n})^k - (a - b\sqrt{n})^k . \end{cases}$$

Les solutions forment deux *séries récurrentes* dont *l'échelle* est $2a$ et $-(a^2 - nb^2) = -1$, c'est-à-dire que $x_{k+1} = 2ax_k - x_{k-1}$ et $y_{k+1} = 2ay_k - y_{k-1}$.

II. Soit (x_1, y_1) la solution en nombres minima, et soit (u, v) une solution non comprise dans la série (x_1, y_1), (x_2, y_2), (x_3, y_3), ... On peut écrire $x_k < u < x_{k+1}$, et il s'ensuivra $y_k < v < y_{k+1}$.

Par suite on aura

$$x_k + y_k\sqrt{n} < u + v\sqrt{n} < x_{k+1} + y_{k+1}\sqrt{n} .$$

Le dernier membre est égal à

$$(x_k + y_k\sqrt{n})(x_1 + y_1\sqrt{n}) = \frac{x_1 + y_1\sqrt{n}}{x_k - y_k\sqrt{n}} ;$$

on a donc :

$$1 < (ux_k - nvy_k) + (vx_k - uy_k)\sqrt{n} < x_1 + y_1\sqrt{n} ;$$

or $(ux_k - nvy_k)^2 - n(vx_k - uy_k)^2 = 1$. On aurait ainsi une solution en termes positifs et moindres que x_1, y_1, ce qui est contre l'hypothèse, laquelle est donc à rejeter. (Voir exercices n^{os} 16 à 21.)

8. *Algorithme d'Euler.* — Soient a' la racine $E\sqrt{n}$ du plus grand carré contenu dans l'entier n, et a'' le reste $n - a'^2$. Considérons la septuple série

$$\begin{array}{cccccccccc} a' & b' & \dots & d' & e' & f' & g' & h' & \dots \\ a'' & b'' & \dots & d'' & e'' & f'' & g''' & h'' & \dots \\ \alpha & \beta & \dots & \delta & \varepsilon & \varphi & \gamma & \eta & \dots \\ a & b & \dots & d & e & f & g & h & \dots \\ \alpha' & \beta' & \dots & \delta' & \varepsilon' & \varphi' & \gamma' & \eta' & \dots \\ A' & B' & \dots & D' & E' & F' & G' & H' & \dots \\ A & B & \dots & D & E & F & G & H & \dots \end{array}$$

dans laquelle les termes f' et f'' supposés connus, les termes qui

suivent ceux-ci sont déterminés par les lois générales suivantes :

$$(\eta)\quad \varphi = \frac{\sqrt{n} + f'}{f''}\ , \qquad (\theta)\quad f = \mathrm{E}\varphi\ , \qquad (\iota)\quad g' = ff'' - f'\ ,$$

$$(\varkappa)\quad g'' = \frac{n - g'^2}{f''}\ , \qquad (\lambda)\quad \varphi' = \frac{\sqrt{n} - g'}{f''} = \frac{g''}{\sqrt{n} + g'}\ ,$$

$$(\mu)\quad \mathrm{F}' = (a', a, b, \ldots e, f)\ , \qquad (\nu)\quad \mathrm{F} = (a, b, \ldots e, f)\ .$$

Les termes représentés par des lettres grecques sont irrationnels ; tous les autres sont entiers : on voit en effet que si $n - f'^2$ est divisible par f'', il en est de même, d'après (ι) de $n - g'^2$; or $n - a'^2$ est divisible par a'' : il en est donc ainsi en général.

L'algorithme renfermé dans les formules (η), (θ), (ι), $(\varkappa)$, (λ), connu probablement de Fermat et entrevu par Bonbelli, Cataldi et Wallis, a été présenté explicitement par Euler et démontré par Lagrange. Il résulte immédiatement de la décomposition de $\sqrt{n}$ en fraction continue, comme il a été dit au n° **1**.

(Voir exercices n^{os} 23 à 26.)

9. — Si on a $2\sqrt{n} > \sqrt{n} + f' > f'' > 0$, il s'ensuit $\varphi > 1$ et, à cause de (θ), $1 > \varphi - f > 0$. Comme, à cause de (η), de (ι) et de (λ), on a :

$$(17)\qquad \varphi - f = \varphi'$$

(λ) donne en outre

$$(18)\qquad f'' + g' > \sqrt{n} > g' \qquad \text{et} \qquad \sqrt{n} + g' > g'' > 0$$

d'où

$$(19)\qquad 2\sqrt{n} > \sqrt{n} + g' > g'' > 0\ .$$

Ainsi, de l'hypothèse où on s'est placé, on conclut que les nombres $\sqrt{n} + g'$ et g'' sont également compris entre $2\sqrt{n}$ et 0 ; et, puisque $2\sqrt{n} > \sqrt{n} + a' > a'' > 0$, cette propriété est générale.

Les nombres $a, b, \ldots f, g, \ldots$ sont donc $\geqq 1$ et $\leqq 2a'$: ils forment par conséquent une série pouvant être partagée en *périodes* d'un nombre fini de termes, puisqu'ils ont des limites finies et se reproduisent d'après une même loi, ce qui fait que la combinaison f', f'', par exemple, doit se retrouver nécessairement, ainsi que le nombre f, qui dépend d'elle.

Cor. De $f' < \sqrt{n}$, on déduit

$$(20)\qquad ff'' = f' + g' < \sqrt{n} + g'\ .$$

Or f est entier et positif, donc, à fortiori,

$$(21) \qquad f'' < \sqrt{n} + g' = \frac{f'' g''}{\sqrt{n} - g'} ,$$

d'où

$$(22) \quad g'' > \sqrt{n} - g' = \sqrt{n} + h' - gg'' \qquad \text{et} \qquad g > \frac{\sqrt{n} + h'}{g''} - 1 .$$

Mais, par le changement de f, f', f'' et g' en g, g', g'' et h', (20) fournit la relation

$$(23) \qquad g < \frac{\sqrt{n} + h'}{g''} ;$$

des deux limites de g qu'on vient ainsi de déterminer, on tire cette formule de Lagrange

$$(24) \qquad g = \mathrm{E}\frac{\sqrt{n} + h'}{g''} .$$

10. — Il est aisé de voir qu'on a :

$$\sqrt{n} = a' + \frac{1}{\alpha} , \quad \alpha = a + \frac{1}{\beta} , \ldots \quad \varphi = f + \frac{1}{\gamma} , \quad \gamma = g + \frac{1}{\eta} , \ldots$$

Le nombre $\sqrt{n}$ peut donc se décomposer en une fraction continue *illimitée*

$$(25) \quad | \, a', a, b, \ldots c, d \, ; \quad e \ldots f, g, h \, ; \quad e \ldots f, g, h \, ; \quad e \ldots |$$

dont les termes sont périodiques et $\leqq 2a'$: cette expression (25) peut d'ailleurs se remplacer par une infinité d'autres fractions continues limitées dont le dernier terme est irrationnel. Ainsi on a :

$$(26) \quad \sqrt{n} = | \, a', a, b, c, \ldots f, \gamma \, | = | \, a', a \ldots e \ldots f \ldots f, \gamma \, | = \ldots$$

Par exemple, pour $n = 19$, on a les valeurs suivantes de a', b', ..., a'', b'', ..., et a, b, ...

$$4, 2, 3, 3, 2, 4 \, ; \quad 4 \ldots$$

$$3, 5, 2, 5, 3, 1 \, ; \quad 3 \ldots$$

$$2, 1, 3, 1, 2, 8 \, ; \quad 2 \ldots$$

ce qui donne

$$\frac{\sqrt{19} + 4}{3} = | \, 2, 1, 3, 1, 2, 8 \, ; \quad 2, 1, 3, 1, 2, 8 \, ; \ldots |$$

(Voir exercices n^{os} 27 et 28.)

11. — Considérons les couples ... c', c''; d', d''; e', e''; et g', g''; h', h''; e', e''; arrêtés à un même couple e', e''. On a, d'après $(\varkappa)$

$$d''e'' + e'^2 = h''e'' + e'^2 \qquad \text{d'où} \qquad d'' = h'' ,$$

et, à cause de (24),

$$d = \mathrm{E}\frac{\sqrt{n} + e'}{d''} = h , \qquad \text{d'où} \qquad d' = dd'' - e' = h' ,$$

et de là,

$$c'' = g'' , \qquad c = g , \qquad c' = g' , \qquad \text{et ainsi de suite.}$$

On conclut de ce qui précède que la période commence au premier terme même de la série, ce qui fait qu'on peut écrire

$$(27) \quad \begin{cases} \sqrt{n} = | \, a', a \ldots f \ldots h \; ; \; a \ldots f \ldots h \; ; \; a \ldots f, \gamma \, | \\ \qquad = | \, a', a \ldots f \ldots h \; ; \; a \ldots f \ldots h \; ; \; a \ldots \, | \end{cases}$$

Mais d'après $(\varkappa)$ on a : $a''h'' = n - a'^2 = a''$. On en conclut que

$$h'' = 1 , \quad h = \mathrm{E}\sqrt{n} + a' = 2a' , \quad h' = hh'' - a' = a' , \quad g'' = \frac{n - h'^2}{h''} = a'' .$$

(Voir exercice n° 29.)

12. — A cause de (11) on a :

$$(28) \qquad \sqrt{n} = \frac{\mathrm{F}'\gamma + \mathrm{E}'}{\mathrm{F}\gamma + \mathrm{E}} ;$$

d'où, en remplaçant γ par sa valeur $\dfrac{\sqrt{n} + g'}{g''}$, effectuant et égalant séparément les parties réelles et les imaginaires de l'égalité résultante,

$$(29) \qquad \mathrm{F}'g' + \mathrm{E}'g'' = \mathrm{F}n$$

$$(30) \qquad \mathrm{F}g' + \mathrm{E}g'' = \mathrm{F}' .$$

Multipliant (29) par F et (30) par F', puis retranchant, il viendra, en remarquant que, suivant la parité du nombre des termes a', a, b, ... f, on a $\mathrm{F}'\mathrm{E} - \mathrm{F}\mathrm{E}' = \pm 1$, la relation

$$(31) \qquad \mathrm{F}'^2 - n\mathrm{F}^2 = \pm g'' .$$

Ainsi l'équation $x^2 - ny^2 = \mathrm{N}$ est toujours résoluble, d'une infinité de manières, à l'aide des formules (η), (θ), (ι), $(\varkappa)$, (λ), (μ) et (ν), si N est l'un des nombres $-a''$, $+b''$, $-c''$, ...

Puisque l'un des nombres a'', b'', ... est égal à 1, l'équation $x^2 - ny^2 = \pm 1$ est toujours possible, en choisissant convena-

blement le signe : on posera en conséquence $x = G'$, $y = G$, $g = a'$ étant l'avant-dernier terme de la période. Si le nombre des termes de celle-ci est pair, il faut le signe + et les valeurs de x ne sont autres que les termes de la série

$$G' = (a', a \dots g), \quad G'_2 = (a' \dots g, h, a \dots g),$$

$$G'_3 = (a' \dots g, h, a \dots g, h, a \dots g), \dots$$

tandis que si les termes de la période sont en nombre impair, les termes de rang impair de cette série seront les valeurs de x dans $x^2 - ny^2 = -1$, et les termes de rang pair, les valeurs de x dans $x^2 - ny^2 = 1$. (Voir exercices n^{os} 30 à 35.)

13. — Désignons par D, D_2, D_3, ... et D'_1, D'_2, D'_3, ... les continuants

$$(a \dots c, d), \quad (a \dots c, d, e, f \dots a \dots d), \quad (a \dots d \dots d \dots d), \dots$$

et

$$(a', a \dots c, d), \quad (a', a \dots d \dots d), \quad (a' \dots d \dots d \dots d) \dots$$

correspondant au même quotient d. On a d'après (ι), en appelant P et Q les continuants $(e, f \dots a \dots c, d)$ et $(f \dots a \dots c, d)$,

$$(32) \qquad D_k = PD_{k-1} + QC_{k-1}, \qquad D'_k = PD'_{k-1} + QC'_{k-1}.$$

Les expressions D, D_2, D_3, ... peuvent donc se calculer par récurrence. On peut aussi les déduire des considérations suivantes : introduisons dans la relation

$$\sqrt{n} = \frac{D'_{k-1}\varepsilon + C_{k-1}}{D_{k-1}\varepsilon + C_{k-1}},$$

les valeurs de C_{k-1} et de C'_{k-1} tirées de (32), il viendra

$$(33) \qquad D'_k - D_k\sqrt{n} = (P - Q\varepsilon)(D'_{k-1} - D_{k-1}\sqrt{n}) ;$$

remplaçant ε par sa valeur $\dfrac{\sqrt{n} + e'}{e''}$, et séparant les parties réelles et les imaginaires, on aura deux égalités permettant de déduire D'_k et D_k de D'_{k-1} et D_{k-1}.

Cor. Dans le cas particulier où ces continuants correspondent à l'avant-dernier terme g de la période, ε devient $\eta = \sqrt{n} + a'$ et en outre on a :

$$P = (h, a \dots, g) = (2a', a \dots g) = 2a'G + (b \dots g) = a'G + G',$$

$$Q = (a \dots g) = G.$$

d'où

$$G'_k - G_k\sqrt{n} = (G' - G\sqrt{n})(G'_{k-1} - G_{k-1}\sqrt{n}) \tag{34}$$

et par suite

$$G'_k - G_k\sqrt{n} = G' - G\sqrt{n})^k \ . \tag{35}$$

D'après ce qui a été dit au n° **7**, cor. II, G′ est la plus petite valeur de x satisfaisant à l'équation de Fermat $x^2 - ny^2 = 1$, et G'_2, G'_3, ... les valeurs suivantes. On a ainsi tout à la fois une nouvelle démonstration de la possibilité de cette équation et le moyen d'en trouver les solutions.

(Voir exercices n^{os} 36 et 37.)

Exercices.

1. *On a :*

$$\left| a \ldots b, c \ldots \right| = \left| a \ldots b + \frac{1}{|c + \ldots|} \right| ;$$

$$|a + \alpha, b \ldots| = \alpha + |a, b \ldots| \ ; \quad |\ldots a, 0, b \ldots| = |\ldots a + b, \ldots| \ ;$$

$$|-a, b, c| = -|a-1, 1, b-1, c| \ ; \quad |a \ldots b| = |a \ldots b-1, 1| \ ;$$

$$|a, -b, c| = |a-1, 1, b-1, -c| = |a-1, 1, b-2, 1, c-1| \ ;$$

$$|-a_1 \ldots -a_k| = (-1)^k |a_1 \ldots a_k| \ ;$$

$$|a, b \ldots g, h|(b \ldots g, h) = |h, g \ldots b, a|(a, b \ldots g) \ ;$$

$$|a, b \ldots c| \times |b \ldots c| \times \ldots \times |c| = (a, b \ldots c) \ .$$

2. *Les réduites sont des fractions irréductibles.* Conséquence de (5).

3. *Les valeurs des réduites oscillent autour de celle de la fraction continue, en s'en rapprochant de plus en plus.* La première partie de ce théorème est une suite de la génération des fractions continues ; la seconde suit de ce que

$$\frac{(a \ldots h)}{(b \ldots h)} - \frac{(a \ldots g)}{(b \ldots g)} = \frac{\pm 1}{(b \ldots h)(b \ldots g)} \ .$$

Cor. I. *La différence de deux réduites consécutives diminue de plus en plus.*

II. *La valeur d'une fraction continue est plus près de la* k^e *réduite que de la* (k − 1)^e.

4. *Toute réduite approche plus de la valeur de la fraction continue qu'une fraction quelconque dont les termes sont plus petits.* Ces propositions entrevues par Wallis et Huygens, ont été démon-

trées par Saunderson, à qui est due la relation donnée à l'exercice 3.

5. *Les réduites correspondantes des développements en fractions continues de deux fractions irréductibles dont la somme est égale à l'unité, ont elles-mêmes une somme égale à l'unité* (Stouvenel).

6. *Soit* $\left| \text{a} \ldots \text{b}, \frac{c'}{c} \right| = \frac{A'}{A}$ *et* $\left| \text{a} \ldots \text{b}, \frac{d'}{d} \right| = \frac{B'}{B}$, *on aura :*

$$\frac{A' + B'}{A + B} = \left| a \ldots b, \frac{c' + d'}{c + d} \right| . \qquad \text{(Ed. Lucas.)}$$

7. *On a :*

$$\frac{(a, b, c, d, e \ldots h)}{(b, c, d, \ldots h)} = \frac{(a)}{1} + \frac{1}{(b)(b, c)} - \frac{1}{(b, c)(b, c, d)} + \frac{1}{(b, c, d)(b, c, d, e)} - \ldots \qquad \text{(Euler.)}$$

8. *Le nombre des termes du continuant de* k *lettres est égal au* k^e *terme de la série de Fibonacci* 1, 1, 2, 3, 5, 8, ... $u_{k+1} = u_k + u_{k-1}$ (Ed. Lucas).

9. *Si* (b ... h) = (a ... g), *la suite* a, b ... g, h *est symétrique, et réciproquement* (Legendre). En effet

$$\frac{(a, b \ldots g, h)}{(b \ldots g, h)} = | a \ldots h | \qquad \text{et} \qquad \frac{(a \ldots h)}{(a \ldots g)} = | h \ldots a | .$$

Si $(b \ldots h) = (a \ldots g)$, et dans ce cas seulement, $| a \ldots h | = | h \ldots a |$. Or une quantité donnée ne peut s'écrire que d'une seule manière en fraction continue.

10. *Démontrer la relation*

$$(a \ldots b, c, d \ldots e, f, g \ldots h)(d \ldots e) - (a \ldots e)(d \ldots h) = (-1)^t (a \ldots b)(g \ldots h)$$

t *désignant le nombre des quantités* d ... e. (Kramp.)

11. *Soit* $N = A + \frac{1}{\alpha}$, $\alpha = a + \frac{1}{\beta}$, $\beta = b + \frac{1}{\gamma}$, ... *on aura :*

$$N\alpha\beta \ldots \gamma\delta\varepsilon = (A, a, b \ldots c, d)\varepsilon + (A, a, b \ldots c) = (A, a, b \ldots c, d, \varepsilon) \qquad \text{(Lagrange.)}$$

12. *On a :*

$$(a, b \ldots c, d, d, c \ldots b, a)(b \ldots c, d, d, c \ldots b) = (a, b \ldots c, d, d, c \ldots b)^2 + 1 ,$$

d'où la décomposition du nombre A^2+1 *en deux facteurs, qui sont eux-mêmes des sommes de deux carrés* (Smith). On élève au carré les deux membres de l'égalité

$$(a \dots d)(b \dots c) - (a \dots c)(b \dots d) = \pm 1 ,$$

et on utilise la relation (13).

13. *Démontrer la relation*

$$(a \dots b, c, d \dots e, f, f, e \dots d)^2 + (a \dots b)^2$$
$$= [(a \dots b, c, d \dots e, f)^2 + (a \dots b, c, d, \dots e)^2][(d \dots e, f)^2 + (d \dots e)^2] .$$

Conséquence de (13) et de l'exercice n° 10.

14. Soient $\omega = \frac{a}{b}$, et x et y tels qu'on ait

$$0 < x - y\frac{a}{b} < \frac{1}{k} , \qquad \text{d'où} \qquad bx - ay < \frac{b}{k} ;$$

soit k l'entier immédiatement supérieur à $\sqrt{b}$. Comme $y < k$, on peut écrire $y^2 < b < k^2$, et de là

$$(bx - ay)^2 < \frac{b^2}{k^2} < b ,$$

$$(\xi) \qquad (bx - ay)^2 + hy^2 < b + hy^2 < (h+1)b .$$

Si donc $a^2 + h$ est multiple de b, il en est de même du premier membre de (ξ), et de plus il est positif à cause de sa forme : sa valeur est donc l'un des nombres b, $2b$, $3b$, ... hb.

Soit $h = 1$; on aura $(bx - ay)^2 + y^2 = b$, puisque le premier membre a une valeur inférieure à $2b$. Donc *tout diviseur de* a^2+1 *est lui-même une somme de deux carrés* (Fermat). Cette démonstration est due à Hermite.

Faisant $h = 2$, puis $h = 3$, on démontrera de même, avec Lebesgue, que le premier membre de (ξ) est égal à b et que, par suite, *les diviseurs de* a^2+2 *et de* a^2+3 *sont respectivement de la forme* x^2+2y^2 *et de la forme* x^2+3y^2 (Euler).

Cor. I. *L'égalité* $x^2+1 = ny^2$ *ne peut avoir lieu qu'autant que* n *est une somme de deux carrés* (Lagrange).

II. *Les équations* $x^2+2 = y^3$, $x^2+4 = y^3$ *ne sont susceptibles, la première, que de la solution* (5, 3) *et la seconde, que des solutions* (2, 2) *et* (11, 5) (Fermat). Démonstration d'Euler. 1° y est de la forme $\xi^2 + 2\eta^2$: on posera donc $x + \sqrt{-2} = (\xi + \eta\sqrt{-2})^3$, d'où $\eta(3\xi^2 - 2\eta^2) = 1$. Il n'y a que la solution possible $\xi = 1$, $\eta = 1$.

2° y est de la forme $\xi^2 + \eta^2$. On fera en conséquence $(x + 2\sqrt{-1}) = (\xi + \eta\sqrt{-1})^3$, d'où $\eta(3\xi^2 - \eta^2) = 2$, ce qui donne $\xi = \eta = 1$ ou $\xi = 1$, $\eta = 2$.

15. *Si un nombre* θ *peut se mettre sous la forme* $x^2 - ny^2$, *il le peut d'une infinité de manières.*

16. On a : $x_{2k} + y_{2k}\sqrt{n} = (x_k + y_k\sqrt{n})^2$, d'où $x_{2k} = x_k^2 + ny_k^2 = 2x_k^2 - 1$. Donc $2(2x_k + 1)$ *est un carré* (Ricalde).

17. $x_{2k+1} \pm 1$ *est divisible par* $x_1 \pm 1$, *et le quotient est un carré dans les deux cas* (Palmström).

18. *Equation* $x^2 - ny^2 = -1$. Elevons au carré les deux membres de cette équation ; il viendra

$$(x^2 + ny^2)^2 - n(2xy)^2 = 1 ,$$

d'où, en désignant par (a, b) une solution de $x^2 - ny^2 = 1$,

$$2(x^2 + ny^2) = (a + b\sqrt{n})^k + (a - b\sqrt{n})^k ,$$

$$2\sqrt{n}(2xy) = (a + b\sqrt{n})^k - (a - b\sqrt{n})^k ;$$

$$(x \pm y\sqrt{n})^2 = (a \pm b\sqrt{n})^k$$

ce qui donne

$$(a^2 - nb^2)^k = (x^2 - ny^2)^2 = 1 ;$$

les valeurs impaires de k fournissent donc les solutions de l'équation $x^2 - ny^2 = -1$, si elles existent (Lagrange).

Cor. I. Si (a', b') est la plus petite solution de $x^2 - ny^2 = -1$, la plus petite de $x^2 - ny^2 = 1$ est $a = 2a' + 1$, $b = 2a'b'$. Donc $x^2 + 1 = ny^2$ *a ou n'a pas de solutions selon que la plus petite valeur* a *est ou n'est pas de la forme* $\frac{1}{2}N^2 + 1$ (Realis).

Ainsi la plus petite valeur de a pour

$$n = 2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, \ldots$$

étant

$$a = 3, 2, 9, 5, 8, 3, 19, 10, 7, 648, 15, 4, 33, \ldots$$

l'équation $x^2 - ny^2 = -1$ est résoluble si $n = 2, 5, 10, 13, 17, \ldots$ auxquels cas correspondent les valeurs $a' = 7, 2, 3, 18, 4, \ldots$

II. On a :

$$(b^2k - a)^2 - (b^2k^2 - 2ak + n)b^2 = -1 .$$

Soit $a^2 - nb^2 = -1$. On pourra ainsi, connaissant une valeur de n conduisant à une solution, en trouver une infinité d'autres. La valeur $n = l^2 + 1$ est dans ce cas.

III. Soient $\alpha^2 - n\beta^2 = 1$ et $a^2 - nb^2 = \gamma$; les solutions de $x^2 - ny^2 = \gamma$ sont

$$x = a\alpha \pm nb\beta , \qquad y = \alpha b \pm \beta a ,$$

formules données par Brahmegupta et retrouvées par Euler.

19. Soit (a, b) la solution primitive de $x^2 - ny^2 = 1$. On aura $(a+1)(a-1) = nb^2$. Si n est un nombre premier, et qu'on fasse $b = fgh$, on aura l'une des relations

$$a + 1 = fg^2 n \qquad \text{et} \qquad a - 1 = fh^2 ,$$

ou bien

$$a + 1 = fg^2 \qquad \text{et} \qquad a - 1 = fh^2 n .$$

d'où

$$f(h^2 - ng^2) = -2 \qquad \text{ou} \qquad f(g^2 - nh^2) = 2 ;$$

f ne peut donc avoir que l'une des valeurs 1 ou 2 ; de là, quatre cas à examiner :

$$(o)\quad h^2 - ng^2 = -1 , \qquad (\pi)\quad g^2 - nh^2 = 1 ,$$

$$(\rho)\quad h^2 - ng^2 = -2 , \qquad (\sigma)\quad g^2 - nh^2 = 2 .$$

La supposition (π) est à écarter, car (a, b) ne serait pas la plus petite solution de l'équation proposée.

Si n est un nombre premier $4 + 1$, quelle que soit la parité de g et de h, les relations (ρ) et (σ) ne peuvent avoir lieu : la seule possible est donc (o), qui doit dès lors être toujours satisfaite, puisque $x^2 - ny^2$ admet toujours une solution.

Donc *si* n *est un nombre premier* $4 + 1$, *l'équation* $x^2 + 1 = ny^2$ *est toujours possible* (Legendre).

En outre on a une nouvelle preuve de cette proposition de Fermat : *tout nombre premier* $4 + 1$ *divise* $x^2 + 1$ (Id.).

Si n est de la forme $8 + 3$, (o) n'a pas lieu, d'après ce qui précède, et on démontrera aisément que (σ) non plus ne peut avoir lieu. La relation (ρ) est seule vraie dans ce cas, et on peut donc dire que *pour* n *premier de forme* $8 + 3$, *l'équation* $x^2 - ny^2 = -2$ *est possible* et, avec Euler, que n *divise un nombre de la forme* $x^2 + 2$ (Id.).

Si n est de la forme $8 - 1$, on démontrera, par des moyens semblables, que la relation (σ) est la seule possible. Donc, *dans ce cas, l'équation* $x^2 - ny^2 = 2$ *est toujours soluble* (Id.).

On trouvera d'autres théorèmes du même genre mais moins simples dans la *Th. des n.* de Legendre, ainsi que dans les *Werke* de Lejeune-Dirichlet.

20. Si (α, β) est la solution primitive de $x^2 - ny^2 = 1$ et qu'on ait

$$(\tau) \qquad f^2 - ng^2 = N ,$$

on aura cette autre solution de $x^2 - ny^2 = N$.

$$(\upsilon) \qquad (f\alpha - ng\beta)^2 - n(f\beta - g\alpha)^2 = N .$$

Si on remplace α et f par leurs valeurs $\sqrt{n\beta^2 + 1}$ et $\sqrt{ng^2 + N}$, on verra immédiatement que $f\alpha - ng\beta > 0$; donc la solution

donnée par (v) est en termes plus petits que ceux de (τ) si on a :

$$f\alpha - ng\beta < f\,, \qquad \text{d'où} \qquad (ng^2)(n\beta^2) < f^2(\alpha - 1)^2$$

et par suite

$$f > \sqrt{\frac{(\alpha+1)\mathrm{N}}{2}} \qquad \text{et} \qquad g > \sqrt{\frac{(\alpha-1)\mathrm{N}}{2n}}\,.$$

L'équation $x^2 - ny^2 = -\mathrm{N}$ peut s'écrire $(ny)^2 - nx^2 = n\mathrm{N}$; donc si (nf', g') est une solution de cette dernière équation, on en aura une autre en termes plus petits pour

$$nf' > \sqrt{\frac{(\alpha+1)n\mathrm{N}}{2}} \qquad \text{et} \qquad g' > \sqrt{\frac{(\alpha-1)n\mathrm{N}}{2n}}$$

ou bien

$$f' > \sqrt{\frac{(\alpha+1)\mathrm{N}}{2n}} \qquad \text{et} \qquad g' > \sqrt{\frac{(\alpha-1)\mathrm{N}}{2}}\,.$$

Ainsi, *α désignant la plus petite valeur de* x *satisfaisant à l'équation* $\mathrm{x}^2 - \mathrm{ny}^2 = 1$, *si l'équation* $\mathrm{x}^2 - \mathrm{ny}^2 = \pm\mathrm{N}$ *est possible, elle a des racines positives inférieures,* x *à* $\sqrt{\frac{(\alpha\pm1)\mathrm{N}}{2}}$ *et* y *à* $\sqrt{\frac{(\alpha\mp1)\mathrm{N}}{2n}}$.

Par exemple, pour $n = -2$, les limites sont $\sqrt{2\mathrm{N}}$ et $\sqrt{\frac{\mathrm{N}}{2}}$,

. . . . . -3, ... $\sqrt{\frac{3\mathrm{N}}{2}}$ et $\sqrt{\frac{\mathrm{N}}{6}}$,

. . . . -5, ... $\sqrt{5\mathrm{N}}$ et $\sqrt{\frac{4}{5}\mathrm{N}}$,

. . . . . .

(Tchebichef)

Cor. Soient (a, b) *et* (c, d) *deux solutions de* $\mathrm{x}^2 - \mathrm{ny}^2 = \mathrm{N}$, *on aura :*

$$(\varphi) \qquad (ac \pm nbd)^2 - n(ad \pm bc)^2 = \mathrm{N}^2\,;$$

et, si elles sont dans les conditions indiquées plus haut, N *est composé ;* en effet on a :

$$(\chi) \qquad ac \pm nbd < \frac{\alpha+1}{2}\mathrm{N} + \frac{\alpha-1}{2}\mathrm{N} = \alpha\mathrm{N}\,.$$

Si $ac \pm nbd$ était divisible par N, il en serait de même de $ad \pm bc$, d'après (φ), ce qui donnerait une solution de $x^2 - ny^2 = 1$, où la valeur de x serait $< \alpha$, d'après (χ), ce qui est contre l'hypothèse. Ainsi aucun des deux nombres $ad \pm bc$ n'est divisible par N. On démontrera de même, dans le cas de N négatif.

Or le produit de ces deux nombres est divisible par N, car il est égal à

$$a^2 d^2 - b^2 c^2 = \pm (d^2 - b^2) \mathrm{N} ,$$

et par conséquent on trouvera deux diviseurs de N en cherchant le p. g. c. d. de N et de chacun des deux nombres $ad \pm bc$ (Id.).

21. *Applications.* I. Les identités

$$(ba^2 \pm 1)^2 - b(ba \pm 2)a^2 = 1 , \qquad (2ba^2 \pm 1)^2 - b(ba^2 \pm 1)(2a)^2 = 1$$

donnent la solution du problème de Fermat dans un grand nombre de cas.

Soit $ax^2 - by^2 = 1$, il viendra $(2ax^2 - 1)^2 - ab(2xy)^2 = 1$. De là le moyen de trouver les solutions de $x^2 - aby^2 = 1$ quand on connaît celles de $ax^2 - by^2 = 1$.

Si $ax^2 - by^2 = 2$, on aura $(ax^2 - 1)^2 - ab(xy)^2 = 1$: conclusion analogue (Realis).

II. a *et* b *étant premiers entre eux, de même que* α *et* β, *si on peut écrire*

$$a^2 - nb^2 = \alpha^2 - n\beta^2 = \mathrm{N} ,$$

il s'ensuit la solution de l'équation de Fermat. En effet $a^2\alpha^2 - n^2 b^2 \beta^2$ est divisible par N ; un et un seul des deux nombres $a\alpha \pm nb\beta$ est divisible par N, car autrement leur somme $2a\alpha$ le serait ainsi que a ou α. Appelons P celui de ces deux nombres qui est divisible par N, et Q celui des deux nombres $b\alpha \pm a\beta$ qui a le même signe que P. On a :

$$(a\alpha \pm nb\beta)^2 - n(b\alpha \pm a\beta)^2 = \mathrm{N}^2 .$$

P étant divisible par N, il en est de même de Q, et il s'ensuit

$$\left(\frac{\mathrm{P}}{\mathrm{N}}\right)^2 - n\left(\frac{\mathrm{Q}}{\mathrm{N}}\right)^2 = 1 . \qquad \text{(Lejeune-Dirichlet)}$$

III. La considération du carré et du cube de $a \pm b\sqrt{n}$ conduit, par multiplication des deux couples d'expression ainsi obtenues, aux identités,

$$(a^2 + nb^2)^2 - n(2ab)^2 = (a^2 - nb^2)^2 ,$$

$$a^2(a^2 + 3b^2 n)^2 - b^2(3a^2 + b^2 n)^2 n = (a^2 - b^2 n)^3 ,$$

dont la première montre que si $a^2 - b^2 n = \pm 2$, $(a^2 \mp 1, ab)$ est une solution de $x^2 - ny^2 = 1$ (Lagrange) et que pour $a^2 - nb^2 = \pm 4$, $(a^2 \mp 2, ab)$ en est une de $x^2 - ny^2 = 4$ (Cayley).

Pour $a^2 - b^2 n = \pm 4$, la deuxième identité se ramène à une équation de Fermat (Lagrange). La supposition $a^2 - b^2 n = \pm 2$ fournit une solution de $x^2 - ny^2 = \pm 1$.

IV. *Soit à trouver les triangulaires qui sont en même temps des carrés* (Euler). On a : $x^2 + x = 2y^2$ ou $(2x + 1)^2 - 2(2y)^2 = 1$. On est ramené à l'équation $X^2 - 2Y^2 = 1$, dont les racines sont $X = 1, 3, 17, 99, 577, 3363, \ldots X_{n+1} = 6X_n - X_{n-1}$.

V. *Trouver les nombres dont les carrés diminués de l'unité donnent des triangulaires.* (Euler). Solution analogue.

VI. *Trouver deux nombres dont le produit, ajouté successivement à chacun d'eux, donne des carrés* (Diophante). Posons $y = x - \lambda$, $z - w = 1$, l'égalité $xy + x = z^2$ deviendra

$$4x^2 - 4(\lambda - 1)x = (\lambda + 1)^2 \qquad \text{d'où} \qquad 2x = \lambda + 1 \pm \sqrt{2\lambda^2 + 2}\ .$$

On est conduit à résoudre $2\lambda^2 + 2 = (2\mu)^2$ ou $\lambda^2 - 2\mu^2 = -1$.

VII. *Soit* r *l'excès de* x *sur le plus grand carré qui y est contenu. Déterminer* x *de manière : 1° que* rx *soit un carré ; 2° que* rx *surpasse également de* r *le plus grand carré qui y est contenu* (Brocard).

1° On a :

$$x - r = y^2\ , \qquad r(y^2 + r) = z^2\ .$$

Posant $z = rz'$, puis $y = ry'$, il vient $z'^2 - ry'^2 = 1$.

2° On a :

$$x - r = y^2\ , \qquad r(y^2 + r) = z^2 + r\ .$$

Posant $z = rz'$, il vient

$$(\psi) \qquad y^2 - rz'^2 = r + 1\ .$$

Si (a, b) est une solution de $x^2 - ry^2 = 1$, $(rb \pm a, a \pm b)$ en est une de (ψ). D'ailleurs z^2 est le plus grand carré contenu dans $r(y^2 + r)$, car autrement on aurait successivement

$$r > 2z\ , \qquad r^2 > 4(ry^2 + r^2 - r)\ , \qquad 3r + 4 > 4y^2\ ; \qquad \text{or} \qquad r < 2y\ .$$

22. Dans le second membre de l'identité

$$(\omega) \qquad \sqrt{n} = a' + \frac{a''}{\sqrt{n} + a'}$$

remplaçons $\sqrt{n}$ par le second membre lui-même ; puis, dans le résultat, $\sqrt{n}$ par le même second membre de (ω), etc. On aura une généralisation de fraction continue, dont les continuants se calculent à l'aide des formules

$$G' = 2a'F' + a''E'\ , \qquad G = 2a'F + a''E\ ,$$

et on a :

$$G'^2 - nG^2 = (-a'')^t\ ,$$

t désignant le rang de G dans la série des continuants A, B, ... G. Si on prend $n = a_1'^2 - a_1''$, on a les solutions de $x^2 - ny^2 = a''^t$, quelle que soit la parité de t (Landry).

23. *Les périodes correspondant aux nombres* a', ... ; a'', ... , *et* a, ... *provenant de la réduction en fraction continue des racines carrées des nombres*

$$a'^2 + 1 , \quad a'^2 + 2 , \quad a'^2 + a' , \quad a'^2 + 2a' - 1 , \quad a'^2 + 2a' ,$$

sont respectivement

a' ; a', a' ; a', a' ; a' , $a' - 1$, $a' - 1$, a' ; a', a' ;

1 ; 2 , 1 ; a', 1 ; $2a' - 1$, 2 , $2a' - 1$, 1 ; $2a'$, 1 ;

$2a'$; a', $2a'$; 2 , $2a'$; 1 , $a' - 1$, 1 , $2a'$; 1 , $2a'$;

En déduire les fractions continues représentant les racines carrées des nombres 2, 3, 5, 6, 7, 8, 10, 11, 12, 14, 15, 17, 18, 20, 23, 24, ...

24. *Etudier les nombres qui donnent les périodes*

a', a, $2a'$; a', a, a, $2a'$; a', a, b, a, $2a'$; a', a, b, b, a, $2a'$;

a', b, c, b, a, $2a'$; etc. (Euler)[1]

25. *Les termes de la série* 1, 5, 29, 169, 985, 5741, ... $u_{k+1} = 6u_k - u_{k-1}$ *provenant de la réduction de* $\sqrt{2}$ *en fraction continue, sont tous des sommes de deux carrés* (Ed. Lucas), *et sont les seuls nombres dont les carrés sont égaux à la somme de deux carrés consécutifs* (Welsch, *I. M.*, 1909, p. 17).

26. *On a* $\sqrt{5} + 1 = 2 \mid 1, 1, 1, \ldots \mid$; *les termes des diverses réduites ne sont autres que les nombres de la série de Fibonacci* (exercice n° 8), *lesquels représentent les continuants* (0), (1), (1, 1), (1, 1, 1), (1, 1, 1, 1), ...[2]

Le k^e *terme de cette série est égal à*

$$\frac{\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k}{\sqrt{5}} ,$$

d'où il suit que si k est un nombre quelque peu considérable, on a :

$$\frac{1{,}61803^k}{\sqrt{5}}$$

pour la valeur de ce k^e terme (Binet).

---

[1] Auparavant Saunderson avait étudié les cas $\mid 1, 2, 3; \ldots \mid$, $\mid 4, 1, 1, 1; \ldots \mid$, $\mid a; \ldots \mid$, $\mid a, b; \ldots \mid$, $\mid a, b; c, d, e; c, d, e; \ldots \mid$. C'est donc lui qui, le premier, a considéré les fractions continues en elles-mêmes.

[2] C'est une conséquence immédiate de ce même exercice n° 8.

27. *La période* (n° **9**) *a au plus* 2n *termes,* puisque $g' < \sqrt{n}$ et $g'' < 2\sqrt{n}$.

28. Des relations (18) et (21), on déduit la suivante

$$f'' + g' > \sqrt{n} > f'' - g'$$

ce qui ne peut avoir lieu que si g' est positif. Donc *tous les termes de la série du n° **8** sont positifs* (Lagrange).

29. *Si* $e'' = 1$, *on a :* $f' = a'$, $e = e' + a'$, $f'' = a''$, *et la suite se reproduit périodiquement.* Conséquence de (η), de (θ) et de (ι).

30. *Démontrer les relations*

$$\sqrt{n}\,\alpha\beta \ldots \varepsilon\varphi\gamma = G'\eta + F' , \qquad \alpha\beta \ldots \varepsilon\varphi\gamma\, G\eta + F$$

et tirer de là une autre démonstration de (28) (Lagrange).

31. D'après (η), $(\varkappa)$ et (λ) on peut écrire

$$\alpha'\beta = \ldots = \delta'\varepsilon = \varepsilon'\varphi = \varphi'\gamma = \gamma'\eta = \eta'\alpha = 1$$

d'où

$$\gamma' = -g + \frac{1}{\varphi'} , \quad \varphi' = -f + \frac{1}{\varepsilon'} , \ldots \beta' = -b + \frac{1}{\alpha'} , \quad \alpha' = -a + \frac{1}{\eta'} ,$$

et de là

$$\frac{\sqrt{n} - a'}{a''} = \frac{\sqrt{n} - h'}{g''} = \gamma' = |\, -g, -f, \ldots -b, -a, \eta' \,|$$

$$= -|\, g, f \ldots b, a, -\eta' \,| .$$

L'expression γ' se développe donc également en une fraction continue inverse de celle de $\sqrt{n}$ (Lagrange).

32. Supposons que dans la succession $\ldots j, k, l \ldots r, s, \ldots$ on ait $r' = l'$ et $r'' = k''$; d'après (θ) et (24), il viendra $r = k$; et en outre, comme on a :

$$k' + l' = kk'' , \qquad r' + s' = rr'' , \qquad j''k'' + k'^2 = r''s'' + s'^2 ,$$

il s'ensuit $s' = k'$, $s'' = j''$.

Mais $a' = h'$, $a'' = g''$; donc $b'' = f''$, $a = g$, $b' = g'$. Opérant de même sur les couples g', b' et f'', b'', il viendra $c'' = e''$, $b = f$, $c' = f'$, et ainsi de suite.

Les termes $a, b, c \ldots e, f, g$ de la période forment donc une *suite symétrique,* ainsi que les nombres $a', b' \ldots$ et $a'', b'' \ldots$

On peut donc écrire :

$$\sqrt{n} = |\, a', a, b, c \ldots c, b, a, 2a' ; a, b, c \ldots \,|$$

Cette forme du développement de $\sqrt{n}$ a été découverte par Euler, ainsi que les lois de ses termes. Elle a été démontrée par Lagrange. Elle montre que, dans une même période il y a au

moins deux solutions de l'équation $x^2 - ny^2 = \pm g''$, à moins que la période ne soit d'un nombre impair de termes et que g'' soit celui du milieu.

A titre de curiosité, voici la demi-période correspondant à $n = 991$, la plus longue pour $n < 1000$,

$$31, 2, 12, 10, 2, 2, 2, 1, 1, 2, 6, 1, 1, 1, 1, 3, 1, 8, 4, 1, 2, 1, 2,$$
$$3, 1, 4, 1, 20, 6, 4 ; 31 ; 4, 6 \ldots$$

ce qui donne, d'après Legendre,

$$x = 37951\ 64009\ 06811\ 93063\ 80148\ 96080 ,$$

pour la racine du plus petit carré qui soit de la forme $991y^2 + 1$.

33. Si la période $a, b \ldots d, e \ldots g, h$ contient un nombre pair de termes, et qu'on ait, par exemple, $d = e$, on aura aussi $d'' = e''$. Or on a en général $d''e'' + e'^2 = n$, ce qui donne, dans ce cas particulier, $e'^2 + d''^2 = n$: mais le nombre des termes $a, b \ldots g, h$ étant pair, l'équation $x^2 + 1 = ny^2$ est toujours résoluble. Donc, dans le même cas, le nombre n est la somme de deux carrés.

Mais l'équation est également résoluble dans le cas où n est un nombre premier $4 + 1$. De là, ce théorème de Fermat : *tout nombre premier* $4 + 1$ *est la somme de deux carrés,* et, en même temps, la décomposition de ce nombre en ses deux carrés (Legendre)[1].

On peut aussi conclure de la première partie de cette démonstration, que si n est un nombre premier $4 - 1$, la période a un nombre impair de termes.

34. D'après (8) on a :

$$(a', a \ldots b, c, d, c, b \ldots a) = CD' + BC' ,$$
$$(a \ldots b, c, d, c, b \ldots a) = C(B + D) ,$$
$$(a', a \ldots c, d, d, c \ldots a) = CC' + DD' ,$$
$$(a \ldots c, d, d, c \ldots a) = C^2 + D^2 .$$

De là le moyen de passer immédiatement du continuant de la demi-période à celui de la période entière, ce qui réduit de moitié le calcul de la solution du problème de Fermat (Van Aubel)[2].

---

[1] D'après certains manuscrits de Fermat retrouvés par Ed. Lucas, cette démonstration serait celle de cet illustre géomètre.

[2] Dans les deux premières formules, Van Aubel trouve, assez péniblement du reste,

$$\frac{n \cdot {}^2 + C'^2}{nC^2 - C'^2} \quad \text{et} \quad \frac{2CC'}{nC^2 - C'^2}$$

au lieu de $CD' + BC'$ et $C(B + D)$. On pourra s'exercer à vérifier l'identité de ces deux expressions. Il tire de ses formules l'idée de rechercher les solutions de l'équation $x^2 - ny^2 = 1$, en remarquant qu'elles reviennent à déterminer ω de telle manière que $n + \omega^2$ et 2ω soient divisibles par $n - \omega^2$, car les deux quotients représentent les valeurs de x et de y, ce qui conduit à déterminer de nombreuses valeurs de n pour lesquelles la solution est immédiate. (Voir *A. F.*, 1885, p. 137 et seq.)

35. *Posons*

$$\frac{G'_{kh}}{G_{kh}} = M_h \qquad \text{et} \qquad \frac{n}{M_h} = N_h \ ;$$

on aura :

$$2M_{2h} = M_h + N_h \qquad \text{et} \qquad N_{2h} = \frac{n}{M_h} \ .$$

Les valeurs des termes de la série M_h, N_h; M_{2h}, N_{2h}; M_{4h}, N_{4h}; ... telle que le premier terme de chaque couple est égal à la moyenne arithmétique des deux précédents, et le second, à leur moyenne harmonique, — *oscillent de part et d'autre de la valeur de la racine* $\sqrt{n}$, *dont elles se rapprochent de plus en plus* (Serret). Cette proposition a lieu pour M_h quelconque, et, sous cette forme, elle était connue des anciens ; la valeur de M_h donnée par Serret fournit une approximation très rapide de $\sqrt{n}$.

36. *Pour que la fraction* $\frac{N}{A}$, *développée en fraction continue, donne une suite symétrique, il faut et il suffit que le nombre* $\frac{A^2 \pm 1}{N}$ *soit entier*. En déduire la décomposition du nombre premier $4 + 1$ en deux carrés (Serret).

37. *Les conditions nécessaires et suffisantes pour que deux irrationnelles* ω *et* ω' *se développent en fractions continues ayant même période, sont qu'elles soient liées par des relations de la forme*

$$\omega' = \frac{A\omega + B}{a\omega + b} \ , \qquad Ab - aB = \pm 1 \ . \qquad \text{(Serret)}$$

38. On a différentes manières de représenter graphiquement les procédés de calcul des fractions continues et de l'équation de Fermat. On se contentera de signaler ici :

1° le moyen d'obtenir le quotient et le reste de la division de a par b, en portant, à l'aide d'un compas, la longueur b sur la longueur a, autant de fois que cela est possible ;

2° la solution, par Poinsot, de l'équation $ax - by = 1$, au moyen de la considération des sommets du b^{gone} (voir *Ent. math.*, 1907, p. 301) ;

3° l'emploi du papier quadrillé sur lequel on trace la droite $ax - by = c$ ou l'hyperbole $x^2 - ny^2 = 1$.

4° L'inscription à l'aide d'un compas, sur la même droite et à une même échelle, des longueurs $ax + b$, $a'x + b'$, ... ce qui permet de trouver immédiatement la solution des systèmes $ax + b = a'x + b' = \ldots$ On pourrait aussi employer des bandes de papier transparent contenant chacune une droite divisée de a en a, de a' en a', ...

39. Les substitutions $X = \alpha x + \beta y$ et $Y = \gamma x + \delta y$ qui rendent l'expression $AX^2 + 2BXY + CY^2$ identique à elle-même sont déterminées par une équation de la forme $t^2 - (B^2 - AC)u^2 = a^2$, a désignant le p. g. c. d. des nombres A, 2B et C.

Plus généralement, si ces mêmes substitutions donnent une formule identique à celle qu'amènent les substitutions $X = \alpha' x + \beta' y$, $Y = \gamma' x + \delta' y$, on a :

$$[A\alpha\alpha' + B(\alpha\gamma' + \alpha'\gamma) + C\gamma\gamma']^2 - (B^2 - AC)(\alpha'\gamma - \alpha\gamma')^2 = a^2 .$$

et plusieurs autres relations de la même forme.

C'est par des considérations de ce genre que Gauss a trouvé sa solution de l'équation $t^2 - nu^2 = a^2$, au moyen de la théorie des formes binaires quadratiques, théorie où elle est de première importance.

40. *Si* n *est un nombre premier* $4 - 1$, *les termes moyens* d'' *et* d' *de la période sont égaux, le premier à* 2 *et le second à la racine du plus grand carré impair contenu dans* n. (Picou ; voir *I. M.*, 1900, p. 302.)

41. *Si* $x^2 - ny^2 = M$, $\frac{x}{y}$ *est une des réduites du développement de* $\sqrt{n}$ *en fraction continue* (Lagrange).

42. *Etendre les théorèmes* n^{os} **8** *à* **13** *au développement en fraction continue des racines de l'équation* $Ax^2 + 2Bx + C = 0$ (Lagrange). Voir par exemple, Legendre, *Th. des n.* ou les traités d'algèbre supérieure de Serret ou de Weber.

On lira aussi avec grand fruit la résolution de l'équation de Fermat en nombres complexes par Lejeune-Dirichlet (Werke, t. I, p. 570).

Pour la théorie des fractions continues généralisées, voir *l'Encycl. math.*, t. I, vol. I, p. 282.

A. Aubry (Dijon).