Det Kgl. Danske Videnskabernes Selskab.
Mathematisk-fysiske Meddelelser. **IV**, 1.

RECHERCHES
SUR
L'ÉQUATION DE FERMAT

PAR

NIELS NIELSEN

KØBENHAVN
HOVEDKOMMISSIONÆR: ANDR. FRED. HØST & SØN, KGL. HOF-BOGHANDEL
BIANCO LUNOS BOGTRYKKERI
1922

INTRODUCTION

FERMAT[1], dans une lettre de février 1657, adressée à Frenicle, a énoncé le théorème:

Soit a un positif entier, sans être un carré, il existe une infinité de nombres entiers y pour lesquels l'expression

$$(1) \qquad ay^2 + 1$$

devient un carré.

On voit immédiatement que ce théorème n'est autre chose que celui-ci:

Soit a un positif entier, sans être un carré, l'équation indéterminée du second degré

$$(2) \qquad x^2 - ay^2 = 1$$

admet une infinité de solutions en positifs entiers.

Peu de temps après l'énonciation du problème susdit, lord WILLIAM BROUNCKER en a donné une résolution que JOHN WALLIS[2] a rédigée et publiée le premier, tandis que JOHN PELL l'a fait réimprimer dans une autre publication.[3] Voilà le seul mérite qu'ait acquis PELL dans la théorie de l'équation (2).

[1] Varia opera mathematica, p. 190; Toulouse 1679. Œuvres, t. II, p. 333—334.

[2] Commercium epistolicum; Londres 1658.

[3] RHONIUS: Algebra translated by TH. BRANKER, much altered and augmented; Londres 1668.

Néanmoins, EULER[1] dit, comme introduction à son aperçu de la résolution de l'équation susdite, due à BROUNCKER:

»Hierzu hat vormals ein gelehrter Engländer, Namens Pell, eine ganz sinnreiche Methode erfunden, welche wir hier erklären wollen.«

Bien que cette remarque soit parfaitement denuée de fondement, l'autorité suprême d'EULER a néanmoins rattaché le nom de PELL à l'équation (2), proposée par FERMAT[2], dans la solution de laquelle il n'a acquis aucun mérite, comme le dit très justement WERTHEIM[3]:

»Sie [l'équation de Fermat] wird jetzt meist noch nach dem Engländer John Pell benannt, durchaus mit Unrecht, da dieser sich nicht das geringste Verdienst um dieselbe erworben hat.«

Malheureusement, la remarque de WERTHEIM n'est que trop vraie, on attribue encore, le plus souvent, à PELL l'équation de FERMAT. On lit par exemple dans les Cours de LEJEUNE DIRICHLET[4]:

»Fermat hat diese Gleichung den Mathematikern zuerst vorgelegt, worauf ihre Lösung von dem Engländer Pell angegeben wurde.«

A cet égard une page d'un volume du *Jahrbuch über die Fortschritte der Mathematik*[5] est très curieuse. En effet, on lit, dans un article: »Geschichte der Fermatschen (so-

[1] Leonhard Eulers vollständige Anleitung zur niederen und höheren Algebra nach der französischen Ausgabe des Herrn DE LA GRANGE mit Anmerkungen und Zusätzen herausgegeben von JOHANN PHILIPP GRÜSON, t. II, p. 242; Berlin 1797.

[2] Voir G. WERTHEIM: Anfangsgründe der Zahlenlehre, p. 402; Brunswick 1902.

[3] Ibid. p. 220.

[4] Vorlesungen über Zahlentheorie, herausgegeben und mit Zusätzen versehen von R. DEDEKIND, 3e édition, p. 200; Brunswick 1879.

[5] Tome 32 (1901), p. 195.

genannte Pellschen) Gleichung«. Et, dans l'article suivant, un autre collaborateur dit tout bonnement: »Lösungen der Pellschen Gleichung.«

Or, ce maintien opiniâtre du faux nom d'équation de PELL me semble un peu choquant, dans ce Journal si méritant, parce qu'on lit, dans le volume qui précède celui que nous venons de citer:[1]

»Die Gleichung $t^2 - Du^2 = 1$ pflegt noch jetzt die Pell'sche genannt zu werden, obgleich seit langer Zeit feststeht, dass sie sich schon bei Fermat findet, einfach weil der ihr von Euler gegebene Name »Pell'sche Gleichung« sich einmal eingebürgert hat.«

Mais, après cette petite réclamation, résultat peut-être de la publication du livre de M. H. KONEN,[2] on ne voit plus, que je sache, dans le *Jahrbuch*, le vrai nom d'équation de FERMAT; on applique, au contraire, exclusivement le faux nom d'équation de PELL.

Si un tel exemple de persistance dans l'erreur est donné par un périodique que tout le monde consulte, je ne me flatte pas de pouvoir détourner mes confrères les mathématiciens du chemin battu qu'il suivent en employant l'appellation incorrecte d'équation de PELL, parce que ce nom s'autorise de la remarque erronée d'EULER. Cependant il m'est impossible de passer sous silence, dans l'Introduction de mon Mémoire sur l'équation de FERMAT, cette bévue historique, parce qu'il s'agit ici d'un des plus grands géomètres de tous les siècles.

A ce propos il faut citer encore une remarque de feu M. BACHMANN[3]:

[1] Tome 31 (1900), p. 189.

[2] Geschichte der Gleichung $t^2 - Du^2 = 1$; Leipsic 1901. (Citation d'après WERTHEIM: Anfangsgründe der Zahlenlehre, p. 220.)

[3] Niedere Zahlentheorie, t. II, p. 76; Leipsic 1910.

»E. Lucas hat diese Reihen [savoir les deux suites dont les éléments sont les nombres $B_n(2)$ et $2A_n(2)$] als Pellsche Reihen bezeichnet, um das Verdienst zu ehren, welches Pell um die Auflösung der sogenannten Pellschen Gleichung zukomme; gegenwärtig weiss man aber, das dies Verdienst gar nicht nachweisbar ist.«

La résolution générale et rigoureuse de l'équation de Fermat est due à l'illustre Lagrange[1] qui a inventé une méthode ingénieuse, en appliquant la fraction continue, infinie et périodique, qui représente $\sqrt{a}$.

En effet, cette méthode de Lagrange donne à la fois toutes les solutions possibles en positifs entiers de l'équation susdite, et une démonstration aussi élégante que facile des propriétés remarquables de la fraction continue en question, propriétés qui ont été connues par Euler, mais que ce grand géomètre n'a pas pu démontrer.

De plus, la méthode de Lagrange donne non seulement la résolution complète de l'équation de Fermat, mais aussi de cette autre

$$x^2 - ay^2 = -1, \tag{3}$$

pourvu que cette équation soit résoluble en positifs entiers.

Or, en donnant sa méthode remarquable pour résoudre aussi l'équation (3), jusque-là restée inaperçue,[2] Lagrange a présenté aux mathématiciens un problème très difficile, savoir de donner la condition suffisante et nécessaire qui doit être remplie par le nombre a, afin que l'équation (3) soit résoluble en positifs entiers.

A cet égard, Legendre[3] a donné la règle très simple:

[1] Miscellanea Taurinensia, t. 4, p. 41—47; 1766—69. Mémoires de l'Académie de Berlin 1767, p. 165—230 (1769).

[2] Euler dans son Algebra t. II, p. 247—248, donne la résolution de l'équation (2) pour $a = 13$, sans s'arrêter à l'équation (3) correspondante.

[3] Théorie des Nombres, t. I, p. 64—71.

L'équation (3) est toujours résoluble en positifs entiers, pourvu que a soit un nombre premier de la forme $4\nu + 1$.

Or, a étant diviseur de la somme $x^2 + 1$, il est évident que ce nombre ne peut contenir aucun facteur premier de la forme $4\nu + 3$.

Lejeune Dirichlet[1] a étudié le cas où a est le produit de deux ou trois nombres premiers de la forme $4\nu + 1$, mais ses belles recherches ne donnent pas, ce me semble, des résultats faciles à appliquer.

Parmi les geomètres qui ont, plus tard, étudié le problème difficile concernant la nature du nombre a qui figure dans l'équation (3), nous citons MM. J. Perott[2], F. Tano[3], E. de Jonquières[4], mais les résultats obtenus par eux me semblent, d'un point de vue général, peu satisfaisants.

C'est ce que Wertheim[5] dit très modestement:

»Trotz der Bemühungen von Legendre, Lejeune Dirichlet u. a. ist est noch nicht vollständig gelungen, die Bedingungen für die Lösbarkeit der Gleichung $x^2 - Ay^2 = -1$ anzugeben.«

Quant à cette équation difficile, on lit dans le *Jahrbuch über die Fortschritte der Mathematik*[6]:

»Das Problem der Angabe aller Determinanten D, für welche $t^2 - Du^2 = -1$ in ganzen Zahlen t, u lösbar ist, scheint sehr schwierig zu sein.«

Pour ma part, je crois que ce problème est aussi difficile

[1] Abhandlungen der Berliner Akademie 1834, p. 649—664. Werke, t. I, p. 221—236.

[2] Journal de Crelle, t. 102, p. 185—223; 1887.

[3] Ibid. t. 105, p. 160—169; 1889.

[4] Comptes rendus, t. 126, p. 1837—1843; 1898.

[5] Anfangsgründe der Zahlenlehre, p. 225; Brunswick 1902.

[6] Tome 29 (1898), p. 174.

que la détermination générale de l'exposant ε qui figure dans la congruence, également due à Lagrange[1],

$$\frac{p-1}{2}! \equiv (-1)^{\varepsilon} \pmod{p},$$

où p est un nombre premier de la forme $4\nu + 3$.

On sait, du reste, que Lejeune Dirichlet[2] a remarqué que l'exposant ε est égal au nombre des non-résidus quadratiques de p, contenus dans l'ensemble

$$1,\ 2,\ 3,\ \ldots,\ \frac{p-1}{2}.$$

Quant à l'équation (3), Wertheim[3] remarque que, parmi les 90 valeurs de a plus petites que 100, 20 seulement donnent des solutions en positifs entiers de l'équation susdite.

Euler[4] a donné une table des plus petites valeurs de x et y qui satisfont à l'équation (2), où a représente les 90 valeurs possibles, plus petites que 100, tandis que le professeur danois C.-F. Degen[5] a étendu cette table jusqu'à $a = 1000$.

De plus, Euler[6] a donné une table des fractions continues qui représentent $\sqrt{a}$, de $a = 2$ jusqu'à $a = 120$, table que M. A.-S. Werebrusoff[7] a récemment étendue jusqu'à $a = 1000$.

Quant au présent Mémoire, il donne une partie des résultats que j'ai obtenus dans mes recherches pendant les dernières treize années, recherches qui ont été inspirées par

[1] Nouveaux Mémoires de Berlin, t. 2 (1771), p. 131; 1773.
[2] Journal de Crelle, t. 3, p. 407—408; 1828. Werke, t. I, p. 105—108.
[3] Anfangsgründe der Zahlenlehre, p. 225; Brunswick 1902.
[4] Algebra, t. II, p. 252—253; Berlin 1797.
[5] Canon Pellianus; Copenhague 1817.
[6] Novi Commentarii Academiæ Petropolitanæ, t. 11, p. 39—45.
[7] Jahrbuch über die Fortschritte der Mathematik t. 35 (1904), p. 232.

le fameux postulat de M. E. de Jonquières[1], savoir que $x = 1$ et $x = 5$ sont les seuls nombres qui satisfont aux deux conditions

$$x = y^2 + (y + 1)^2, \quad x^2 = z^2 + (z + 1)^2,$$

postulat que l'on n'a pas encore réussi à démontrer rigoureusement, que je sache.

Quant aux nombres A_n et B_n, déterminés par une équation de Fermat

$$A_n^2 - aB_n^2 = (-1)^{nk}, \quad n = 1, 2, 3, \ldots,$$

ils possèdent beaucoup de propriétés remarquables. Nous nous bornerons à indiquer ici que ces nombres A_n et B_n, parfaitement déterminés à l'aide du nombre a, forment un groupe de nombres bien limité.

En effet, il est possible de former des A_n et des B_n tant une Théorie des Nombres, concernant la théorie du plus grand commun diviseur et du plus petit commun multiple, qu'une Trigonométrie élémentaire, ayant ses formules d'addition et logarithmiques. De plus, soit p un positif entier donné, quelconque du reste, il existe un indice r, tel que les B_{nr}, où n est un positif entier quelconque, représentent l'ensemble des nombres B_m qui sont divisibles par p, ce qui est essentiel dans plusieurs recherches.

Quant aux résultats que j'ai obtenus, je me suis efforcé d'annoter ceux que j'ai trouvés dans la littérature et d'insérer dans mon texte systématiquement des résultats déjà connus, souvent trouvés par hasard et sans des points de vue généraux, bien que plusieurs de ces résultats soient des conséquences immédiates des propriétés des nombres A_n et B_n susdits. Or, ce travail a été assez difficile et fatigant, parce que la

[1] Nouvelles Annales (2) t. 17, pp. 241—247, 289—310; 1878.

littérature sur l'équation de FERMAT est très eparse, et que plusieurs des publications en question ne se trouvent pas dans nos bibliothèques.

De plus, le *Jahrbuch über die Fortschritte der Mathematik* qui m'a été très utile, dans d'autres occasions, et principalement par les excellents comptes rendus de M. A. WANGERIN, me semble un guide moins sûr en ce qui concerne l'équation de FERMAT. Cela se comprend, du reste, car plusieurs des travaux dont il s'agit ici sont simplement insupportables, à cause de leur dilettantisme.

C'est pourquoi je demande l'indulgence de mes lecteurs, si mes citations ne sont pas toujours suffisamment épuisantes.

J'ajouterai qu'une étude plus approfondie de la littérature sur l'équation de FERMAT m'a causé plusieurs étonnements, principalement parce que je n'y ai trouvé aucune mention de trois faits très curieux, savoir:

1° L'abréviation considérable des calculs nécessaires pour la détermination des nombres A_1 et B_1, savoir des plus petites solutions de l'équation de FERMAT dont il s'agit, bien que ces abréviations soient simplement les conséquences des propriétés d'une fraction continue symétrique.

C'est pourquoi j'ai donné, dans le Chapitre Premier, un aperçu des formules fondamentales en question.

2° La méthode de BROUNCKER n'est autre chose qu'un établissement heuristique de la fraction continue de LAGRANGE; du point de vue pratique la méthode de BROUNCKER est énormément compliquée, du point de vue théorique elle est très difficile, parce qu'elle exige la connaissance des nombres ω_r et p_r, nombres qui donnent, du reste, des éclaircissements intéressants sur la fraction continue dont il s'agit.

3° Les solutions générales d'une équation quelconque de FERMAT ne sont autre chose que les polynomes de CAUCHY, pris des nombres A_1 et B_1, ce qui met en pleine lumière l'analogie frappante qui existe entre les formules récursives de LAGRANGE et les formules fondamentales de la Trigonométrie élémentaire.

Copenhague, le 21 octobre 1921.

NIELS NIELSEN.

CHAPITRE PREMIER

La fraction continue de Lagrange.

I. Remarques sur le problème général.

Soit a un positif entier, qui n'est pas un carré, Lagrange[1] a démontré l'existence d'un développement en fraction continue, infinie et périodique, de la forme

$$\sqrt{a} = \alpha + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \ddots + \cfrac{1}{\alpha_{k-1} + \cfrac{1}{2\alpha + \cfrac{1}{\alpha_1 + \ddots}}}}},$$

savoir, sous forme symbolique

$$\sqrt{a} = \left[\alpha, (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{k-1}, 2\alpha)\right], \tag{1}$$

où particulièrement

$$\sqrt{a} = \left[\alpha, (2\alpha)\right]. \tag{1 bis}$$

Dans ces deux formules, α et les α_r sont des positifs entiers, tels que

$$\alpha_r = \alpha_{k-r}, \qquad 1 \leq r \leq k-1. \tag{2}$$

Désignons ensuite par

[1] Miscellanea Taurinensia, t. 4, p. 41—47; 1766—1769. Mémoires de l'Académie de Berlin 1767, p. 165—230 (1769).

$$(3) \qquad \frac{y_0}{z_0},\ \frac{y_1}{z_1},\ \frac{y_2}{z_2},\ \ldots,\ \frac{y_{nk-2}}{z_{nk-2}},\ \frac{y_{nk-1}}{z_{nk-1}},\ \ldots,$$

où n est un positif entier quelconque, les réduites de la fraction continue susdite, LAGRANGE a aussi démontré que les nombres

$$(4) \qquad A_n = y_{nk-1},\ B_n = z_{nk-1}$$

représentent l'ensemble des solutions en positifs entiers de l'équation indéterminée du second degré

$$(5) \qquad x^2 - ay^2 = \pm 1,$$

proposée, en 1657, par FERMAT[1], de sorte que l'on aura, quel que soit l'indice n,

$$(6) \qquad A_n^2 - aB_n^2 = (-1)^{nk}.$$

Cela posé, il est évident que l'équation indéterminée

$$(7) \qquad x^2 - ay^2 = -1$$

n'est, pour k pair, jamais résoluble en positifs entiers.

Dans ce qui suit, nous désignons pour abréger a comme la base de l'équation indéterminée (5), k comme le nombre caractéristique de cette base. De plus, nous disons que a est une base de première ou de seconde espèce, selon que son nombre caractéristique k est impair ou pair, savoir selon que l'équation indéterminée (7) est résoluble en positifs entiers ou non. Enfin nous écrivons $A_n(a)$ et $B_n(a)$ au lieu de A_n et B_n, dans les cas où il s'agit, en même temps, de plusieurs bases différentes.

Soit maintenant p un positif entier quelconque, l'équation de FERMAT

$$(8) \qquad x^2 - ap^2y^2 = 1,$$

[1] Varia opera mathematica, p. 190; Toulouse 1679. Œuvres, t. II, p. 333—334.

de la base ap^2, admet aussi une infinité de solutions en positifs entiers. Or, l'équation (8) n'étant autre chose que celle-ci

$$x^2 - a(py)^2 = 1, \tag{8 bis}$$

il est évident qu'une infinité des nombres B_n, définis par la seconde des formules (4), sont divisibles par le positif entier p, problème que nous avons à étudier plus amplement dans l'article X.

Soit ensuite a une expression fractionnaire irréductible, savoir

$$a = \frac{b}{c_1 c_2^2}, \tag{9}$$

où c_1 est sans facteurs quadratiques, il existe, aussi dans ce cas, un développement en fraction continue, infinie et périodique, de la forme (1), et l'on aura de même

$$y_{nk-1}^2 - \frac{b}{c_1 c_2^2} z_{nk-1}^2 = (-1)^{nk}; \tag{10}$$

c'est-à-dire que z_{nk-1} est, quel que soit l'indice n, divisible par $c_1 c_2$. Posons

$$y_{nk-1} = \eta_n, \quad z_{nk-1} = c_1 c_2 \xi_n, \tag{11}$$

il résulte donc, en vertu de (10),

$$\eta_n^2 - bc_1 \xi_n^2 = (-1)^{nk}, \tag{12}$$

et, dans cette équation, bc_1 est un positif entier. Appliquons encore la remarque faite concernant les équations (8), nous avons démontré le théorème:

I. Afin de résoudre, en positifs entiers, l'équation indéterminée

$$x^2 - ay^2 = \pm 1, \tag{13}$$

où la base a est un nombre rationnel plus grand que l'unité, il suffit de résoudre une équation de la même forme, où la base a est un positif entier sans facteurs quadratiques.

Or, il existe, dans l'équation (13), des positifs entiers a, sans facteurs quadratiques, qui ne sont premiers à aucune des valeurs de y.

On voit par exemple que le nombre 6 est une base de seconde espèce, parce que le nombre premier 3 ne peut pas diviser la somme $x^2 + 1$.

De plus, dans l'équation de FERMAT correspondante

$$x^2 - 6y^2 = 1, \tag{14}$$

x étant nécessairement un nombre impair, $x^2 - 1$ est toujours de la forme 8ν; c'est-à-dire que y est un nombre pair, de sorte que l'équation (14) est la même que celle-ci

$$x^2 - 24y^2 = 1. \tag{14 bis}$$

Soit, comme second exemple de ce genre, n et p des positifs entiers quelconques, l'équation de FERMAT

$$x^2 - (n^{2p} - 2)\, y^2 = 1, \quad n > 1, \tag{15}$$

est satisfaite par

$$x = A_1 = n^{2p} - 1, \quad y = B_1 = n^p, \tag{15 bis}$$

et il résulte, en vertu du théorème I de l'article VII, que tous les B_n sont divisibles par n^p.

Quant aux valeurs fractionnaires de a, on aura par exemple, en supposant $\alpha > 1$,

$$\sqrt{\frac{\alpha + 1}{\alpha}} = \left[1, (2\alpha, 2)\right], \tag{16}$$

et l'équation de FERMAT correspondante, savoir

$$x^2 - \frac{\alpha + 1}{\alpha}\, y^2 = 1, \tag{17}$$

est résolue à l'aide des positifs entiers qui satisfont à celle-ci

$$x^2 - (\alpha^2 + \alpha)\, y^2 = 1. \tag{18}$$

Remarquons, en passant, que nous aurons

$$\sqrt{\alpha^2 + \alpha} = \left[\alpha,\ (2,\ 2\alpha)\right], \tag{19}$$

mais que la relation curieuse entre les périodes des deux fractions continues (16) et (19) ne correspond à aucune loi générale.

Enfin, nous avons à remarquer que nous désignons, dans ce qui suit, comme solution triviale de l'équation de Fermat

$$x^2 - ay^2 = \pm 1,$$

les valeurs

$$x = A_0 = 1, \quad y = B_0 = 0, \tag{20}$$

valeurs qui correspondent, en effet, à l'hypothèse $n = 0$.

II. Des réduites de la fraction continue.

Revenons maintenant à la fraction continue de Lagrange, écrite sous la forme

$$\sqrt{a} = \left[\alpha,\ (\alpha_1,\ \alpha_2,\ \alpha_3,\ \ldots,\ \alpha_{nk-1},\ 2\alpha)\right], \tag{1}$$

où n est un positif entier quelconque, nous avons tout d'abord à étudier plus amplement ses réduites

$$\frac{y_0}{z_0},\ \frac{y_1}{z_1},\ \frac{y_2}{z_2},\ \ldots,\ \frac{y_{nk-2}}{z_{nk-2}},\ \frac{y_{nk-1}}{z_{nk-1}},\ \ldots \tag{2}$$

A cet égard, nous introduisons la fraction continue, finie et symétrique,

$$K = (\alpha,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \ldots,\ \alpha_{nk-1},\ \alpha), \tag{3}$$

dont les nk premières réduites coïncident avec les nk premiers des nombres (2), tandis que la dernière réduite de K se présente sous la forme

$$\frac{M}{N} = \frac{\alpha y_{nk-1} + y_{nk-2}}{\alpha z_{nk-1} + z_{nk-2}}, \tag{4}$$

ce qui donnera

$$y_{nk-1} = N = \alpha z_{nk-1} + z_{nk-2},$$

car la fraction continue K est symétrique.

Posons ensuite

$$\left\{\begin{aligned} A_n &= y_{nk-1}, & B_n &= z_{nk-1} \\ a_n &= y_{nk-2}, & b_n &= z_{nk-2}, \end{aligned}\right. \tag{5}$$

il résulte la formule générale

$$A_n = \alpha B_n + b_n, \tag{6}$$

et le numérateur M de la réduite (4) se présente sous la forme $\quad M = \alpha A_n + a_n;$

c'est-à-dire que la formule

$$M z_{nk-1} - N y_{nk-1} = (-1)^{nk-1}$$

donnera $\quad (\alpha A_n + a_n) B_n - A_n^2 = (-1)^{nk-1},$

de sorte que nous aurons la formule, analogue à (6),

$$a B_n = \alpha A_n + a_n. \tag{7}$$

Cela posé, nous avons à déterminer la réduite à l'indice nk de la suite (2); il résulte, en vertu de (5) et (6),

$$\begin{aligned} y_{nk} &= 2\alpha A_n + a_n = \alpha A_n + a B_n \\ z_{nk} &= 2\alpha B_n + b_n = \alpha B_n + A_n, \end{aligned}$$

ou, ce qui est la même chose,

$$\begin{aligned} y_{nk} &= A_n y_0 + a B_n z_0 \\ z_{nk} &= B_n y_0 + A_n z_0, \end{aligned}$$

et la conclusion de m à $m+1$ donnera immédiatement les formules générales

$$(8) \quad \begin{cases} y_{nk+r} = A_n y_r + a B_n z_r \\ z_{nk+r} = B_n y_r + A_n z_r, \end{cases}$$

essentielles dans la théorie de l'équation de FERMAT.

Résolvons, par rapport aux nombres y_r et z_r, les équations (8), il résulte les formules inverses

$$(8 \text{ bis}) \quad \begin{cases} y_r = (-1)^{nk} (A_n y_{nk+r} - a B_n z_{nk+r}) \\ z_r = (-1)^{nk} (A_n z_{nk+r} - B_n y_{nk+r}). \end{cases}$$

Posons ensuite, quel que soit l'indice r,

$$(9) \qquad y_r^2 - a z_r^2 = (-1)^{r-1} \omega_r,$$

il est évident que les ω_r sont des positifs entiers, parce que la suite (2) a la valeur limite $\sqrt{a}$. Soit particulièrement, dans (9), $r = nk - 1$, on aura toujours, quel que soit n,

$$\omega_{nk-1} = 1,$$

formule qui n'est qu'un cas particulier du théorème general:

I. Les positifs entiers ω_r, définis par la formule (9), sont périodiques, parce que nous aurons, quel que soit n,

$$(10) \qquad \omega_{nk+r} = \omega_r.$$

En effet, on aura, en vertu de (8),

$$y_{nk+r}^2 - a z_{nk+r}^2 = (A_n^2 - a B_n^2)(y_r^2 - a z_r^2),$$

ce qui n'est autre chose que la formule (10).

Dans l'article qui suit, nous avons à démontrer une autre propriété fondamentale des nombres ω_r que nous aurons, du reste, à étudier plus amplement dans les articles IV, VI, XXVI.

Déterminons par exemple les valeurs ω_{nk}, nous prenons pour point de départ les valeurs

$$y_0 = \alpha, \ z_0 = 1,$$

ce qui donnera immédiatement

(11) $$\omega_{nk} = \omega_0 = a - \alpha^2,$$

ou, ce qui est la même chose,

(11 bis) $$y_{nk}^2 - a z_{nk}^2 = (-1)^{nk} (\alpha^2 - a).$$

Étudions encore les nombres $a_n = y_{nk-2}$ et $b_n = z_{nk-2}$, nous aurons, en vertu des formules (6) et (7),

(12) $$A_n = \frac{ab_n - a_n}{a - \alpha^2}, \quad B_n = \frac{a_n - \alpha b_n}{a - \alpha^2},$$

et il résulte

(13) $$a_n^2 - ab_n^2 = (-1)^{nk} (\alpha^2 - a),$$

ce qui donnera la congruence

(14) $$a_n^2 \equiv (-1)^{nk} \alpha^2 \pmod{a},$$

que nous avons à appliquer dans l'article VIII, où nous nous bornerons à l'étude des nombres $a_n = y_{nk-2}$, bien que les y_{nk} satisfassent à la même congruence.

Soit maintenant $k = 2$, la fraction continue

(15) $$\sqrt{a} = [\alpha, (\beta, 2\alpha)] = \sqrt{\alpha^2 + \frac{2\alpha}{\beta}},$$

où 2α est supposé divisible par β, est parmi celles que P. Seeling[1] à étudiées. Dans ce cas, nous n'avons qu'à déterminer le seul nombre ω_0, et nous aurons donc

(16) $$y_{2n+1}^2 - \left(\alpha^2 + \frac{2\alpha}{\beta}\right) z_{2n+1}^2 = 1$$

(17) $$y_{2n}^2 - \left(\alpha^2 + \frac{2\alpha}{\beta}\right) z_{2n}^2 = -\frac{2\alpha}{\beta},$$

formules qui sont valables, quel que soit n.

[1] Archiv de Grunert, t. 49, p. 4—44; 1868.

Appliquons ensuite les formules récursives

$$y_{2n+1} = \beta y_{2n} + y_{2n-1}, \qquad z_{2n+1} = \beta z_{2n} + z_{2n-1}$$
$$y_{2n} = \alpha y_{2n-1} + y_{2n-2}, \qquad z_{2n} = \alpha z_{2n-1} + z_{2n-2},$$

il résulte, après un simple calcul

$$y_n y_{n-1} - \left(\alpha^2 + \frac{2\alpha}{\beta}\right) z_n z_{n-1} = (-1)^n \alpha, \tag{18}$$

et l'on voit que le second membre de cette formule est indépendant de β.

Il est évident, du reste, que ces formules spéciales se présentent sous une forme élégante pour $\beta = \alpha$, hypothèse que nous avons à étudier plus amplement dans l'article XIV.

Nous avons encore à étudier cette autre fraction continue, finie et symétrique,

$$K_1 = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{nk-2}, \alpha_{nk-1}); \tag{19}$$

soient

$$\frac{u_1}{v_1}, \frac{u_2}{v_2}, \ldots, \frac{u_{nk-2}}{v_{nk-2}}, \frac{u_{nk-1}}{v_{nk-1}} \tag{20}$$

les réduites de (19), de sorte que

$$u_{nk-2} = v_{nk-1}, \tag{21}$$

nous aurons, quel que soit indice $r > 0$, pour les réduites (2),

$$\frac{y_r}{z_r} = \alpha + \frac{v_r}{u_r}, \tag{22}$$

ou, ce qui est la même chose,

$$\left\{\begin{aligned} y_r &= \alpha u_r + v_r \\ z_r &= u_r; \end{aligned}\right. \tag{23}$$

car les fractions qui figurent, dans (22), sont irréductibles.

Soit maintenant, dans (23), $r = nk - 1$, on aura donc

$$\left\{\begin{aligned} B_n &= u_{nk-1} \\ A_n &= \alpha u_{nk-1} + v_{nk-1} = \alpha B_n + v_{nk-1}, \end{aligned}\right. \tag{24}$$

tandis que l'hypothèse $r = nk - 2$ donnera de même

$$(25)\qquad \begin{cases} b_n = u_{nk-2} = v_{nk-1} \\ a_n = \alpha b_n + v_{nk-2}. \end{cases}$$

III. Du calcul des nombres A_1 et B_1.

Quant à la détermination des nombres A_1 et B_1, savoir les plus petites parmi les solutions de l'équation de FERMAT, la formule (6) de l'article précédent donnera la proposition curieuse:

I. Le calcul des nombres A_1 et B_1 exige seulement la détermination des dénominateurs des réduites de la fraction continue qui représente $\sqrt{a}$, savoir

$$(1)\qquad z_0,\ z_1,\ z_2,\ \ldots,\ z_{k-2},\ z_{k-1} = B_1,$$

puis on aura

$$(2)\qquad A_1 = y_{k-1} = \alpha z_{k-1} + z_{k-2}.$$

Considérons par exemple la fraction continue

$$\sqrt{76} = \left[8,\ (1,\ 2,\ 1,\ 1,\ 5,\ 4,\ 5,\ 1,\ 1,\ 2,\ 1,\ 16)\right],$$

la suite (1) deviendra

1, 1, 3, 4, 7, 39, 163, 859, 1017, 1871, 4759, 6630,

et nous aurons donc

$$B_1 = 6630$$
$$A_1 = 8 \cdot 6630 + 4759 = 57799.$$

Curieusement, la proposition I, que je ne me rappelle pas avoir vue autrefois, est précisément le noyau de la méthode de BROUNCKER, dépouillée de ses énormes calculs superflus, nous le verrons dans l'article V.

Il est évident, du reste, que la formule (7) de l'article précédent donnera une proposition analogue à I, savoir:

II. La détermination des nombres A_1 et B_1 exige seulement le calcul des numérateurs des réduites de la fraction continue qui représente $\sqrt{a}$, savoir

$$y_0, \; y_1, \; y_2, \; \ldots, \; y_{k-2}, \; y_{k-1} = A_1, \tag{3}$$

puis on aura

$$aB_1 = \alpha y_{k-1} + y_{k-2}. \tag{4}$$

Considérons par exemple la fraction continue

$$\sqrt{86} = \left[9, \; (3, \; 1, \; 1, \; 1, \; 8, \; 1, \; 1, \; 1, \; 3, \; 18)\right],$$

la suite (3) deviendra

$$9, \; 28, \; 37, \; 65, \; 102, \; 881, \; 983, \; 1864, \; 2847, \; 10405,$$

et nous aurons donc

$$\begin{aligned} A_1 &= 10405 \\ 86\,B_1 &= 9 \cdot 10405 + 2847 = 96492, \quad B_1 = 1122. \end{aligned}$$

Mais on voit que cette dernière méthode est plus compliquée que la précédente.

Quant au calcul des nombres A_1 et B_1, nous avons encore à appliquer les fondements de la théorie des fractions continues symétriques.[1]

A cet effet, nous prenons pour point de départ la fraction continue

$$K_\nu = (\alpha_\nu, \; \alpha_{\nu-1}, \; \alpha_{\nu-2}, \; \ldots, \; \alpha_2, \; \alpha_1, \; \alpha), \tag{5}$$

où il faut supposer $2\nu \leqq k$ ou $2\nu + 1 \leqq k$, selon que k est pair ou impair.

Soient ensuite

$$\frac{\eta_0}{\xi_0}, \; \frac{\eta_1}{\xi_1}, \; \frac{\eta_2}{\xi_2}, \; \ldots, \; \frac{\eta_{\nu-1}}{\xi_{\nu-1}}, \; \frac{\eta_\nu}{\xi_\nu} \tag{6}$$

[1] Voir par exemple E. LUCAS: Théorie des Nombres, t. I, p. 452—454; Paris 1891.

les réduites de K_ν, les égalités

$$\alpha_{k-r} = \alpha_r, \quad 1 \leqq r \leqq k-1,$$

donnent immédiatement

$$(7) \quad \begin{cases} \eta_{\nu-1} = z_\nu, & \xi_{\nu-1} = z_{\nu-1} \\ \eta_\nu = y_\nu, & \xi_\nu = y_{\nu-1}, \end{cases}$$

tandis que les formules récursives des nombres y_m et z_m donnent

$$y_{k-\nu} = \alpha_\nu y_{k-\nu-1} + y_{k-\nu-2} = \eta_0 y_{k-\nu-1} + \xi_0 y_{k-\nu-2}$$
$$z_{k-\nu} = \alpha_\nu z_{k-\nu-1} + z_{k-\nu-2} = \eta_0 z_{k-\nu-1} + \xi_0 z_{k-\nu-2},$$

de sorte que la conclusion de m à $m+1$ conduira immédiatement aux formules générales

$$(8) \quad \begin{cases} y_{k-\nu+r} = \eta_r y_{k-\nu-1} + \xi_r y_{k-\nu-2} \\ z_{k-\nu+r} = \eta_r z_{k-\nu-1} + \xi_r z_{k-\nu-2}. \end{cases}$$

Cela posé, soit particulièrement $r = \nu - 1$, on aura, en vertu de (7), et en se rappelant que $A_1 = y_{k-1}$ et $B_1 = z_{k-2}$,

$$(9) \quad \begin{cases} A_1 = z_\nu y_{k-\nu-1} + z_{\nu-1} y_{k-\nu-2} \\ B_1 = z_\nu z_{k-\nu-1} + z_{\nu-1} z_{k-\nu-2}, \end{cases}$$

tandis que l'hypothèse $r = \nu$ donnera, en vertu de la formule (7) de l'article précédent,

$$(10) \quad \begin{cases} A_1 = y_\nu z_{k-\nu-1} + y_{\nu-1} z_{k-\nu-2} \\ aB_1 = y_\nu y_{k-\nu-1} + y_{\nu-1} y_{k-\nu-2}. \end{cases}$$

Soit maintenant k un nombre impair, savoir $k = 2\mu + 1$, les formules (9) et (10) donnent, pour $\nu = \mu$, où $\mu \geqq 1$,

$$(11) \quad \begin{cases} y_{2\mu} = y_\mu z_\mu + y_{\mu-1} z_{\mu-1} \\ z_{2\mu} = z_\mu^2 + z_{\mu-1}^2 \\ a z_{2\mu} = y_\mu^2 + y_{\mu-1}^2 \end{cases}$$

où l'on aura par conséquent

$$(11 \text{ bis}) \qquad y_{2\mu} = A_1, \quad z_{2\mu} = B_1.$$

Désignons maintenant par $2n+1$ un positif entier impair quelconque, il est évident que la fraction continue, composée des $2n+1$ premières périodes de la fraction continue proposée, conduira à des formules analogues à (11), où μ est remplacé par $2n\mu+\mu$, ce qui donnera le théorème général:

III. Soit a une base de première espèce, ayant le nombre caractéristique $2\mu+1 \geqq 3$, on aura, quel que soit l'indice $2n+1$,

$$(12) \begin{cases} A_{2n+1} = y_{2n\mu+n+\mu} z_{2n\mu+n+\mu} + y_{2n\mu+n+\mu-1} z_{2n\mu+n+\mu-1} \\ B_{2n+1} = z^2_{2n\mu+n+\mu} + z^2_{2n\mu+n+\mu-1} \\ a B_{2n+1} = y^2_{2n\mu+n+\mu} + y^2_{2n\mu+n+\mu-1}. \end{cases}$$

Dans le cas exclu $\mu = 0$, la fraction continue est de la forme $\left[\alpha, (2\alpha)\right]$, et tous les nombres y_ν et z_ν sont des A_n et B_n, savoir

$$y_\nu = A_{\nu+1}, \quad z_\nu = B_{\nu+1},$$

de sorte que les formules analogues à (11) donnent, pour une valeur paire de ν, savoir en replaçant, dans (11), μ par ν,

$$(12\text{ bis}) \begin{cases} A_{2n+1} = A_{n+1}B_{n+1} + A_n B_n \\ B_{2n+1} = B^2_{n+1} + B^2_n \\ a B_{2n+1} = A^2_{n+1} + A^2_n, \end{cases}$$

et l'on aura, dans ce cas,

$$a = \alpha^2 + 1,$$

base que nous avons à étudier plus amplement, dans l'article XI.

Études maintenant le cas où k est un nombre pair, savoir $k = 2\mu$, les formules (9) et (10) donnent, pour $\nu = \mu - 1$, où il faut supposer $\mu \geqq 2$,

$$(13) \quad \begin{cases} y_{2\mu-1} = y_\mu z_{\mu-1} + y_{\mu-1} z_{\mu-2} \\ z_{2\mu-1} = (z_\mu + z_{\mu-2}) z_{\mu-1} \\ a z_{2\mu-1} = (y_\mu + y_{\mu-2}) y_{\mu-1}, \end{cases}$$

où l'on aura par conséquent

$$(13 \text{ bis}) \qquad y_{2\mu-1} = A_1, \quad z_{2\mu-1} = B_1.$$

Or, il est évident que les formules (13) sont valables pour la fraction continue, composée de n périodes de la fraction continue proposée, ce qui donnera cet autre théorème, analogue au précédent:

IV. Soit a une base de seconde espèce, ayant le nombre caractéristique 2μ, on aura

$$(14) \quad \begin{cases} A_n = y_{n\mu} z_{n\mu-1} + y_{n\mu-1} z_{n\mu-2} \\ B_n = (z_{n\mu} + z_{n\mu-2}) z_{n\mu-1} \\ aB_n = (y_{n\mu} + y_{n\mu-2}) y_{n\mu-1}, \end{cases}$$

où il faut supposer $n \geqq 1$ pour $\mu > 1$, tandis que l'hypothèse $\mu = 1$ exige $n > 1$.

Remarquons, en passant, que le dernier nombre de la suite

$$\omega_0, \ \omega_1, \ \omega_2, \ \ldots, \ \omega_{n\mu-1}$$

est d'une nature très différente selon que n est pair ou impair.

En effet, soit tout d'abord n un nombre pair, on aura

$$\omega_{n\mu-1} = \omega_{2\mu-1} = 1,$$

tandis que l'hypothèse n impair donnera

$$\omega_{n\mu-1} = \omega_{\mu-1} > 1.$$

Les formules que nous venons de développer sont certainement connues, sous une autre forme peut-être, néanmoins je ne me rappelle pas les avoir vu appliquer dans la théorie de l'équation de Fermat, où elles jouent un rôle essentiel, parce qu'elles permettent d'abréger beaucoup les calculs nécessaires, afin de déterminer les nombres A_1 et B_1.

Soit par exemple $a = 61$, la fraction continue deviendra

$$\sqrt{61} = \left[7, (1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14)\right],$$

de sorte que la base 61 a le nombre caractéristique 11, et il faut donc calculer les 6 premières des réduites, afin de déterminer A_1 et B_1, savoir

$$\frac{7}{1}, \frac{8}{1}, \frac{39}{5}, \frac{125}{16}, \frac{164}{21}, \frac{453}{58},$$

ce qui donnera

$$A_1 = 453 \cdot 48 + 164 \cdot 21 = 29718$$
$$B_1 = 58^2 + 21^2 = 3805.$$

Soit, comme second exemple, $a = 94$, on aura la fraction continue

$$\sqrt{94} = \left[9, (1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18)\right],$$

et la base 94 a donc le nombre caractéristique $2\mu = 16$, de sorte qu'il faut calculer les 9 premiers des réduites, savoir

$$\frac{9}{1}, \frac{10}{1}, \frac{29}{3}, \frac{97}{10}, \frac{126}{13}, \frac{223}{23}, \frac{1241}{128}, \frac{1464}{151}, \frac{12953}{1336},$$

et l'on aura

$$A_1 = 12953 \cdot 151 + 1464 \cdot 128 = 2143295$$
$$B_1 = 151\,(1336 + 128) = 221064.$$

Revenons maintenant aux formules (9) et (10), afin de déterminer, à l'aide de ces deux groupes d'équations, les nombres z_ν respectivement y_ν, nous aurons

$$(15) \quad \left\{ \begin{aligned} (-1)^{k-\nu} z_\nu &= A_1 z_{k-\nu-2} - B_1 y_{k-\nu-2} \\ (-1)^{k-\nu} y_\nu &= a B_1 z_{k-\nu-2} - A_1 y_{k-\nu-2}, \end{aligned} \right.$$

ce qui donnera immédiatement la proposition supplémentaire de la proposition I de l'article précédent:

V. Les nombres ω_r qui correspondent à la même période sont symétriques, savoir

$$\omega_{k-r-2} = \omega_r, \qquad 0 \leqq r \leqq k-2. \tag{16}$$

Cela posé, on voit que les formules (11) et (13) de l'article précédent donnent la formule (16) qui correspond à $r = 0$.

Soit par exemple $a = 97$, la fraction continue deviendra

$$\sqrt{97} = \left[9,\ (1,\ 5,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 5,\ 1,\ 18)\right],$$

de sorte que la base 97 a le nombre caractéristique $k = 11$, et l'on aura par conséquent à calculer les 5 premières de ses réduites, savoir

$$\frac{9}{1},\ \frac{10}{1},\ \frac{59}{6},\ \frac{69}{7},\ \frac{128}{13},$$

ce qui donnera

$$\omega_0 = \omega_9 = 16, \quad \omega_1 = \omega_8 = 3, \quad \omega_2 = \omega_7 = 11, \quad \omega_3 = \omega_6 = 8,$$
$$\omega_4 = \omega_5 = 9.$$

Soit, comme second exemple, $a = 71$, on aura la fraction continue

$$\sqrt{71} = \left[8,\ (2,\ 2,\ 1,\ 7,\ 1,\ 2,\ 2,\ 16)\right];$$

c'est-à-dire que la base 71 a le nombre caractéristique $k = 8$; il faut donc calculer les 4 premières de ses réduites, savoir

$$\frac{8}{1},\ \frac{17}{2},\ \frac{42}{5},\ \frac{59}{7},$$

et l'on aura

$$\omega_0 = \omega_6 = 7, \quad \omega_1 = \omega_5 = 5, \quad \omega_2 = \omega_4 = 11, \quad \omega_3 = 2.$$

IV. Des nombres premiers de la forme $4\nu + 3$.

Legendre[1] a démontré qu'un nombre premier de la forme $4\nu + 1$ est toujours une base de première espèce,

[1] Théorie des Nombres, t. I, p. 65; 3e édition, Paris 1830.

théorème que nous aurons à généraliser, en démontrant par deux méthodes différentes, dans les articles X et XXIII, que le nombre $a = (4\nu + 1)^{2\varrho+1}$ est une base de première espèce, de sorte que, pour ces valeurs de a, les nombres B_{2n+1} et aB_{2n+1} sont toujours la somme de deux carrés.

Or, les nombres de la forme $a = (4\nu + 3)^{2\varrho+1}$ où $4\nu + 3$ est un nombre premier, conduiront à des propriétés intéressantes des nombres A_{2n+1} et B_{2n+1}, mais d'une nature différente de celles des B_{2n+1} du cas précédent.

A cet effet, nous prenons pour point de départ les formules (15) de l'article précédent; en supposant $k = 2\mu$, nous aurons pour $\nu = \mu - 1$, où nous supposons $\mu > 1$,

$$(1) \qquad \left\{ \begin{aligned} A_1 z_{\mu-1} - B_1 y_{\mu-1} &= (-1)^{\mu-1} z_{\mu-1} \\ a B_1 z_{\mu-1} - A y_{\mu-1} &= (-1)^{\mu-1} y_{\mu-1}. \end{aligned} \right.$$

Or, $y_{\mu-1}$ et $z_{\mu-1}$ étant premiers entre eux, la première de ces formules donnera

$$(2) \qquad B_1 = z_{\mu-1}\varrho_{\mu-1},$$

où $\varrho_{\mu-1}$ est un positif entier; on aura du reste, en vertu des formules (13) de l'article précédent,

$$(3) \qquad \varrho_{\mu-1} = z_\mu + z_{\mu-2}.$$

Cela posé, la première des formules (1) se présente sous la forme

$$(4) \qquad \varrho_{\mu-1} y_{\mu-1} = A_1 + (-1)^\mu,$$

tandis que la dernière de ces formules deviendra, en vertu de (2),

$$(5) \qquad a\varrho_{\mu-1} z_{\mu-1}^2 = \left(A_1 - (-1)^\mu\right) y_{\mu-1},$$

ce qui donnera

$$(6) \qquad a\varrho_{\mu-1} = \sigma_{\mu-1} y_{\mu-1},$$

où $\sigma_{\mu-1}$ est un positif entier, de sorte que la formule (5) se transforme en celle-ci

(7) $$\sigma_{\mu-1} z_{\mu-1}^2 = A_1 - (-1)^\mu,$$

tandis que la formule (4) donnera, en vertu de (6),

(8) $$\sigma_{\mu-1} y_{\mu-1}^2 = a\left(A_1 + (-1)^\mu\right).$$

Éliminons ensuite, des deux dernières formules, le nombre A_1, il résulte

(9) $$\sigma_{\mu-1}(y_{\mu-1}^2 - a z_{\mu-1}^2) = (-1)^\mu 2a,$$

ou, ce qui est la même chose,

(9 bis) $$\sigma_{\mu-1}\,\omega_{\mu-1} = 2a.$$

Remarquons encore qu'il résulte, en vertu de (2) et (6),

(10) $$aB_1 = \sigma_{\mu-1} y_{\mu-1} z_{\mu-1},$$

tandis que la dernière des formules (13) de l'article précédent donnera, en vertu de (10),

(10 bis) $$\sigma_{\mu-1} z_{\mu-1} = y_\mu + y_{\mu+2}.$$

Il est évident que toutes les formules que nous venons de développer sont valables pour une base quelconque de seconde espèce.

Soit maintenant

$$a = (4\nu + 3)^{2\varrho+1}, \quad \varrho \geqq 0,$$

où $4\nu + 3$ et un nombre premier, il est possible d'approfondir beaucoup les résultats susdits.

A cet effet, supposons tout d'abord que $\sigma_{\mu-1}$ ne soit pas divisible par $4\nu + 3$, il résulte, en vertu de (9),

(11) $$\sigma_{\mu-1} = 1 \quad \text{ou} \quad \sigma_{\mu-1} = 2.$$

Or, il est facile de démontrer que la valeur $\sigma_{\mu-1} = 1$ est inadmissible, parce qu'elle donnera, en vertu de (7),

$$A_1 = z_{\mu-1}^2 + (-1)^\mu,$$

et l'on aura

$$A_1 = z_{\mu-1} y_\mu + z_{\mu-2} y_{\mu-1} > z_{\mu-1}^2 + 1.$$

Quant à la seconde des valeurs (11), on aura

$$A_1 = 2z_{\mu-1}^2 + (-1)^\mu = z_{\mu-1} y_\mu + z_{\mu-2} y_{\mu-1},$$

savoir

$$z_{\mu-1}(2z_{\mu-1} - y_\mu) = z_{\mu-2} y_{\mu-1} - (-1)^\mu. \tag{12}$$

Or, nous aurons toujours, abstraction faite du cas spécial, $\nu = \varrho = 0$, $a = 3$,

$$y_\mu > 2z_\mu \geqq 2z_{\mu-1}. \tag{13}$$

En effet, remarquons que nous aurons $\alpha \geqq 2$, $\alpha_1 \geqq 1$, il résulte

$$\begin{aligned} y_0 &= \alpha, & z_0 &= 1, & y_0 &\geqq 2z_0 \\ y_1 &= \alpha\alpha_1 + 1, & z_1 &= \alpha_1, & y_1 &> 2z_1, \end{aligned}$$

et la conclusion de m à $m+1$ conduira immédiatement à l'inégalité générale (13); c'est-à-dire que la formule (12) ne peut exister, donc la valeur $\sigma_{\mu-1} = 2$ n'est pas appliquable.

Cela posé, il est évident que $\sigma_{\mu-1}$ est nécessairement divisible par le nombre premier $4\nu + 3$, savoir

$$\sigma_{\mu-1} = (4\nu + 3)^\tau k_{\mu-1}, \tag{14}$$

où il faut admettre, en vertu de (9),

$$k_{\mu-1} = 1 \quad \text{ou} \quad k_{\mu-1} = 2. \tag{14 bis}$$

Démontrons maintenant que $y_{\mu-1}$ ne peut jamais être divisible par $4\nu + 3$. En effet, soit

$$y_{\mu-1} = (4\nu + 3)^\sigma t_{\mu-1}, \qquad \sigma > 0,$$

on aura, en vertu de (3) et (6),

$$\sigma_{\mu-1} y_{\mu-1} = a(z_\mu + z_{\mu-2}), \tag{15}$$

ce qui donnera

$$(4\nu + 3)^{\sigma+\tau} t_{\mu-1} k_{\mu-1} = (4\nu + 3)^{2\varrho+1}(z_\mu + z_{\mu-2}),$$

de sorte qu'il faut supposer

$$\sigma + \tau \geqq 2\varrho + 1, \tag{16}$$

parce que nous ne savons pas dès à présent si $z_\mu + z_{\mu-2}$ est divisible par $4\nu + 3$ ou non.

Introduisons maintenant, dans (9), les expressions susdites de $\sigma_{\mu-1}$ et de $y_{\mu-1}$, il résulte

$$\left\{ \begin{aligned} &(4\nu + 3)^{\tau} k_{\mu-1} \left((4\nu + 3)^{2\sigma} t_{\mu-1}^2 - (4\nu + 3)^{2\varrho+1} z_{\mu-1}^2\right) = \\ &\qquad = (-1)^{\mu} 2 (4\nu + 3)^{2\varrho+1}. \end{aligned} \right. \tag{17}$$

Or, il est facile de voir que cette équation est inadmissible, parce que le premier membre est divisible par une puissance de $4\nu + 3$ plus élévée que celle qui divise le second membre. En effet, l'exposant de cette puissance de $4\nu + 3$ deviendra ou $\tau + 2\sigma$ ou $\tau + 2\varrho + 1$, selon que $\sigma \leqq \varrho$ ou $\sigma > \varrho$.

Cela posé, il est évident que $y_{\mu-1}$ ne peut jamais être divisible par $4\nu + 3$, et l'on aura donc, en vertu de (9),

$$\tau = 2\varrho + 1,$$

ce qui donnera, en vertu de (14),

$$\sigma_{\mu-1} = a \quad \text{ou} \quad \sigma_{\mu-1} = 2a. \tag{18}$$

Or, la dernière de ces deux valeurs est inadmissible, parce qu'elle donnera, en vertu de (9),

$$y_{\mu-1}^2 - a z_{\mu-1}^2 = (-1)^{\mu},$$

ce qui exige nécessairement que μ soit un nombre pair, car a est une base de seconde espèce, mais on aura $A_1 > y_{\mu-1}$, et A_1 et B_1 sont les plus petites solutions de l'équation de Fermat en question. C'est-à-dire qu'il ne nous reste que la valeur $\sigma_{\mu-1} = a$, ce qui donnera

$$(19)\quad \begin{cases} y_{\mu-1} = z_\mu + z_{\mu-2} \\ az_{\mu-1} = y_\mu + y_{\mu-2} \\ y^2_{\mu-1} = az^2_{\mu-1} + (-1)^\mu 2, \end{cases}$$

savoir

$$(20)\qquad \omega_{\mu-1} = 2;$$

de plus, on aura, pour les nombres A_1 et B_1,

$$(21)\quad \begin{cases} A_1 = y^2_{\mu-1} - (-1)^\mu \\ B_1 = y_{\mu-1}\, z_{\mu-1}. \end{cases}$$

Dans ces développements, nous avons supposé $\mu > 1$, de sorte qu'il nous reste à considérer le cas spécial $\mu = 1$, ce qui nous conduira à la fraction continue (15) de l'article II, et nous aurons par conséquent

$$a = \alpha^2 + \frac{2\alpha}{\beta},$$

où 2α est divisible par β.

Cela posé, soit $\alpha = k\beta$ ou $\alpha = 2k\beta$, on aura respectivement

$$a = k(k\beta^2 + 2), \quad a = 4k(k\beta^2 + 1),$$

et il est évident que ces deux nombres ne sont ni un premier ni une puissance d'un premier, à moins que $k = 1$, ce qui donnera

$$a = \beta^2 + 2, \quad a = 4\beta^2 + 4,$$

et, le second de ces nombres n'étant jamais une puissance de $4\nu + 3$, il nous reste seulement à considérer le premier.

La fraction continue correspondante, savoir

$$\sqrt{\beta^2 + 2} = \left[\beta, (\beta, 2\beta)\right],$$

donnera immédiatement

$$y_0 = \beta,\; z_0 = 1;\; y_1 = A_1 = \beta^2 + 1,\; z_1 = B_1 = \beta,$$

de sorte que les formules (20) et (21) sont valables aussi dans ce cas, quel que soit le nombre $\beta^2 + 2$, premier ou non.

De plus, il est évident que le cas $a = 3$, exclu dans la démonstration de l'inégalité (13), est contenu dans la forme $\beta^2 + 2$, savoir pour $\beta = 1$; c'est-à-dire que les formules (20) et (21) sont valables, quel que soit le nombre premier $4\nu + 3$, savoir quel que soit le positif entier μ.

Quant à la dernière des formules (19), remarquons, avec LEGENDRE[1], que les nombres $y_{\mu-1}$ et $z_{\mu-1}$ sont tous deux impairs, et que le premier membre de la formule susdite est de la forme $8\sigma - 2$ ou $8\sigma + 2$, selon que ν est pair ou impair, savoir $a = 8\tau + 3$ respectivement $a = 8\tau + 7$, ce qui donnera la proposition curieuse que je ne me rappelle pas avoir vue autrefois:

I. Soit $4\nu + 3$ un nombre premier, et soit 2μ le nombre caractéristique de la base

$$a = (4\nu + 3)^{2\varrho+1}, \quad \varrho \geqq 0, \tag{22}$$

μ et ν sont toujours de différente parité, de sorte que $\mu + \nu$ est un nombre impair.

Cela posé, je dis que les formules que nous venons de développer donnent les deux théorèmes suivants:

II. Soit 2μ le nombre caractéristique de la base $a = (4\nu + 3)^{2\varrho+1}$, où $4\nu + 3$ est un nombre premier, on aura, quel que soit n,

$$\left\{\begin{aligned} A_{2n+1} &= y^2_{2n\mu+\mu-1} + (-1)^\nu \\ B_{2n+1} &= y_{2n\mu+\mu-1}\, z_{2n\mu+\mu-1}. \end{aligned}\right. \tag{23}$$

En effet, on voit que les deux formules en question sont vraies pour $n = 0$. De plus, les formules récursives de LAGRANGE, que nous avons à étudier plus amplement dans l'article VII, donnent, en vertu de (21),

[1] Théorie des Nombres, t. I, p. 66; 3e édition, Paris 1830.

$$A_{2n+1} = A_{2n}\left(y^2_{\mu-1} + (-1)^\nu\right) + aB_{2n}\,y_{\mu-1}\,z_{\mu-1}$$
$$B_{2n+1} = A_{2n}\,y_{\mu-1}\,z_{\mu-1} + B_{2n}\left(y^2_{\mu-1} + (-1)^\nu\right),$$

tandis que nous aurons, en vertu des formules générales (8) de l'article II,

$$(24)\quad \left\{\begin{aligned} y_{2n\mu+\mu-1} &= A_n\,y_{\mu-1} + aB_n\,z_{\mu-1} \\ z_{2n\mu+\mu-1} &= B_n\,y_{\mu-1} + A_n\,z_{\mu-1}. \end{aligned}\right.$$

Introduisons maintenant, dans (23), ces expressions, puis appliquons les formules

$$A_{2n} = A_n^2 + aB_n^2, \quad B_{2n} = 2A_nB_n,$$

conséquences immédiates des formules récursives de Lagrange, la vérification des formules en question est faite.

De plus, les formules (24) donnent immédiatement, en vertu de (19), le second des théorèmes susdits, savoir:

III. Soit 2μ le nombre caractéristique de la base $a = (4\nu+3)^{2\varrho+1}$, où $4\nu+3$ est un nombre premier, on aura, quel que soit n,

$$(25)\quad \left\{\begin{aligned} y^2_{2n\mu+\mu-1} - a z^2_{2n\mu+\mu-1} &= (-1)^{\nu-1}2 \\ y_{2n\mu+\mu-1} &= z_{2n\mu+\mu} + z_{2n\mu+\mu-2} \\ az_{2n\mu+\mu-1} &= y_{2n\mu+\mu} + y_{2n\mu+\mu-2}. \end{aligned}\right.$$

Dans l'article XXIII, nous avons à revenir, d'un autre point de vue, aux formules (23).

Quant à la dernière des formules (19), nous avons encore à démontrer la proposition:

IV. Soit $a = (4\nu+3)^{2\varrho+1}$, où $4\nu+3$ est un nombre premier, l'équation indéterminée

$$(26)\qquad x^2 - ay^2 = (-1)^\mu 2$$

n'est jamais résoluble en positifs entiers, à moins que μ et ν ne soient de différente parité; dans ce cas, la solution complète de l'équation susdite deviendra

$$x = y_{2n\mu+\mu-1}, \quad y = z_{2n\mu+\mu-1}. \tag{27}$$

La partie de la proposition qui concerne les nombres μ et ν est évidente. Supposons ensuite résoluble en positifs entiers l'équation (26), puis désignons par u, v une solution quelconque, les deux nombres u et v sont nécessairement tous deux impairs. Posons ensuite

$$\xi = u^2 - (-1)^{\mu}, \quad \eta = uv, \tag{28}$$

un calcul direct donnera, en vertu de (26),

$$\xi^2 - a\eta^2 = 1,$$

de sorte que nous aurons

$$\xi = A_{2n+1}, \quad \eta = B_{2n+1},$$

car η est un nombre impair, et les $B_{2n} = 2A_nB_n$ sont des nombres pairs.

Cela posé, nous aurons, en vertu de (23),

$$\xi = y^2_{2n\mu+\mu-1} - (-1)^{\mu}, \quad \eta = y_{2n\mu+\mu-1}z_{2n\mu+\mu-1},$$

donc les formules (28) donnent

$$u = y_{2n\mu+\mu-1}, \quad v = z_{2n\mu+\mu-1}, \tag{29}$$

savoir les expressions (27).

V. De la méthode de Brouncker.

Quant à la première méthode appliquée pour résoudre l'équation de FERMAT, savoir la méthode de BROUNCKER, rédigée et publiée par WALLIS[1], mais faussement attribuée à PELL, d'après une remarque erronée d'EULER[2], on lit par exemple dans les Cours de LEJEUNE DIRICHLET[3].

[1] Commercium epistolicum, Londres 1658.

[2] Algebra, t. II, p. 242, herausgegeben von J. P. GRÜSON; Berlin 1797. Voir aussi G. WERTHEIM: Anfangsgründe der Zahlenlehre, p. 402; Brunswick 1902.

[3] Vorlesungen über Zahlentheorie, herausgegeben von R. DEDEKIND, 3e édition, p. 200; Brunswick 1879.

»... allein obwohl seine Methode [la méthode de BROUNCKER faussement attribuée à PELL] die Lösung in jedem Falle wirklich giebt, so lag doch in ihr nicht der Nachweis, dass sie immer zum Ziele führen muss.«

De même, WERTHEIM[1] dit:

».... [la méthode de BROUNCKER] hat nicht nur den Nachteil, höchst umständlich zu sein, sondern sie lässt auch nicht erkennen, dass die Aufgabe immer möglich ist.«

Ces remarques amènent tout naturellement le lecteur à se demander quelle est donc la nature cachée et énigmatique de cette méthode compliquée. Or, EULER ayant développé très nettement la méthode susdite, il est possible de donner une réponse complète à une telle question.

A cet effet, soit a la base en question, et soit k son nombre caractéristique, nous posons

$$\sqrt{a} = \left[\alpha, (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{\nu-2}, \alpha_{\nu-1}, 2\alpha)\right], \tag{1}$$

où il faut admettre $\nu = k$ ou $\nu = 2k$, selon que k est pair ou impair; c'est-à-dire que ν est toujours un nombre pair. De plus, nous désignons par

$$\frac{y_0}{z_0}, \frac{y_1}{z_1}, \frac{y_2}{z_2}, \ldots, \frac{y_{\nu-2}}{z_{\nu-2}}, \frac{y_{\nu-1}}{z_{\nu-1}} \tag{2}$$

les ν premières réduites de la fraction continue (1), de sorte que nous aurons

$$\left\{\begin{array}{l} A_1 = y_{\nu-1}, \quad B_1 = z_{\nu-1} \\ A_2 = y_{\nu-1}, \quad B_2 = z_{\nu-1}, \end{array}\right. \tag{3}$$

selon que k est pair ou impair.

Ces définitions adoptées, je dis que:

I. *La méthode de Brouncker pour résoudre l'équation de* FERMAT

$$x^2 - ay^2 = 1 \tag{4}$$

[1] Anfangsgründe der Zahlenlehre, p. 219; Brunswick 1902.

n'est, du point de vue pratique, qu'un calcul successif et extrêmement compliqué des dénominateurs z_r des réduites (2), d'après les formules récursives

$$z_r = \alpha_r z_{r-1} + z_{r-2}, \quad 0 \leqq r \leqq \nu - 1, \tag{5}$$

puis $y_{\nu-1}$ se détermine, en vertu de la formule

$$y_{\nu-1} = \alpha z_{\nu-1} + z_{\nu-2}; \tag{6}$$

c'est-à-dire que la méthode de Brouncker est, d'un point de vue pratique, l'établissement masqué et énormément compliqué de la fraction continue de LAGRANGE. Mais d'un point de vue théorique, la méthode de Brouncker présente d'autres difficultés considérables.

Or, il n'est pas possible de démontrer, d'un point de vue général, ce postulat, parce que le procédé de BROUNCKER n'est pas une méthode générale.

En effet, EULER[1] dit expressément:

»Diese [la méthode de BROUNCKER, faussement attribuée à PELL] ist aber nicht so beschaffen, dass sie auf eine allgemeine Art für eine jede Zahl a, sondern nur für einen jeden Fall besonders gebraucht werden kann.«

Cela posé, il ne nous reste donc qu'à examiner quelques-uns des exemples considéres par EULER, et, afin de mettre en pleine lumière la vraie nature de la méthode de BROUNCKER, nous coordonnons les racines carrées, appliquées par EULER, et les expressions correspondantes de y_r, savoir

$$y_r = \sqrt{a z_r^2 - (-1)^r \omega_r}, \quad 0 \leqq r \leqq \nu - 1, \tag{7}$$

tirées directement de la définition des nombres ω_r, savoir la formule (9) de l'article II.

[1] Algebra, herausgegeben von J. P. GRÜSON, t. II, p. 242; Berlin 1797.

Exemple I. $\quad a = 6, \quad \nu = k = 2.$

Dans ce cas, la fraction continue et ses deux premières réduites deviennent

$$\sqrt{6} = [2, (2, 4)], \quad \frac{2}{1}, \quad \frac{5}{2},$$

et l'on aura, d'après Euler,

$$m^2 = 6n^2 + 1, \quad m > 2n, \quad m = 2n + p,$$

d'où, en éliminant m, puis cherchant n de l'équation quadratique ainsi obtenue,

$$n = \frac{2p + \sqrt{6p^2 - 2}}{2}, \quad y_0 = \sqrt{6z_0^2 - 2},$$

ce qui donnera $n > 2p$, savoir $n = 2p + q$, d'où il résulte, en éliminant n, puis cherchant p de l'équation quadratique ainsi obtenue,

$$p = 2q + \sqrt{6q^2 + 1},$$

où la racine carrée est de la même forme que celle obtenue pour m, savoir

$$m = \sqrt{6n^2 + 1}.$$

Posons ensuite $q = 0$, nous aurons successivement

$$p = 1, \quad n = 2, \quad m = 5.$$

Exemple II. $\quad a = 7, \quad \nu = k = 4,$

ce qui donnera la fraction continue et ses 4 premières réduites

$$\sqrt{7} = [2, (1, 1, 1, 4)], \quad \frac{2}{1}, \quad \frac{3}{1}, \quad \frac{5}{2}, \quad \frac{8}{3}.$$

Posons ensuite avec Euler

$$m^2 = 7n^2 + 1, \quad m > 2n, \quad m = 2n + p,$$

nous aurons, par le procédé indiqué dans l'exemple I,

$$n = \frac{2p + \sqrt{7p^2 - 3}}{3}, \quad y_2 = \sqrt{7z_2^2 - 3};$$

$$n > p, \quad n = p + q$$

$$p = \frac{q + \sqrt{7q^2 + 2}}{2}, \quad y_1 = \sqrt{7z_1^2 + 2};$$

$$p > q, \quad p = q + r$$

$$q = \frac{r + \sqrt{7r^2 - 3}}{3}, \quad y_0 = \sqrt{7z_0^2 - 3};$$

$$q > r, \quad q = r + s, \quad r = 2s + \sqrt{7s^2 + 1},$$

où la racine carrée est de la même forme que celle obtenue pour m, savoir

$$m = \sqrt{7n^2 + 1}.$$

Soit donc $s = 0$, on aura successivement

$$r = 1, \ q = 1, \ p = 2, \ n = 3, \ m = 8.$$

Quant à la méthode ainsi expliquée, EULER[1] fait la remarque caractéristique:

»Bisweilen gelangt man bald zu seinem Zweck, bisweilen aber werden dazu viele Operationen erfordert, nach Beschaffenheit der Zahl a, wovon man doch keine gewisse Kennzeichen angeben kann. Bis zu der Zahl 13 geht es noch ziemlich schnell; kömmt man aber zu dem Falle, wo $a = 13$, so wird die Rechnung viel weitläufiger, und daher wird es gut seyn, diesen Fall genauer zu betrachten.«

Cela posé, il nous semble utile de donner un aperçu de la résolution, d'après la méthode de BROUNCKER, de l'équation de FERMAT qui correspond à $a = 13$.

Exemple III. $a = 13, \ k = 5, \ \nu = 2k = 10.$

La fraction continue correspondante

$$\sqrt{13} = \left[3, (1, 1, 1, 1, 6, 1, 1, 1, 1, 6)\right]$$

a les 10 premières réduites

[1] Algebra, herausgegeben von J. P. GRÜSON, t. II, p. 246; Berlin 1797.

$$(8)\quad \frac{3}{1},\ \frac{4}{1},\ \frac{7}{2},\ \frac{11}{3},\ \frac{18}{5},\ \frac{119}{33},\ \frac{137}{38},\ \frac{256}{71},\ \frac{393}{109},\ \frac{649}{180}.$$

Posons maintenant, avec Euler

$$m = 13n^2 + 1, \quad m > 3n, \quad m = 3n + p,$$

nous aurons, comme dans les deux exemples précédents,

$$\begin{array}{lll}
m = 3n + p, & n = \dfrac{3p + \sqrt{13p^2 - 4}}{4}, & y_8 = \sqrt{13z_8^2 - 4} \\[2ex]
n = p + q, & p = \dfrac{q + \sqrt{13q^2 + 3}}{3}, & y_7 = \sqrt{13z_7^2 + 3} \\[2ex]
p = q + r, & q = \dfrac{2r + \sqrt{13r^2 - 3}}{3}, & y_6 = \sqrt{13z_6^2 - 3} \\[2ex]
q = r + s, & r = \dfrac{s + \sqrt{13s^2 + 4}}{4}, & y_5 = \sqrt{13z_5^2 + 4} \\[2ex]
r = s + t, & s = 3t + \sqrt{13t^2 - 1}, & y_4 = \sqrt{13z_4^2 - 1} \\[2ex]
s = 6t + u, & t = \dfrac{3u + \sqrt{13u^2 + 4}}{4}, & y_3 = \sqrt{13z_3^2 + 4} \\[2ex]
t = u + v, & u = \dfrac{v + \sqrt{13v^2 - 3}}{3}, & y_2 = \sqrt{13z_2^2 - 3} \\[2ex]
u = v + x, & v = \dfrac{2x + \sqrt{13x^2 + 3}}{3}, & y_1 = \sqrt{16z_1^2 + 3} \\[2ex]
v = x + y, & x = \dfrac{y + \sqrt{13y^2 - 4}}{4}, & y_0 = \sqrt{16z_0^2 - 4} \\[2ex]
x = y + z, & y = 3z + \sqrt{13z^2 + 1}. &
\end{array}$$

Ayant ainsi obtenu une racine carrée de la même forme que celle qui représente m, savoir $\sqrt{13n^2 + 1}$, nous posons $z = 0$, et nous trouvons successivement

$$y = 1,\ x = 1,\ v = 2,\ u = 3,\ t = 5,\ s = 33,\ r = 38,\ q = 71,$$
$$p = 109,\ n = 180,\ m = 649,$$

savoir les dénominateurs des réduites (8) et le numérateur de la dernière.

De plus, on voit que les relations rationnelles établies entre les m, n, p, q etc., ne sont autre chose que les formules récursives (5), appliquées aux dénominateurs des réduites (8), suppléées par la formule (6) correspondante.

On voit, du reste, que les exemples $a = 7$, $a = 13$ sont peu caractéristiques, à cause des nombreux nombres 1 dans les périodes, mais EULER n'en donne pas d'autres plus caractéristiques, et il saute aux yeux que ces exemples confirment parfaitement notre postulat concernant la méthode de BROUNCKER.

Remarquons que cette méthode donne dans l'ordre inverse les formules récursives (5) et par conséquent aussi les dénominateurs z_r, mais ce renversement ne joue aucun rôle pour la fraction continue, parce que sa période est symétrique.

Revenons maintenant au cas $a = 13$; EULER poursuit ses calculs sans s'arrêter à la relation curieuse

$$s = 3t + \sqrt{13t^2 - 1}, \quad y_4^2 - 13z_4^2 = -1,$$

savoir à la résolution de l'équation indéterminée

$$x^2 - 13y^2 = -1,$$

ce qui s'accorde bien avec le fait que les équations

$$x^2 - ay^2 = -1$$

sont restées complètement inaperçues jusqu'à ce que LAGRANGE a donné sa résolution ingénieuse de l'équation de FERMAT.

Remarquons encore que le cas $a = 13$ donne des relations de la forme

$$\omega_r z_{r+1} = p_r z_r + y_r, \tag{9}$$

où les p_r sont des positifs entiers que nous avons à étudier dans l'article qui suit. De plus, les formules en question montrent une périodicité des nombres p_r, analogue à celle que nous avons établie, dans l'article II, pour les ω_r.

Revenons maintenant à la méthode de Brouncker.

Euler[1], ayant terminé les longs calculs exigés par $a = 13$, remarque:

»Aus diesem Beyspiele sieht man deutlich, wie weitläufig eine solche Rechnung werden könne. Denn unter den grösseren Zahlen muss man oft wohl zehn mal mehr Operationen machen, als hier bey der Zahl 13 vorgekommen sind: man kann auch nicht wohl voraus sehen, bey welchen Zahlen so grosse Mühe erfordert wird.«

Oui, les manques fondamentaux de la méthode de Brouncker sont évidents. En effet, du point de vue théorique, la méthode étant complètement heuristique, elle ne peut donner aucune démonstration générale de l'existence des positifs entiers qui satisfont à l'équation correspondante de Fermat. Mais, de plus, la méthode de Brouncker exige la connaissance des nombres ω_r et p_r, étrangers à la méthode de Lagrange. Or, cette dernière méthode fondée, c'est-à-dire l'existence des solutions de l'équation de Fermat établie, la méthode de Brouncker nous permet une étude plus approfondie de la fraction continue de Lagrange, nous le verrons dans l'article qui suit.

En second lieu, du point de vue pratique, la méthode de Brouncker est énormément compliquée, comme le montre clairement le cas $a = 13$ qui exige, en effet, 10 évaluations numériques pour déterminer les α_r, 9 éliminations et 9 résolutions d'une équation quadratique pour déterminer les valeurs

$$A_2 = 649, \quad B_2 = 180.$$

[1] Algebra, herausgegeben von J. P. Grüson, t. II, p. 249; Berlin 1797.

Quant à la méthode de LAGRANGE, elle exige seulement le calcul des trois premières des réduites (8), parce que les formules (12) de l'article III donnent

$$B_1 = z_4 = 2^2 + 1^2 = 5$$
$$A_1 = y_4 = 7\cdot 2 + 4\cdot 1 = 18,$$

et nous aurons donc, en vertu des formules récursives de LAGRANGE, que nous avons à étudier, dans l'article VII,

$$A_2 = 2A_1^2 + 1 = 649$$
$$B_2 = 2A_1 B_1 = 180.$$

VI. Des nombres ω_r et p_r.

Revenons maintenant aux positifs entiers p_r, définis heuristiquement par la formule (9) de l'article précédent, savoir

$$\omega_r z_{r+1} = p_r z_r + y_r. \tag{1}$$

A cet effet, supposons vraie cette formule, puis appliquons la définition des nombres ω_r, indiquée par la formule (9) de l'article II, savoir

$$y_r^2 - a z_r^2 = (-1)^{r-1}\omega_r, \tag{2}$$

nous aurons

$$z_{r+1}(y_r^2 - a z_r^2) = (-1)^{r-1}(p_r z_r + y_r),$$

ou, ce qui est la même chose

$$y_r\left(y_r z_{r+1} + (-1)^r\right) = z_r\left(a z_r z_{r+1} - (-1)^r p_r\right).$$

Appliquons ensuite l'équation, fondamentale dans la théorie des fractions continues,

$$y_r z_{r+1} - z_r y_{r+1} = (-1)^{r+1}, \tag{3}$$

il résulte, après un simple calcul,

$$y_r y_{r+1} - a z_r z_{r+1} = (-1)^{r+1} p_r. \tag{4}$$

Inversement, définissons, par la formule (4), la suite des nombres p_r, puis cherchons, de (3) et (4), les valeurs de y_{r+1} et de z_{r+1}, nous trouvons, outre la formule (1), cette autre formule analogue à (1)

$$\omega_r y_{r+1} = p_r y_r + a z_r, \tag{5}$$

de sorte qu'il ne nous reste qu'à démontrer que les nombres entiers p_r sont toujours positifs.

A cet effet, nous avons tout d'abord à démontrer deux propriétés des nombres entiers p_r, définis par la formule (4), savoir:

I. Les nombres p_r sont périodiques, parce que

$$p_{nk+r} = p_r, \quad 0 \leqq r \leqq k-3, \tag{6}$$

et les nombres p_r qui appartiennent à la même période sont symétriques, car

$$p_{k-r-3} = p_r, \quad 0 \leqq r \leqq k-3. \tag{7}$$

En effet, la formule (6) est une conséquence immédiate des formules générales (8) de l'article II, tandis que la formule (7) provient directement des formules (15) de l'article III, de sorte que la démonstration des formules (6) et (7) est parfaitement analogue à la démonstration des formules correspondantes pour les ω_r.

Cela posé, il nous reste seulement à démontrer que les p_{2r} sont toujours positifs. En effet, soit, dans (6), $n = 1$ et k et r des nombres impairs, il est évident que $k + r$ est pair. De même, soit, dans (7), k pair et r impair, le nombre $k - r - 3$ est pair.

Démontrons maintenant que les p_{2r} sont toujours positifs.

A cet effet, nous posons, quel que soit l'indice r,

$$\frac{y_{2r}}{z_{2r}} = \sqrt{a} - \varepsilon_{2r}, \quad \frac{y_{2r+1}}{z_{2r+1}} = \sqrt{a} + \varepsilon_{2r+1},$$

les nombres irrationnels ε_{2r} et ε_{2r+1} sont tous deux positifs, et nous aurons, en outre, $\varepsilon_{2r} > \varepsilon_{2r+1}$. Multiplions maintenant les deux formules susdites, il résulte

$$\frac{y_{2r}\, y_{2r+1}}{z_{2r}\, z_{2r+1}} - a = -(\varepsilon_{2r} - \varepsilon_{2r+1})\sqrt{a} - \varepsilon_{2r}\,\varepsilon_{2r+1} < 0,$$

ou, ce qui est la même chose, les p_{2r} sont toujours positifs.

Or, l'existence des formules heuristiques (1) et (5) étant ainsi rigoureusement établie, les formules (2) et (4) montrent clairement l'analogie des deux suites formées des nombres ω_r et des nombres p_r.

Quant au nombre p_{k-2}, qui ne figure pas dans la formule (7), les équations (6) et (7) de l'article II, savoir

$$y_{k-1} = \alpha z_{k-1} + z_{k-2}, \quad a z_{k-1} = \alpha y_{k-1} + y_{k-2},$$

donnent immédiatement

$$p_{k-2} = \alpha, \tag{8}$$

résultat qui est intéressant, nous le verrons dans ce qui suit.

Les nombres ω_r et p_r, introduits par la méthode de Brouncker, jouent un rôle intéressant dans la théorie de la fraction continue de Lagrange. Or, pour mettre en pleine lumière les propriétés fondamentales des nombres susdits, nous avons tout d'abord à démontrer la proposition:

II. *Soit a une base quelconque, les deux valeurs $a = 3$ et $a = 8$ seulement exceptées, on aura toujours, quel que soit r,*

$$\omega_r < \frac{a}{2}. \tag{9}$$

On aura, en effet, en vertu de la définition de ω_r, savoir la formule (2),

$$\frac{\omega_r}{z_r^2} = \left|\frac{y_r^2}{z_r^2} - a\right| < \left|\frac{y_r^2}{z_r^2} - \frac{y_{r+1}^2}{z_{r+1}^2}\right|,$$

ce qui donnera

$$\omega_r < \frac{y_r z_{r+1} + z_r y_{r+1}}{z_{r+1}^2} < \frac{2y_{r+1}}{z_{r+1}}.$$

De plus, nous aurons évidemment

$$\frac{y_{r+1}}{z_{r+1}} < \sqrt{a} + \frac{1}{z_{r+1} z_{r+2}} \leqq \sqrt{a} + \frac{1}{z_{r+2}} \leqq \sqrt{a} + \frac{1}{2},$$

ce qui donnera

$$\omega_r < \frac{2y_{r+1}}{z_{r+1}} < 2\sqrt{a} + 1,$$

donc nous aurons certainement

$$\omega_r < \frac{a}{2},$$

pourvu que

$$2\sqrt{a} + 1 < \frac{a}{2}, \quad a > 4\sqrt{a} + 2,$$

ou, ce qui est la même chose,

$$(\sqrt{a} - 2)^2 > 6, \quad \sqrt{a} - 2 > \sqrt{6},$$

savoir

$$a > 10 + 4\sqrt{6},$$

ce qui a certainement lieu pour $a \geqq 20$, car $2\sqrt{6} < 5$.

Cela posé, il s'agit seulement des onze nombres

(10) $$3, 6, 7, 8, 11, 12, 13, 14, 15, 18, 19,$$

car les nombres 2, 5, 10, 17, étant de la forme $\alpha^2 + 1$, ne donnent aucun nombre ω_r outre $\omega_0 = 1$.

Quant aux sept des nombres (10), savoir

(11) $$3, 6, 8, 11, 12, 15, 18,$$

ils sont contenus dans les expressions

$$\alpha^2 - 1, \ \alpha^2 + 2, \ \alpha^2 + \alpha,$$

et les périodes des fractions continues correspondantes ne contiennent que deux nombres, de sorte qu'il s'agit seulement du nombre ω_0 qui a les valeurs correspondantes

(11 bis) $$2, 2, 4, 2, 3, 6, 2.$$

De plus, les nombres 7 et 14 sont de la forme $\alpha^2 - 2$, et la fraction continue correspondante, savoir

$$\sqrt{\alpha^2 - 2} = \left[\alpha - 1, (1, \alpha - 2, 1, 2\alpha - 2)\right], \quad \alpha \geqq 3,$$

a les deux premières réduites

$$\frac{\alpha - 1}{1}, \quad \frac{\alpha}{1},$$

ce qui donnera

$$\omega_0 = \omega_2 = 2\alpha - 3, \quad \omega_1 = 2,$$

et l'on aura, pour $\alpha \geqq 3$,

$$\alpha^2 - 2 > 4\alpha - 6, \quad \alpha^2 - 4\alpha + 4 > 0; \quad \alpha^2 > 4.$$

Cela posé, il ne nous reste que les deux nombres 13 et 19, et la fraction continue

$$\sqrt{13} = \left[3, (1, 1, 1, 1, 6)\right]$$

donnera

$$\omega_0 = \omega_3 = 4, \quad \omega_1 = \omega_2 = 3,$$

tandis que nous aurons

$$\sqrt{19} = \left[4, (2, 1, 3, 1, 2, 8)\right],$$

et les valeurs de ω_r deviennent

$$\omega_0 = \omega_4 = 3, \quad \omega_2 = 2, \quad \omega_1 = \omega_3 = 5.$$

Ces calculs faits, on voit, en vertu de (11) et (11 bis), que les nombres (10) donnent seulement deux exceptions de l'inégalité (9), savoir $a = 3$, $\omega_0 = 2$ et $a = 8$, $\omega_0 = 4$.

L'inégalité fondamentale (9) ainsi établie, nous avons à revenir aux nombres p_r.

A cet effet, multiplions par az_{r+1}, respectivement par y_{r+1} les formules (1) et (5), puis soustrayons les deux équations ainsi obtenues, nous aurons la formule curieuse

(12) $$\omega_r \, \omega_{r+1} = a - p_r^2,$$

ce qui donnera, quel que soit l'indice r,

$$p_r < \sqrt{a}, \tag{13}$$

et nous avons donc la proposition:

III. Soit a une base quelconque, on aura toujours, quel que soit l'indice r,

$$p_r \leqq \alpha. \tag{14}$$

Quant à ce dernier résultat, la formule (8) montre que p_r peut avoir la valeur maximum α.

En second lieu, éliminons de (1) et (5) et de l'expression de ω_{r+1} les y_{r+1} et les z_{r+1}, en appliquant les formules récursives ordinaires, nous aurons respectivement

$$p_r + p_{r-1} = \alpha_r \omega_r \tag{15}$$

$$\omega_{r+1} - \omega_{r-1} = 2\alpha_r p_{r-1} - \alpha_r^2 \omega_r, \tag{16}$$

d'où il résulte, en éliminant ω_r,

$$\omega_{r+1} - \omega_{r-1} = \alpha_r (p_{r-1} - p_r). \tag{17}$$

Appliquons maintenant les inégalités (14), puis remarquons que $\omega_r \geqq 2$, nous aurons la proposition:

IV. Soit k le nombre caractéristique de la base a, on aura, dans la fraction continue, infinie et périodique,

$$\sqrt{a} = \left[\alpha, (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{k-2}, \alpha_{k-1}, 2\alpha)\right],$$

constamment

$$\alpha_r \leqq \alpha, \quad 1 \leqq r \leqq k-1. \tag{18}$$

Revenons encore une fois à la définition des ω_r, savoir la formule (2), puis appliquons la formule (16) de l'article III, nous aurons la proposition curieuse:

V. Soit a une base de première espèce ayant le nombre caractéristique $k > 1$, on aura constamment

$$(19)\quad y_0^2+y_1^2+y_2^2+\ldots+y_{k-2}^2=a(z_0^2+z_1^2+z_2^2+\ldots+z_{k-2}^2).$$

Soit, au contraire, la base a de seconde espèce, ayant le nombre caractéristique $k = 2\mu$, on aura, en vertu de (2),

$$(20)\quad \sum_{r=0}^{r=\mu-2} y_r^2 - a\sum_{r=0}^{r=\mu-2} z_r^2 = (-1)^{\mu}\omega_{\mu-1} + 2\sum_{r=0}^{r=\mu-2}(-1)^{r+1}\,\omega_r,$$

où il faut supposer naturellement $\mu \geqq 2$, tandis que l'on aura, pour $\mu = 1$,

$$(20\text{ bis})\qquad y_0^2 - az_0^2 = -\omega_0.$$

Quant à la différence qui figure au premier membre de (20), je ne me rappelle pas avoir vu un seul cas, où elle est positif ou zéro, mais j'ignore complètement les propriétés générales de cette différence.

CHAPITRE II

Propriétés générales des solutions.

VII. Formules d'addition et formules logarithmiques.

Revenons maintenant aux formules (8) et (8 bis) de l'article II, savoir les formules récursives

$$(1)\qquad \begin{cases} y_{nk+r} = A_n y_r + aB_n z_r \\ z_{nk+r} = A_n z_r + B_n y_r \end{cases}$$

et les formules inverses

$$(2)\qquad \begin{cases} y_r = (-1)^{nk} (A_n y_{nk+r} - aB_n z_{nk+r}) \\ z_r = (-1)^{nk} (A_n z_{nk+r} - B_n y_{nk+r}), \end{cases}$$

il est évident que les formules (1) permettent de déterminer les numérateurs et les dénominateurs appartenant à une période quelconque de la fraction continue

$$(3)\qquad \sqrt{a} = \left[\alpha,\ (\alpha_1,\ \alpha_2,\ \alpha_3,\ \ldots,\ \alpha_{k-1},\ 2\alpha)\right],$$

où k est le nombre caractéristique de la base a, pourvu que les nombres susdits, appartenant à la première période, et les solutions A_n et B_n de l'équation correspondante de Fermat soient connus.

Soit maintenant $r = pk - 1$, où p est un positif entier quelconque, on aura les formules récursives, dues à Lagrange[1],

$$(4)\qquad \begin{cases} A_{n+p} = A_n A_p + aB_n B_p \\ B_{n+p} = A_n B_p + B_n A_p \end{cases}$$

[1] Mémoires de l'Académie de Berlin 1767, p. 174—176 (1769).

et les formules inverses

$$(5)\qquad \begin{cases} A_p = (-1)^{nk}(A_n A_{n+p} - aB_n B_{n+p}) \\ B_p = (-1)^{nk}(A_n B_{n+p} - B_n A_{n+p}), \end{cases}$$

tandis que l'hypothèse $r = pk - 2$ donnera

$$(6)\qquad \begin{cases} a_{n+p} = A_n a_p + aB_n b_p \\ b_{n+p} = A_n b_p + B_n a_p \end{cases}$$

et les formules inverses

$$(7)\qquad \begin{cases} a_p = (-1)^{nk}(A_n a_{n+p} - aB_n b_{n+p}) \\ b_p = (-1)^{nk}(A_n b_{n+p} - B_n a_{n+p}). \end{cases}$$

Cela posé, les formules (4) donnent immédiatement, par la conclusion de m à $m+1$, ces autres formules générales, également dues à LAGRANGE[1],

$$(8)\qquad (A_r \pm \sqrt{a}B_r)^n = A_{nr} \pm \sqrt{a}B_{nr},$$

savoir

$$(9)\qquad \begin{cases} A_{nr} = \dfrac{(A_r + \sqrt{a}\,B_r)^n + (A_r - \sqrt{a}\,B_r)^n}{2} \\[2ex] B_{nr} = \dfrac{(A_r + \sqrt{a}\,B_r)^n - (A_r - \sqrt{a}\,B_r)^n}{2\sqrt{a}}; \end{cases}$$

de plus, on aura, en appliquant la formule binomiale,

$$(10)\qquad \begin{cases} A_{nr} = \displaystyle\sum_{s=0}^{\leqq \frac{n}{2}} \binom{n}{2s} A_r^{n-2s} B_r^{2s} a^s \\[3ex] B_{nr} = \displaystyle\sum_{s=0}^{\leqq \frac{n-1}{2}} \binom{n}{2s+1} A_r^{n-2s-1} B_r^{2s+1} a^s. \end{cases}$$

Or, ces deux dernières formules donnent immédiatement

[1] Loc. cit. pp. 226, 229.

deux propositions qui sont essentielles dans les recherches qui nous occupent ici, savoir:

I. Soit r et n des positifs entiers quelconques, B_{nr} est toujours divisible par B_r.

II. Tous les nombres A_{2nr+r} sont divisibles par A_r, tandis que A_{2nr} est toujours premier avec A_r.

On voit que le théorème I et la première partie du théorème II sont des conséquences immédiates des formules (10). Quant aux nombres A_{2nr}, on aura, en vertu de la première des formules (10), une expression de la forme

$$A_{2nr} = KA_r^2 + a^n B_r^{2n},$$

où K est un positif entier, et la formule

$$A_r^2 - aB_r^2 = (-1)^{rk} \tag{11}$$

montre clairement que A_r est premier et avec a et avec B_r.

Soit particulièrement $r = 1$, on voit que B_n est toujours divisible par B_1, et que A_{2n+1} est toujours divisible par A_1.

De plus, il est évident que les deux théorèmes susdits sont valables, quels que soient, dans (8), les positifs entiers A_r et B_r.

La publication la plus ancienne, où je me rappelle avoir vu le théorème I, est de GENOCCHI[1], mais, chose curieuse, dans l'»Educational Times«[2], on a proposé de démontrer que les B_{2n} sont divisibles par B_1, et les B_{2n+1}?

Posons maintenant, dans (4), $p = n$, il résulte

$$A_{2n} = A_n^2 + aB_n^2, \quad B_{2n} = 2A_nB_n, \tag{12}$$

d'où, en vertu de (11),

$$A_{2n} = 2A_n^2 - (-1)^{nk} = 2aB_n^2 + (-1)^{nk}, \tag{13}$$

ce qui donnera

[1] Annali di Mathematica (2) t. 2, p. 256—257; 1868.

[2] Jahrbuch über die Fortschritte der Mathematik, t. 7 (1875), p. 96.

(14) $A_{2n} + (-1)^{nk} = 2A_n^2, \quad A_{2n} - (-1)^{nk} = 2aB_n^2.$

Cela posé, soit a une base de première espèce, il résulte, en vertu de (12) et (13), que les plus petites solutions, x_1 et y_1, de l'équation

$$x^2 - ay^2 = 1,$$

savoir A_2 et B_2, se présentent nécessairement sous la forme

$$x_1 = 2n^2 + 1, \quad y_1 = 2nr.$$

Or, M. B. Niewenglouski[1] a démontré que cette condition nécessaire est suffisante aussi, afin que a soit une base de première espèce, savoir que l'équation

$$x^2 - ay^2 = -1$$

soit résoluble en positifs entiers.

Revenons maintenant aux formules (1), puis remplaçons n par $2n$, il résulte, en vertu de la première des formules (14),

$$\begin{aligned} y_{2nk+r} + (-1)^{nk} y_r &= 2A_n^2 y_r + 2aA_nB_n z_r \\ z_{nk+r} + (-1)^{nk} z_r &= 2A_n^2 z_r + 2A_nB_n y_r, \end{aligned}$$

ce qui donnera immédiatement

$$(15) \quad \left\{ \begin{aligned} y_{2nk+r} + (-1)^{nk} y_r &= 2A_n y_{nk+r} \\ z_{2nk+r} + (-1)^{nk} z_r &= 2A_n z_{nk+r}, \end{aligned} \right.$$

et l'on aura, en vertu de la dernière des formules (14), ces deux équations analogues aux précédentes

$$(16) \quad \left\{ \begin{aligned} y_{2nk+r} - (-1)^{nk} y_r &= 2aB_n z_{nk+r} \\ z_{2nk+r} - (-1)^{nk} z_r &= 2B_n y_{nk+r}. \end{aligned} \right.$$

Cela posé, appliquons la proposition I, il résulte, en vertu de la première des formules (16), cette autre proposition:

[1] Bulletin de la Société Mathématique de France, t. 35, p. 126—131; 1907.

III. Soit r un indice quelconque, on aura toujours

$$y_{2nk+r} \equiv (-1)^{nk} y_r \pmod{2aB_1}. \tag{27}$$

Soit maintenant, dans les formules (15) et (16), $r = pk - 1$, il résulte

$$\left\{\begin{aligned} A_{2n+p} + (-1)^{nk} A_p &= 2 A_n A_{n+p} \\ B_{2n+p} + (-1)^{nk} B_p &= 2 A_n B_{n+p} \end{aligned}\right. \tag{18}$$

$$\left\{\begin{aligned} A_{2n+p} - (-1)^{nk} A_p &= 2 a B_n B_{n+p} \\ B_{2n+p} - (-1)^{nk} B_p &= 2 B_n A_{n+p}, \end{aligned}\right. \tag{19}$$

tandis que l'hypothèse $r = pk - 2$ donnera de même

$$\left\{\begin{aligned} a_{2n+p} + (-1)^{nk} a_p &= 2 A_n a_{n+p} \\ b_{2n+p} + (-1)^{nk} b_p &= 2 A_n b_{n+p} \end{aligned}\right. \tag{20}$$

$$\left\{\begin{aligned} a_{2n+p} - (-1)^{nk} a_p &= 2 a B_n b_{n+p} \\ b_{2n+p} - (-1)^{nk} b_p &= 2 B_n a_{n+p}. \end{aligned}\right. \tag{21}$$

On voit que l'analogie entre les formules développées, pour les A_n et les B_n, et les formules fondamentales de la Trigonométrie est parfaite.

En effet, les formules (4) et (5) correspondent aux formules d'addition de $\cos(x \pm y)$ et de $\sin(x \pm y)$; de même, la formule (8) correspond à la formule de Moivre, tandis que les formules (18) et (19) sont analogues aux formules logarithmiques obtenues pour les expressions $\cos x \pm \cos y$ et $\sin x \pm \sin y$.

Or, dans l'article XII, nous avons à démontrer que cette analogie des formules susdites est une identité, parce que les A_n et les B_n sont, quelle que soit la base a, intimement liés aux polynomes de Cauchy.

VIII. Des nombres A_n et a_n.

Il est évident que les formules demontrées dans l'article précédent, donnent une suite de résultats intéressants concernant les nombres A_n et B_n.

Étudions tout d'abord les A_n, la première des formules (12) de l'article précédent, savoir

$$A_{2n} = A_n^2 + aB_n^2, \tag{1}$$

donnera immédiatement la proposition:

I. Le nombre $-a$ est résidu quadratique de tous les facteurs premiers de A_{2n}.

Appliquons ensuite la formule

$$A_{2n} = 2A_n^2 - (-1)^{nk}, \tag{2}$$

tirée directement de (1), il résulte de même:

II. Soit a une base de première espèce, et soit donc k un nombre impair, les facteurs premiers des A_{4n} sont tous de la forme $8\nu \pm 1$, tandis que les facteurs premiers des A_{4n+2} sont de la forme $8\nu + 1$ ou $8\nu + 3$.

III. Soit a une base de seconde espèce, et soit donc k un nombre pair, les facteurs premiers des A_{2n} sont tous de la forme $8\nu \pm 1$.

Appliquons ensuite les formules (14) et (19) de l'article précédent, savoir

$$A_{2n} - (-1)^{nk} = 2aB_n^2$$

$$A_{2n+1} - (-1)^{nk}A_1 = 2aB_nB_{n+1},$$

puis remarquons que les B_m sont tous divisibles par B_1, nous aurons:

IV. Les nombres A_m satisfont, quelle que soit la bas a, aux congruences

$$
(3) \qquad \begin{cases} A_{2n} \equiv (-1)^{nk} & (\text{mod } 2aB_1^2) \\ A_{2n+1} \equiv (-1)^{nk} A_1 & (\text{mod } 2aB_1^2). \end{cases}
$$

Or, il est bien curieux, ce me semble, que les nombres a_n, savoir les y_{nk-2}, satisfassent à des congruences analogues à (3).

En effet, la première des formules (21) de l'article précédent donnera, pour $p = 1$,

$$
a_{2n+1} - (-1)^{nk} a_1 = 2aB_1 b_{n+1};
$$

appliquons ensuite la formule (7) de l'article II, savoir

$$
aB_m = \alpha A_m + a_m,
$$

il résulte pour $m = 2n$,

$$
2aA_n B_n = \left(A_{2n} \pm (-1)^{nk}\right)\alpha + \left(a_{2n} \pm (-1)^{nk}\alpha\right),
$$

et nous aurons donc, en vertu du théorème précédent:

V. Les nombres $a_m = y_{mk-2}$ satisfont, quelle que soit la base a, aux congruences

$$
(4) \qquad \begin{cases} a_{2n} \equiv (-1)^{nk-1}\alpha & (\text{mod } 2aB_1) \\ a_{2n+1} \equiv (-1)^{nk} a_1 & (\text{mod } 2aB_1). \end{cases}
$$

La première de ces deux congruence est bien remarquable en comparaison avec la congruence (14) de l'article II.

Quant aux deux derniers théorèmes, il est évident que les deux congruences contenant les A_m et les a_m présentent une différence essentielle, selon que la base a est de première ou de seconde espèce.

En effet, soit a une base de première espèce, et soit donc le nombre caractéristique k impair, nous connaissons dès à présent le reste modulo $2aB_1$ de tous les x et de tous les a_m, tirés de l'équation

$$
(5) \qquad x^2 - ay^2 = 1.
$$

Soit, au contraire, a une base de seconde espèce, et soit donc le nombre caractéristique k pair, nous ne connaissons dès à présent que les restes modulo $2aB_1$ des A_{2n} et des a_{2n} tirés de l'équation correspondante (5). Quant aux restes des A_{2n+1} et des a_{2n+1}, il ne sont pas généralement égaux à ± 1 ou à $\pm \alpha$, mais ces restes fixes se présentent certainement dans le cas spécial, où la base a est une puissance impaire d'un nombre premier impair, cas spécial que nous avons à étudier plus amplement ici.

A cet effet, remarquons tout d'abord que LEGENDRE[1] a démontré qu'un nombre premier de la forme $4\nu + 1$ est toujours une base de première espèce, nous avons à généraliser, dans l'article X, ce théorème, en démontrant que la puissance

$$a = (4\nu + 1)^{2\varrho+1}, \quad \varrho \geqq 0, \tag{6}$$

a la même propriété. De plus, nous démontrerons directement, dans l'article XXIII, que la puissance (6) du nombre premier $4\nu + 1$ est toujours une base de première espèce.

Cela posé, il résulte immédiatement des théorèmes IV et V:

VI. Pour la base $a = (4\nu + 1)^{2\varrho+1}$, où $4\nu + 1$ est un nombre premier, on aura les congruences

$$\left\{\begin{aligned} A_{2n} &\equiv (-1)^n \pmod{a} \\ a_{2n} &\equiv (-1)^{n-1}\alpha \pmod{a} \end{aligned}\right. \tag{7}$$

$$\left\{\begin{aligned} A_{2n+1} &\equiv (-1)^n A_1 \pmod{a} \\ a_{2n+1} &\equiv (-1)^n a_1 \pmod{a}. \end{aligned}\right. \tag{8}$$

Quant au nombre premier $4\nu + 3$, il est toujours une base de seconde espèce, parce qu'il ne peut jamais diviser la somme $x^2 + 1$, et il est évident que la puissance

[1] Théorie des Nombres, t. I, p. 65; 3e édition, Paris 1830.

$$(9) \qquad a = (4\nu + 3)^{2\varrho+1} \quad \varrho \geqq 0,$$

est aussi une base de seconde espèce.

Or, dans ce cas, l'équation de FERMAT

$$(A_1 + 1)(A_1 - 1) = aB_1^2$$

donnera une congruence de la forme

$$(10) \qquad A_1 \equiv (-1)^{\varepsilon} \pmod{a},$$

où l'exposant ε est facile à déterminer. En effet, il résulte, en vertu de la première des formules (23) de l'article IV,

$$y_{\mu-1}^2 + (-1^{\nu} - (-1)^{\varepsilon} \equiv 0 \pmod{a},$$

tandis que la première des formules (25) de l'article IV donnera

$$y_{\mu-1}^2 + (-1)^{\nu} 2 \equiv 0 \pmod{a}.$$

Cela posé, on aura pour l'exposant ε qui figure dans la congruence (10)

$$\varepsilon = \nu - 1.$$

Appliquons ensuite l'identité

$$aB_1 = \left(A_1 + (-1)^{\nu}\right)\alpha + \left(a_1 - (-1)^{\nu}\alpha\right),$$

tirée directement de la formule (7) de l'article II, nous aurons cet autre théorème, supplémentaire au précédent:

VII. Pour la base $a = (4\nu + 3)^{2\varrho+1}$, où $4\nu + 3$ est un nombre premier, on aura les congruences

$$(11) \qquad \begin{cases} A_n \equiv (-1)^{n\nu+n} & \pmod{a} \\ a_n \equiv (-1)^{n\nu+n-1}\alpha & \pmod{a}. \end{cases}$$

IX. Des nombres B_n.

Les nombres B_n qui correspondent à une base quelconque, savoir les valeurs de y, tirées de l'équation de FERMAT

$$x^2 - a y^2 = \pm 1, \tag{1}$$

présentent un intérêt particulier, parce qu'ils admettent un algorithme analogue à celui de la division ordinaire, mais notamment parce qu'ils donnent naissance aux rangs des nombres entiers, essentiels dans la théorie de l'équation de FERMAT,

Quant aux formules de ce genre, en partie déjà connues, et aux autres que nous avons à déduire, nous prenons pour point de départ l'équation de FERMAT, analogue à (1),

$$u^2 - a p^2 v^2 = \pm 1, \tag{2}$$

ou p désigne un positif entier quelconque, équation déjà mentionnée dans l'article I, afin d'établir qu'un positif entier quelconque divise une infinité des nombres B_n, problème que nous avons à étudier plus amplement dans l'article présent et dans celui qui suit.

A cet égard, nous avons tout d'abord à introduire une définition qui facilite les démonstrations, en simplifiant la terminologie.

En effet, soit p un positif entier quelconque, et soit B_r le plus petit des nombres B_m qui soit divisible par p, nous disons que p est, pour la base a, du rang r.

Soient maintenant

$$u = \alpha_1, \quad v = \beta_1 \tag{3}$$

les plus petites solutions en positifs entiers de l'équation (2), il existe, en vertu de (1), un indice r, tel que

$$\alpha_1 = A_r, \quad p\beta_1 = B_r, \tag{4}$$

et p est donc du rang r, parce que p ne peut diviser aucun B_m plus petit que B_r.

Remarquons ensuite que les solutions générales α_n et β_n de l'équation (2) se déterminent par la formule

$$(\alpha_1 \pm p\sqrt{a}\,\beta_1)^n = \alpha_n \pm p\sqrt{a}\,\beta_n,$$

ce qui n'est, en vertu de (4), autre chose que celle-ci

$$(A_r \pm \sqrt{a}\,B_r)^n = A_{nr} \pm \sqrt{a}\,B_{nr},$$

donc nous aurons, quel que soit l'indice n,

$$\alpha_n = A_{nr}, \quad p\beta_n = B_{nr}, \tag{5}$$

ce qui donnera le théorème essentiel:

I. Soit le positif entier p, quelconque du reste, du rang r pour la base a, les B_{nr} représentent l'ensemble des B_m qui sont divisibles par p, et les solutions générales de l'équation (2) sont déterminées par les formules (5).

Appliquons maintenant les formules récursives de Lagrange

$$B_{m+n} = A_n B_m + B_n A_m$$
$$(-1)^{nk} B_{m-n} = A_n B_m - B_n A_m,$$

où k est le nombre caractéristique de la base a, nous aurons immédiatement les deux propositions suivantes:

II. Un diviseur commun de B_m et de B_n est aussi diviseur des deux nombres $B_{m\pm n}$.

III. Soit f le plus grand commun diviseur des indices m et n, un diviseur commun quelconque des nombres B_m et B_n est aussi diviseur de B_f.

En effet, soit tout d'abord m divisible par n, n est le plus grand commun diviseur de m et n, et la proposition est évidente.

Soit ensuite

$$m = nq + s, \quad 0 < s < n,$$

et soit p un diviseur commun de B_m et B_n, il résulte, en vertu de I et II, que p est aussi diviseur de B_s, et ainsi de suite.

Cela posé, nous aurons de plus la proposition:

IV. Soient r et s les rangs de p et de q, et soit n le plus petit commun multiple de r et s, le produit pq est du rang n.

Soit, en effet, B_m divisible et par p et par q, l'indice m est aussi divisible et par r et par s, et il est évident que le produit pq est du rang n.

Remarquons ensuite que B_r est le plus grand de tous les nombres du rang r, il résulte, en vertu de II, III, IV:

V. Soit B_m divisible par B_n, l'indice m est divisible par l'indice n, et inversement.

VI. Soit M le plus petit commun multiple des indices m et n, le produit $B_m B_n$ est du rang M.

VII. Soit f le plus grand commun diviseur des indices m et n, B_f est le plus grand commun diviseur de B_m et B_n.

Quelques-uns de ces théorèmes concernant les nombres B_m et B_n sont bien connus,[1] mais on ne semble pas avoir remarqué jusqu'ici qu'ils sont des cas particuliers d'autres théorèmes beaucoup plus généraux.

Quant à la base a, nous aurons à démontrer le théorème:

VIII. Le diviseur p de la base a est précisément du rang p, pourvu que p et B_1 soient premiers entre eux.

En effet, soit, dans la dernière des formules (10) de l'article VIII, $r = 1$, on aura une expression de la forme

$$B_n = nA_1^{m-1}B_1 + aK,$$

où K est un positif entier. Or, remarquons que p est premier et avec A_1 et avec B_1, il est évident que B_n n'est

[1] Voir P. Bachmann: Niedere Zahlentheorie, t. II, p. 80; Leipsic 1910.

divisible par p que dans le cas, où n est divisible par p; c'est-à-dire que p est précisément du rang p.

Nous avons encore à démontrer un théorème essentiel concernant les nombres A_m, savoir:

IX. La nombre A_r, supposé plus grand que l'unité, est du rang $2r$, et les nombres B_{2nr} et A_{2nr+r} représentent les ensembles des nombres B_m et A_m qui sont divisibles par A_r.

La formule

$$B_{2r} = 2A_r B_r$$

montre clairement que B_{2r} est toujours divisible par A_r. Supposons maintenant que B_m, où $m < 2r$, soit divisible par A_r, nous aurons nécessairement $m > r$, parce que $A_r > B_r$. Soit ensuite $m = r + s$, on aura donc $0 < s < r$, et la formule

$$B_{r+s} = B_r A_s + A_r B_s,$$

où A_r et B_r sont premiers entre eux, montre clairement que A_s est divisible par A_r, pourvu que B_{r+s} le soit, ce qui est impossible.

Cela posé, il ne nous reste évidemment qu'à démontrer que les A_{2nr+r} sont les seuls nombres A_m qui soient divisibles par A_r.

Or, nous savons déjà, d'après le théorème II de l'article VII, que les A_{2nr+r} sont tous divisibles par A_r. Soit ensuite A_m divisible par A_r, je dis que le nombre A_{m+s}, où $0 < s < 2r$, ne peut jamais être divisible par A_r, ce qui est une conséquence immédiate de la formule

$$A_{m+s} = A_m A_s + aB_m B_s,$$

parce que A_r est premier et avec a et avec B_m; du plus A_r est du rang $2r$, de sorte que B_s ne peut pas être divisible par A_r.

X. Du rang d'un nombre entier.

Le rang d'un positif entier que nous venons d'introduire, dans l'article précédent, joue un rôle si important dans la théorie de l'équation de FERMAT qu'il nous semble utile de développer une suite de théorèmes concernant cette idée.

I. *Soit m le rang du nombre premier p, et soit B_m divisible précisément par p^{ϱ}, la puissance p^r, où $r > \varrho$, est du rang $mp^{r-\varrho}$.*

La dernière des formules (10) de l'article VII se présentant sous la forme

$$B_{mn} = B_m (n A_m^{n-1} + B_m^2 K), \tag{1}$$

où K est un positif entier, il est évident que B_{mn} n'est divisible par $p^{\varrho+1}$ que dans le cas, où n est divisible par p; c'est-à-dire que $p^{\varrho+1}$ est du rang mp. Remplaçons maintenant, dans (1), m par mp, il résulte que $p^{\varrho+2}$ est du rang mp^2, et ainsi de suite.

Mais comment déterminer les deux nombres m et ϱ, parfaitement définis, pourvu que a et p soient donnés?

On aura immédiatement, comme corollaire du théorème I, la proposition:

II. *Soit le nombre premier impair p du rang impair, une puissance quelconque de p est aussi du rang impair.*

Considérons maintenant une base a de première espèce, puis supposons que le positif entier p soit du rang m, les deux nombres

$$C_1 = A_m, \; D_1 = \frac{B_m}{p}$$

satisfont à l'équation de FERMAT

$$C_1^2 - (ap^2) D_1^2 = (-1)^m,$$

ce qui donnera le théorème:

III. Soit a une base de première espèce, le nombre ap^2 est une base de première ou de seconde espèce, selon que le rang de p est un nombre impair ou pair.

On aura, comme corollaire de ce théorème, la proposition:

IV. Soit a une base de première espèce, le nombre aB_{2n+1}^2 a toujours la même propriété, tandis que tous les nombres aA_n^2 sont des bases de seconde espèce.

En se rappelant que Legendre[1] a démontré qu'un nombre premier de la forme $4\nu + 1$ est toujours une base de première espèce, il résulte, en vertu de II, un théorème essentiel que nous venons de mentionner, dans l'article VIII, et que nous avons à démontrer, d'un autre point de vue, dans l'article XXIII, savoir:

V. Soit $4\nu + 1$ un nombre premier, la puissance $(4\nu + 1)^{2\varrho+1}$ est toujours une base de première espèce.

En effet, soit $a = 4\nu + 1$, on voit, en vertu de la formule

$$B_n = nA_1^{n-1}B_1 + aK,$$

appliquée dans l'article précédent, que a est ou du rang 1 ou du rang $4\nu + 1$, de sorte que le rang de a est toujours un nombre impair.

VI. Un nombre du rang impair ne peut diviser aucun des nombres A_m, de sorte que deux nombres A_m et B_{2n+1} sont toujours premiers entre eux, quels que soient leurs indices.

Soit $2r + 1$ le rang de p, et soit A_m divisible par p, il est évident que B_{2m} est aussi divisible par p, de sorte que

[1] Théorie des Nombres, t. I, p. 65; 3[e] édition; Paris 1830.

$2m$, savoir m, est nécessairement divisible par $2r+1$, ce qui entraîne que B_m soit divisible par p, supposition impossible, parce que A_m et B_m sont premiers entre eux.

Cela posé, il est évident qu'un nombre premier qui divise B_{2n+1} ne peut diviser aucun A_m.

VII. Soit p un nombre premier impair, et soit la puissance p^ϱ du rang pair $2r$, les B_{2nr} et les A_{2nr+r} représentent l'ensemble des A_m et des B_m qui sont divisibles par p^ϱ.

Il est évident que B_r ne peut pas être divisible par p^ϱ, parce que cette puissance est du rang $2r$; soit donc B_r divisible par $p^{\varrho-\sigma}$, il resulte, en vertu de la formule

$$B_{2r} = 2A_rB_r,$$

que A_r est divisible par p^σ, ce qui est impossible, parce que A_r et B_r sont premiers entre eux; c'est-à-dire que B_r ne peut pas être divisible par p, donc A_r est divisible par p^ϱ, et les A_{2nr+r} sont tous divisibles par A_r.

VIII. Soit a une base de première espèce, un nombre de la forme $4\nu+3$ est toujours du rang pair.

En effet, un nombre de la forme $4\nu+3$ contient au moins un facteur premier de la même forme, et un tel nombre premier ne peut jamais diviser la somme x^2+1.

CHAPITRE III

Les polynomes de Cauchy et l'équation de Fermat.

XI. De la base $a = \alpha^2 + 1$.

Soit particulièrement, dans l'équation de FERMAT,

$$x^2 - ay^2 = \pm 1, \tag{1}$$

$B_1 = 1$, plusieurs des théorèmes de l'article IX se présentent sous une forme très simple.

On aura par exemple, en vertu du théorème VII de l'article susdit:

I. Soient les deux indices n et p premiers entre eux, les deux nombres B_n et B_p auront la même propriété, et inversement.

De plus, le théorème VIII de l'article IX donnera:

II. Un diviseur quelconque p de la base a est précisément du rang p.

Quant à l'équation (1) qui est satisfaite par $y = 1$, il est évident que la base a se présente sous la forme

$$a = \alpha^2 \pm 1, \tag{2}$$

où α est la valeur positive entière de x qui correspond à $y = 1$.

Cela posé, nous avons tout d'abord à étudier la valeur $\alpha^2 + 1$; la fraction continue correspondante, savoir

$$\sqrt{\alpha^2 + 1} = \left[\alpha, (2\alpha)\right], \quad \alpha \geqq 1, \tag{3}$$

a les réduites

$$(4) \qquad \frac{\alpha}{1},\ \frac{2\alpha^2+1}{2\alpha},\ \frac{4\alpha^3+3\alpha}{4\alpha^2+1},\ \frac{8\alpha^4+8\alpha^2+1}{8\alpha^3+4\alpha},\ \ldots,$$

dont les numérateurs $\varphi_n(\alpha)$ et les dénominateurs $\psi_n(\alpha)$ représentent, pour $n = 1, 2, 3, \ldots,$ l'ensemble des polynomes entiers qui satisfont à l'identité algébrique

$$(5) \qquad \varphi_n^2(\alpha) - (\alpha^2+1)\,\psi_n^2(\alpha) = (-1)^n.$$

De plus, la définition même des polynomes $\varphi_n(\alpha)$ et $\psi_n(\alpha)$ donnera les formules récursives

$$(6) \qquad \begin{cases} \varphi_n(\alpha) = 2\alpha\,\varphi_{n-1}(\alpha) + \varphi_{n-2}(\alpha) \\ \psi_n(\alpha) = 2\alpha\,\psi_{n-1}(\alpha) + \psi_{n-2}(\alpha), \end{cases}$$

d'où il résulte, par la conclusion de n à $n+1$, ces autres identités

$$(7) \qquad \begin{cases} \psi_{n+1}(\alpha) + \psi_{n-1}(\alpha) = 2\,\varphi_n(\alpha) \\ \psi_{n+1}(\alpha) - \psi_{n-1}(\alpha) = 2\alpha\,\psi_n(\alpha) \end{cases}$$

$$(8) \qquad \varphi_n(\alpha) \pm \alpha\,\psi_n(\alpha) = \psi_{n\pm 1}(\alpha).$$

Appliquons ensuite les formules générales, développées dans l'article III, nous aurons

$$(9) \qquad \varphi_{2n}(\alpha) = 2\,\varphi_n^2(\alpha) - (-1)^n$$

$$(10) \qquad \psi_{2n}(\alpha) = 2\,\varphi_n(\alpha)\,\psi_n(\alpha).$$

Quant aux polynomes $\varphi_{2n+1}(\alpha)$ et $\psi_{2n+1}(\alpha)$, remarquons que les formules récursives (6) se présentent sous la forme

$$\begin{aligned} \varphi_n(\alpha) &= \psi_2(\alpha)\,\varphi_{n-1}(\alpha) + \psi_1(\alpha)\,\varphi_{n-2}(\alpha) \\ \psi_n(\alpha) &= \psi_2(\alpha)\,\psi_{n-1}(\alpha) + \psi_1(\alpha)\,\psi_{n-2}(\alpha), \end{aligned}$$

la conclusion de p à $p+1$ donnera les formules générales

$$\begin{aligned} \varphi_n(\alpha) &= \psi_p(\alpha)\,\varphi_{n-p+1}(\alpha) + \psi_{p-1}(\alpha)\,\varphi_{n-p}(\alpha) \\ \psi_n(\alpha) &= \psi_p(\alpha)\,\psi_{n-p+1}(\alpha) + \psi_{p-1}(\alpha)\,\psi_{n-p}(\alpha), \end{aligned}$$

d'où, en posant $n = m + p$,

$$(11)\quad \begin{cases} \varphi_{m+p}(\alpha) = \psi_p(\alpha)\,\varphi_{m+1}(\alpha) + \psi_{p-1}(\alpha)\,\varphi_m(\alpha) \\ \psi_{m+p}(\alpha) = \psi_p(\alpha)\psi_{m+1}(\alpha) + \psi_{p-1}(\alpha)\psi_m(\alpha). \end{cases}$$

Soit particulièrement $p = m + 1$, il résulte, en vertu de (11), si nous remplaçons m par n,

$$(12)\quad \begin{cases} \varphi_{2n+1}(\alpha) = \varphi_{n+1}(\alpha)\psi_{n+1}(\alpha) + \varphi_n(\alpha)\psi_n(\alpha) \\ \psi_{2n+1}(\alpha) = \psi^2_{n+1}(\alpha) + \psi^2_n(\alpha), \end{cases}$$

formules qui correspondent aux deux premières des formules (12 bis) de l'article III. Quant à la troisième de ces formules, elle devient ici

$$(12\text{ bis})\qquad (\alpha^2+1)\,\psi_{2n+1}(\alpha) = \varphi^2_{n+1}(\alpha) + \varphi^2_n(\alpha),$$

d'où, en vertu de (9),

$$(13)\qquad 2(\alpha^2+1)\,\psi_{2n+1}(\alpha) = \varphi_{2n+2}(\alpha) + \varphi_{2n}(\alpha),$$

savoir la première des formules logarithmiques (19) de l'article VII.

Multiplions ensuite les deux formules (7), il résulte

$$(14)\qquad 2\alpha\,\psi_{2n}(\alpha) = \psi^2_{n+1}(\alpha) - \psi^2_{n-1}(\alpha),$$

tandis que l'identité (5), écrite sous la forme

$$\big(\varphi_n(\alpha) + \alpha\,\psi_n(\alpha)\big)\big(\varphi_n(\alpha) - \alpha\,\psi_n(\alpha)\big) = \psi^2_n(\alpha) + (-1)^n,$$

donnera, en vertu des formules (8),

$$(15)\qquad \psi_{n+1}(\alpha)\,\psi_{n-1}(\alpha) = \psi^2_n(\alpha) + (-1)^n,$$

d'où, en supposant n pair, puis remplaçant n par $2n$:

III. Soit α un positif entier quelconque, le produit

$$(16)\qquad \psi_{2n+1}(\alpha)\psi_{2n-1}(\alpha) = \psi^2_{2n}(\alpha) + 1$$

est toujours une base de première espèce, et les solutions générales de l'équation de correspondante de Fermat se présentent sous la forme

$$A_m = \varphi_m(\beta),\ B_m = \psi_m(\beta),\ \beta = \psi_{2n}(\alpha). \tag{17}$$

Remarquons, en passant, qu'on cherchera en vain à démontrer que le nombre $\psi_{2n+1}(\alpha)$ est toujours une base de première espèce, parce qu'il peut arriver que $\psi_{2n+1}(\alpha)$ soit un carré, nous le verrons par exemple dans l'article XIX.

Appliquons ensuite, au premier membre de (16), la dernière des formules (12), il résulte, après un simple calcul,

$$\left(\psi_{n+1}(\alpha) \pm \psi_{n-1}(\alpha)\right)^2 \psi_n^2(\alpha) + \left(\psi_{n+1}(\alpha)\psi_{n-1}(\alpha) \pm \psi_n^2(\alpha)\right)^2 = \\ = \psi_{2n}^2(\alpha) + 1.$$

On voit, en vertu des formules (7) et (15), que les signes supérieurs donnent une identité formelle, tandis qu'il résulte, en vertu de (7), pour les signes inférieurs, la formule curieuse

$$4\alpha^2\psi_n^4(\alpha) + \left(2\psi_n^2(\alpha) + (-1)^n\right)^2 = \psi_{2n}^2(\alpha) + 1, \tag{18}$$

qui se présente, dans le cas spécial $\alpha = 1$, et seulement dans ce cas, sous une forme très élégante. Dans l'article XVIII nous avons à citer la formule singulière ainsi obtenue.

Quant à la dernière des formules (12), remarquons que Catalan[1] a démontré que, dans l'équation indéterminée

$$(\alpha^2 + 1)x^2 = y^2 + 1,$$

le nombre x est toujours la somme de trois carrés. On aura, en effet,

$$x = \psi_{4n\pm 1}(\alpha) = \psi_{2n\pm 1}^2(\alpha) + \psi_{2n}^2(\alpha),$$

[1] Atti della Accademia Pontificia dei Nuovi Lincei, t. 37, p. 49—114; 1885. Citation d'après le Jahrbuch über die Fortschritte der Mathematik, t. 17 (1885), p. 133.

ce qui donnera

$$x = \psi_{2n}^2(\alpha) + \left(\psi_n^2(\alpha) - \psi_{n\pm1}^2(\alpha)\right)^2 + \left(2\psi_n(\alpha)\psi_{n\pm1}(\alpha)\right)^2,$$

mais j'ignore si cette formule est identique à celle de CATALAN.

Nous avons encore à mentionner ici que la fraction continue de SEELING, définie par la formule (15) de l'article II, conduira à un résultat intéressant, si nous remplaçons α par 2α, puis posons $\beta = \alpha$. On aura, en effet, en vertu des formules (16) et (17) de l'article II, pour les numérateurs et les dénominateurs des réduites de la fraction continue

$$\sqrt{4\alpha^2 + 4} = \left[2\alpha,\ (2\alpha,\ 4\alpha)\right],$$

les deux relations

$$y_{2n+1}^2 - (4\alpha^2 + 4)\ z_{2n+1}^2 = 1$$
$$y_{2n}^2 - (4\alpha^2 + 4)\ z_{2n}^2 = -4;$$

c'est-à-dire que y_{2n} est toujours divisible par 2, ce qui donnera, en vertu de (5), la proposition curieuse:

IV. Une réduite quelconque de la fraction continue $\left[2\alpha, (\alpha, 4\alpha)\right]$ est précisément le double de la réduite au même indice de la fraction continue $\left[\alpha, (2\alpha)\right]$.

Revenons maintenant aux formules récursives (6), puis supposons α égal à un positif entier, il est évident que les $\varphi_n(\alpha)$ et les $\psi_n(\alpha)$ deviennent, quel que soit l'indice n, des positifs entiers. Or, la conclusion de n à $n+1$ donnera immédiatement la proposition, essentielle dans l'étude de plusieurs équations indéterminées:

V. Soit p un positif entier quelconque, les nombres $\psi_n\left(\frac{p}{2}\right)$, sont aussi, quel que soit l'indice n, des positifs entiers.

Cela posé, nous avons à étudier l'idéntité

$$\varphi_n(\alpha)\,\psi_{n-1}(\alpha) - \varphi_{n-1}(\alpha)\,\psi_n(\alpha) = (-1)^n, \tag{19}$$

tirée directement de la définition des $\varphi_n(\alpha)$ et des $\psi_n(\alpha)$ comme les numérateurs respectivement les dénominateurs des réduites (4),

A cet effet, posons, en vertu de (8),

$$\varphi_n(\alpha) = \alpha\,\psi_n(\alpha) + \psi_{n-1}(\alpha),\ \varphi_{n-1}(\alpha) = \psi_n(\alpha) - \alpha\,\psi_{n-1}(\alpha),$$

il résulte, après un simple calcul,

$$\psi_n^2(\alpha) - 2\,\alpha\,\psi_n(\alpha)\psi_{n-1}(\alpha) - \psi_{n-1}^2(\alpha) = (-1)^{n-1}, \tag{20}$$

ce qui donnera le théorème:

VI. L'équation indéterminée

$$x^2 - pxy - y^2 = \pm 1, \tag{21}$$

où p désigne un positif entier quelconque, admet une infinité de solutions en positifs entiers x_n et y_n, déterminées, à l'aide des valeurs initiales

$$x_1 = p,\ y_1 = 1, \tag{22}$$

par les formules récursives

$$x_{n+1} = px_n + y_n,\ y_{n+1} = x_n. \tag{22 bis}$$

En effet, posons, dans (19),

$$\alpha = \frac{p}{2},$$

il résulte, comme solutions de l'équation (21),

$$x_n = \psi_{n+1}\left(\frac{p}{2}\right),\ y_n = \psi_n\left(\frac{p}{2}\right),$$

ce qui donnera, en vertu de la dernière des formules récursives (6), les valeurs indiquées par les formules (22).

Inversement, l'équation indéterminée proposée, savoir

$$x_n^2 - p x_n y_n - y_n^2 = (-1)^n,$$

donnera

$$(23) \qquad x_n = \frac{p y_n}{2} + \sqrt{\left(\left(\frac{p}{2}\right)^2 + 1\right) y_n^2 + (-1)^n},$$

de sorte que nous aurons l'équation de Fermat

$$z_n^2 - \left(\left(\frac{p}{2}\right)^2 + 1\right) y_n^2 = (-1)^n,$$

satisfaite par

$$z_n = \varphi_n\left(\frac{p}{2}\right), \; y_n = \psi_n\left(\frac{p}{2}\right),$$

et il résulte donc, en vertu de (23),

$$x_n = \frac{p}{2}\psi_n\left(\frac{p}{2}\right) + \varphi_n\left(\frac{p}{2}\right) = \psi_{n+1}\left(\frac{p}{2}\right);$$

c'est-à-dire que les formules (22) représentent toutes les solutions en positifs entiers de l'équation indéterminée (21).

Étudions maintenant la seconde des bases, indiquées dans la formule (2), savoir

$$a = \alpha^2 - 1,$$

les réduites de la fraction continue correspondante, savoir

$$(24) \qquad \sqrt{\alpha^2 - 1} = \left[\alpha - 1, (1, 2\alpha - 2)\right], \; \alpha \geqq 2,$$

deviennent

$$(25) \quad \frac{\alpha - 1}{1}, \frac{\alpha}{1}, \frac{2\alpha^2 - \alpha - 1}{2\alpha - 1}, \frac{2\alpha^2 - 1}{2\alpha}, \frac{4\alpha^3 - 2\alpha^2 - 3\alpha + 1}{4\alpha^2 - 2\alpha - 1}.$$

Cela posé, désignons par $\zeta_n(\alpha)$ et $\eta_n(\alpha)$ les numérateurs et les dénominateurs des réduites (25) qui correspondent à des indices impairs, les $\zeta_n(\alpha)$ et les $\eta_n(\alpha)$, ainsi définis, représentent l'ensemble des polynomes entiers qui satisfont à l'identité algébrique

$$(26) \qquad \zeta_n^2(\alpha) - (\alpha^2 - 1)\,\eta_n^2(\alpha) = 1,$$

de sorte que nous aurons, en vertu de (5),

$$(27) \qquad \zeta_n(\alpha) = i^{-n}\varphi_n(i\alpha), \quad \eta_n(\alpha) = i^{1-n}\psi_n(i\alpha).$$

Quant aux polynomes $\varphi_n(\alpha)$ et $\psi_n(\alpha)$, $\zeta_n(\alpha)$ et $\eta_n(\alpha)$, il est très intéressant qu'ils nous permettent de déterminer toutes les solutions de l'équation générale de FERMAT,

$$(28) \qquad A_m^2 - a B_m^2 = (-1)^{mk},$$

pourvu que les premières de ces solutions, savoir les A_1 et les B_1, soient connues.

Cette propriété essentielle des polynomes susdits se présente, en effet, comme cas très spécial du théorème:

VII. Soient r et n des indices quelconques, on aura, pour les solutions générales de l'equation de Fermat,

$$(29) \qquad A_{nr} = \zeta_n(A_r), \quad B_{nr} = B_r \eta_n(A_r)$$

respectivement

$$(29\text{ bis}) \qquad A_{nr} = \varphi_n(A_r), \quad B_{nr} = B_r \psi_n(A_r),$$

selon que rk est pair ou impair.

A cet effet, remarquons tout d'abord que B_{nr} est divisible par B_r, puis posons

$$A_{nr} = C_n, \quad B_{nr} = B_r D_n,$$

il résulte, en vertu de (28),

$$(30) \qquad C_n^2 - \left(a B_r^2\right) D_n^2 = (-1)^{nrk},$$

De plus, nous aurons

$$A_r^2 - a B_r^2 = (-1)^{rk},$$

de sorte que l'équation (30) se transforme en celle-ci

$$(31) \qquad C_n^2 - \left(A_r^2 - (-1)^{rk}\right) D_n^2 = (-1)^{nrk},$$

et les expressions générales (29) sont évidentes.

Soit particulièrement $r = 1$, il résulte donc

$$(32) \qquad A_n = \zeta_n(A_1), \; B_n = B_1\, \eta_n(A_1)$$

respectivement

$$(32 \text{ bis}) \qquad A_n = \varphi_n(A_1), \; B_n = B_1 \psi_n(A_1)$$

selon que k est pair ou impair.

Le théorème VII, intéressant en lui-même, conduira à des résultats très remarquables, nous le verrons, dans l'article qui suit.

XII. Analogies des formules trigonométriques.

Revenons maintenant aux polynomes $\zeta_n(\alpha)$ et $\eta_n(\alpha)$, les valeurs des premiers de ces polynomes, savoir

$$\begin{aligned}
\zeta_0(\alpha) &= 1 & \eta_0(\alpha) &= 0 \\
\zeta_1(\alpha) &= \alpha & \eta_1(\alpha) &= 1 \\
\zeta_2(\alpha) &= 2\alpha^2 - 1 & \eta_2(\alpha) &= 2\alpha \\
\zeta_3(\alpha) &= 4\alpha^3 - 3\alpha & \eta_3(\alpha) &= 4\alpha^2 - 1 \\
\zeta_4(\alpha) &= 8\alpha^4 - 4\alpha^2 + 1 & \eta_4(\alpha) &= 8\alpha^3 - 4\alpha,
\end{aligned}$$

suppléées par les deux formules récursives

$$\begin{aligned}
\zeta_n(\alpha) &= 2\alpha\,\zeta_{n-1}(\alpha) - \zeta_{n-2}(\alpha) \\
\eta_n(\alpha) &= 2\alpha\,\eta_{n-1}(\alpha) - \eta_{n-2}(\alpha),
\end{aligned}$$

tirées directement des formules (6) et (27) de l'article précédent, donnent immédiatement, par la conclusion de n à $n+1$, le théorème essentiel:

I. Posons $\alpha = \cos x$, où x est une variable complexe quelconque, nous aurons, quel que soit l'indice n,

$$(1) \qquad \zeta(\cos x) = \cos nx, \;\; \eta_n(\cos x) = \frac{\sin nx}{\sin x}.$$

Cela posé, appliquons les identités

$$(2) \qquad \varphi_n(\alpha) = i^{-n}\zeta_n(i\alpha), \;\; \psi_n(\alpha) = i^{1-n}\eta_n(i\alpha),$$

savoir les formules (27) de l'article précédent, il est évident que les formules (1) donnent, en vertu du théorème VII de l'article précédent, une suite de formules concernant les solutions générales de l'équation de FERMAT

$$A_m^2 - a B_m^2 = (-1)^{mk}. \tag{3}$$

A cet effet, nous posons, dans ce qui suit, pour abréger et conformément aux significations appliquées dans le théorème VII de l'article précédent,

$$rk = \varepsilon. \tag{4}$$

En premier lieu, prenons pour point de départ les formules qui expriment, sous forme des polynomes entiers de $\cos x$, les fonctions (1), puis remplaçons $\cos x$ par A_r, il résulte les formules générales

$$\left\{\begin{aligned} A_{nr} &= 2^{n-1} A_r^n + \sum_{s=1}^{\leq \frac{n}{2}} \frac{(-1)^{s\varepsilon+s}\, n}{2s} \binom{n-s-1}{s-1} (2A_r)^{n-2s} \\ B_{nr} &= B_r \sum_{s=0}^{\leq \frac{n-1}{2}} (-1)^{s\varepsilon+s} \binom{n-s-1}{s} (2A_r)^{n-2s-1}. \end{aligned}\right. \tag{5}$$

Soit particulièrement $r = 1$, les formules (5) nous permettent de déterminer les A_n et les B_n, directement à l'aide de A_1 et de B_1, ce qui n'a pas lieu pour les formules (10) de l'article VII, parce que ces dernières formules contiennent la base a.

En second lieu, appliquons les formules qui expriment, sous forme des polynomes entiers de $\sin x$, ou sous forme de tels polynomes multipliés par $\cos x$, les fonctions (1), puis remarquons que, pour ε pair, le nombre

$$A_r^2 - 1 = a B_r^2$$

correspond à

$$\cos^2 x - 1 = -\sin^2 x,$$

il résulte, en vertu de (2), les quatre formules générales

$$(6)\quad \left\{ \begin{aligned} A_{2nr} &= 2^{n-1}\left(aB_r^2\right)^n + \sum_{s=1}^{s=n} \frac{(-1)^{s\varepsilon} n}{s} \binom{2n-s-1}{s-1} \left(4aB_r^2\right)^{n-s} \\ B_{2nr+r} &= B_r\left(\left(4aB_r^2\right)^n + \sum_{s=1}^{s=n} \frac{(-1)^{s\varepsilon}(2n+1)}{s} \binom{2n-s}{s-1} \left(4aB_r^2\right)^{n-s}\right) \end{aligned} \right.$$

$$(7)\quad \left\{ \begin{aligned} B_{2nr} &= B_{2r} \sum_{s=0}^{s=n-1} (-1)^{s\varepsilon} \binom{2n-s-1}{s} \left(4aB_r^2\right)^{n-s-1} \\ A_{2nr+r} &= A_r \sum_{s=0}^{s=n} (-1)^{s\varepsilon} \binom{2n-s}{s} \left(4aB_r^2\right)^{n-s}. \end{aligned} \right.$$

Posons maintenant, dans les six formules générales ainsi obtenues, $r = 1$, puis introduisons

$$B_1 = 1,\ A_1 = \alpha,\ a = \alpha^2 - (-1)^\varepsilon,\ B_2 = 2\alpha,$$

nous aurons des expressions générales pour les quatre polynomes $\varphi_n(\alpha)$ et $\psi_n(\alpha)$, $\zeta_n(\alpha)$ et $\eta_n(\alpha)$.

Cela posé, on aura par exemple

$$2\zeta_n(\alpha) = (2\alpha)^n + \sum_{s=1}^{\leq \frac{n}{2}} \frac{(-1)^s n(n-s-1)!}{s!(n-2s)!} (2\alpha)^{n-2s},$$

ce qui donnera

$$2\zeta_n\left(\frac{\alpha}{2}\right) = \sum_{s=0}^{\leq \frac{n}{2}} \frac{(-1)^s n(n-s-1)!}{s!(n-2s)!} \alpha^{n-2s},$$

savoir les polynomes étudiés par CAUCHY[1].

Quant aux inversions des six formules générales que nous venons de développer, la représentation de $\cos^n x$,

[1] Cours d'Analyse de l'École Polytechnique, t. I, p. 550; Paris 1821.

d'après les $\cos(n-2s)x$, donnera, par le procédé que nous venons d'appliquer,

$$(8) \qquad 2^{n-1} A_r^n = \sum_{s=0}^{\leq \frac{n}{2}}{}' (-1)^{s\varepsilon} \binom{n}{s} A_{nr-2sr},$$

où l'accent, fixé au signe sommatoire, indique qu'il faut prendre la moitié du dernier terme, dans le cas où n est un nombre pair.

De même, les développements de $(\sin x)^{2n}$ et de $(\sin x)^{2n+1}$, d'après les $\cos(n-2s)x$ ou les $\sin(n-2s+1)x$, donnent

$$(9) \qquad 2^{n-1}\left(a B_r^2\right)^n = \sum_{s=0}^{s=n}{}' (-1)^{s\varepsilon+s} \binom{2n}{s} A_{2nr-2sr}$$

$$(10) \qquad 2^{2n} a^n B_r^{2n+1} = \sum_{s=0}^{s=n} (-1)^{s\varepsilon+s} \binom{2n+1}{s} B_{2nr-2sr+r},$$

où l'accent fixé au signe sommatoire, dans la formule (9), indique qu'il faut, pour $s = n$, remplacer A_0 par $\frac{1}{2}$.

En dernier lieu, les deux formules trigonométriques

$$\cos 2x + \cos 4x + \ldots + \cos 2nx = \frac{\sin nx \cos(n+1)x}{\sin x}$$

$$\sin 2x + \sin 4x + \ldots + \sin 2nx = \frac{\sin nx \sin(n+1)x}{\sin x}$$

et les deux formules analogues contenant, au premier membre, des multiples impairs de x, donnent

$$(11) \qquad \left\{ \begin{aligned} \sum_{s=0}^{s=n-1} (-1)^{s\varepsilon} A_{2nr-2sr} &= \frac{B_{nr} A_{2nr+r}}{B_r} \\ \sum_{s=0}^{s=n-1} (-1)^{s\varepsilon} B_{2nr-2sr} &= \frac{B_{nr} B_{2nr+r}}{B_r} \end{aligned} \right.$$

$$
(12)\quad \left\{ \begin{aligned} &\sum_{s=0}^{s=n} (-1)^{s\varepsilon} A_{2nr-2sr+r} = \frac{B_{2nr+2r}}{2B_r} \\ &\sum_{s=0}^{s=n} (-1)^{s\varepsilon} B_{2nr-2sr+r} = \frac{B_{nr+r}^2}{B_r}. \end{aligned} \right.
$$

Remarquons, en passant, que LEJEUNE DIRICHLET a publié un petit Mémoire intitulé: Sur une manière de résoudre l'équation $t^2 - pq^2 = 1$ au moyen des fonctions circulaires.[1]

De plus, l'illustre géomètre allemand a appliqué l'équation[2]

$$
1040^2 - 1753 \cdot 617 \cdot 1^2 = -1,
$$

sans indiquer qu'elle se présente sous la forme

$$
1040^2 - (1040^2 + 1) \cdot 1^2 = -1,
$$

ce qui n'est autre chose que l'équation (5) de l'article précédent pour $\alpha = 1040$, $n = 1$.

XIII. Applications diverses.

Les quatre polynomes $\varphi_m(\alpha)$ et $\psi_m(\alpha)$, $\zeta_m(\alpha)$ et $\eta_m(\alpha)$, étudiés dans les deux articles précédents, donnent immédiatement la résolution de plusieurs équations indéterminées, dont quelques-unes seront étudiées plus amplement dans ce qui suit.

1° Remarquons tout d'abord que les formules (8) et (20) de l'article XI donnent, en vertu des identités (27) du même article,

$$
(1)\quad \left\{ \begin{aligned} &\zeta_n(\alpha) \pm \alpha \eta_n(\alpha) = \pm \eta_{n \pm 1}(\alpha) \\ &\eta_n^2(\alpha) - 2\alpha \eta_n(\alpha) \eta_{n-1}(\alpha) + \eta_{n-1}^2(\alpha) = 1, \end{aligned} \right.
$$

[1] Journal de Crelle, t. 17, p. 286—290; 1837; Werke, t. I, p. 343—350.

[2] Abhandlungen der Königlich Preussischen Akademie der Wissenschaften 1834. Werke, t. I, p. 230.

nous aurons immédiatement le théorème suivant, supplément du théorème VI de l'article XI:

I. L'équation indéterminée

$$x^2 - pxy + y^2 = 1, \tag{2}$$

où p désigne un positif entier quelconque, admet une infinité de solutions en positifs entiers, x_n et y_n, déterminées par les valeurs initiales

$$x_1 = p, \quad y_1 = 1 \tag{3}$$

à l'aide des formules récursives

$$x_{n+1} = px_n - y_n, \quad y_{n+1} = x_n. \tag{3 bis}$$

2° Il est évident que les polynomes

$$f_n(\alpha) = \varphi_{2n}(\alpha), \quad g_n(\alpha) = \frac{1}{2}\psi_{2n}(\alpha) \tag{4}$$

représentent toutes les solutions de l'identité algébrique

$$f_n(\alpha)^2 - (4\alpha^2 + 4)\, g_n^2(\alpha) = 1. \tag{5}$$

Cela posé, il résulte, en vertu du théorème VI de l'article XI, que l'ensemble des solutions en positifs entiers des deux équations indéterminées

$$x^2 - 4pxy - 4y^2 = 1, \tag{6}$$

où p désigne un positif entier quelconque, est représenté par les nombres

$$x = \varphi_{2n\pm 1}(p), \quad y = \frac{1}{2}\psi_{2n}(p). \tag{6 bis}$$

3° Les hypothèses

$$f_n(\alpha) = \zeta_{2n}(\alpha), \quad g_n(\alpha) = \frac{1}{2}\eta_{2n}(\alpha) \tag{7}$$

donnent de même l'ensemble des polynomes entiers qui satisfont à l'identité algébrique

$$f_n^2(\alpha) - (4\alpha^2 - 4)\, g_n^2(\alpha) = 1. \tag{8}$$

Or, les réduites de la fraction continue correspondante, savoir

$$\sqrt{4\alpha^2 - 4} = \left[2\alpha - 1, (1, \alpha - 2, 1, 4\alpha - 2)\right], \quad \alpha \geqq 3, \tag{9}$$

étant, pour $n = 1, 2, 3, 4, \ldots$

$$\frac{y_n(\alpha)}{z_n(\alpha)} = \frac{2\alpha - 1}{1}, \ \frac{2\alpha}{1}, \ \frac{2\alpha^2 - 2\alpha - 1}{\alpha - 1}, \ \frac{2\alpha^2 - 1}{\alpha}, \ldots,$$

on aura, quel que soit n,

$$y_{4n}(\alpha) = \zeta_{2n}(\alpha), \quad z_{4n}(\alpha) = \frac{1}{2}\eta_{2n}(\alpha). \tag{10}$$

De plus, il est facile de démontrer que

$$h_n(\alpha) = y_{4n+2}(\alpha), \quad k_n(\alpha) = z_{4n+2}(\alpha) \tag{11}$$

représentent l'ensemble des polynomes entiers qui satisfont à l'identité algébrique

$$h_n^2(\alpha) - (4\alpha^2 - 4)\, g_n^2(\alpha) = 4. \tag{11 bis}$$

En effet, remarquons tout d'abord que les formules (11) sont vraies pour $n = 0$, il résulte, en vertu du théorème I de l'article II, que les formules en question sont valables pour une valeur quelconque de l'indice n.

Cela posé, remarquons que l'identité (11 bis) est aussi satisfaite par

$$h_n(\alpha) = \frac{1}{2}\zeta_{2n+1}(\alpha), \quad k_n(\alpha) = \eta_{2n+1}(\alpha),$$

et que $y_{4n+2}(\alpha)$ est du même degré par rapport à α que $\zeta_{2n+1}(\alpha)$, savoir du degré $2n + 1$, il résulte, quel que soit n,

$$y_{4n+2}(\alpha) = \frac{1}{2}\zeta_{2n+1}(\alpha), \quad z_{4n+2}(\alpha) = \eta_{2n+1}(\alpha), \tag{12}$$

car les polynomes qui satisfont à l'identité (11 bis) sont parfaitement déterminés, pourvu que leurs degrés soient donnés.[1]

Quant à l'équation indéterminée

$$x^2 - 2pxy + 4y^2 = 1, \tag{13}$$

où p désigne un positif entier quelconque, ses solutions en positifs entiers deviennent, en vertu du théorème I,

$$x = \frac{1}{2}\zeta_{2n+1}(p), \quad y = \eta_{2n+1}(p). \tag{13 bis}$$

4° Les fonctions

$$f_n(\alpha) = \zeta_n(2\alpha + 1), \quad g_n(\alpha) = \eta_n(2\alpha + 1) \tag{14}$$

représentent l'ensemble des polynomes entiers qui satisfont à l'identité algébrique

$$f_n^2(\alpha) - (\alpha^2 + \alpha)\, g_n^2(\alpha) = 1. \tag{15}$$

La fraction continue correspondante, savoir

$$\sqrt{\alpha^2 + \alpha} = \left[\alpha, (2, 2\alpha)\right], \quad \alpha \geqq 2, \tag{15 bis}$$

ne présente, à ce point de vue, aucun intérêt, et c'est la même chose pour l'équation indéterminée

$$x^2 - (2p + 1)xy + y^2 = 4. \tag{16}$$

En effet, on voit que les nombres entiers x et y sont nécessairement tous deux pairs. Supprimons ensuite le facteur commun 4, il est évident que (16) n'est autre chose que l'équation (2).

5° Les fonctions

$$(17) \left\{ \begin{aligned} \Phi_{2n}(\alpha) &= \varphi_{2n}\left(\frac{\alpha}{\sqrt{2}}\right), & \Psi_{2n}(\alpha) &= \frac{1}{\sqrt{2}}\psi_{2n}\left(\frac{\alpha}{\sqrt{2}}\right) \\ \Phi_{2n+1}(\alpha) &= \sqrt{2}\,\varphi_{2n+1}\left(\frac{\alpha}{\sqrt{2}}\right), & \Psi_{2n+1}(\alpha) &= \psi_{2n+1}\left(\frac{\alpha}{\sqrt{2}}\right) \end{aligned} \right.$$

[1] Voir ma Note: Sur la généralisation du problème de Fermat. Det Kongelige Danske Videnskabernes Selskabs mathematisk-fysiske Meddelelser III, 16.

représentent l'ensemble des polynomes entiers qui satisfont aux identités algébriques

$$(18) \quad \begin{cases} \Phi_{2n}^2(\alpha) - (\alpha^2 + 2)\, \Psi_{2n}^2(\alpha) = 1 \\ \Phi_{2n+1}^2(\alpha) - (\alpha^2 + 2)\, \Psi_{2n+1}^2(\alpha) = -2. \end{cases}$$

Nous nous bornerons ici à ces indications concernant les polynomes $\Phi_m(\alpha)$ et $\Psi_m(\alpha)$, parce que nous avons à étudier plus amplement, dans l'article qui suit, ces polynomes qui présentent un intérêt particulier.

6° Il est évident que les fonctions

$$(19) \quad \begin{cases} Z_{2n}(\alpha) = \zeta_{2n}\left(\dfrac{\alpha}{\sqrt{2}}\right), & H_{2n}(\alpha) = \dfrac{1}{\sqrt{2}}\,\eta_{2n}\left(\dfrac{\alpha}{\sqrt{2}}\right) \\ Z_{2n+1}(\alpha) = \sqrt{2}\,\zeta_{2n+1}\left(\dfrac{\alpha}{\sqrt{2}}\right), & H_{2n+1}(\alpha) = \eta_{2n+1}\left(\dfrac{\alpha}{\sqrt{2}}\right) \end{cases}$$

analogues aux $\Phi_m(\alpha)$ et $\Psi_m(\alpha)$, représentent la solution complète, en polynomes entiers, des deux identités algébriques

$$(19 \text{ bis}) \quad \begin{cases} Z_{2n}^2(\alpha) - (\alpha^2 - 2)\, H_{2n}^2(\alpha) = 1 \\ Z_{2n+1}^2(\alpha) - (\alpha^2 - 2)\, H_{2n+1}^2(\alpha) = 2. \end{cases}$$

La fraction continue correspondante, savoir

$$(20) \quad \sqrt{\alpha^2 - 2} = \left[\alpha - 1, (1, \alpha - 2, 1, 2\alpha - 2)\right], \quad \alpha \geqq 3,$$

ayant, pour $n = 1, 2, 3, 4, \ldots$, les réduites

$$(20\,\text{bis}) \quad \frac{y_n(\alpha)}{z_n(\alpha)} = \frac{\alpha - 1}{1}, \ \frac{\alpha}{1}, \ \frac{\alpha^2 - \alpha - 1}{\alpha - 1}, \ \frac{\alpha^2 - 1}{\alpha}, \ldots,$$

on aura par conséquent

$$(21) \quad y_{4n}(\alpha) = \zeta_{2n}\left(\frac{\alpha}{\sqrt{2}}\right), \quad z_{4n}(\alpha) = \frac{1}{\sqrt{2}}\,\eta_{2n}\left(\frac{\alpha}{\sqrt{2}}\right).$$

De plus, nous aurons, quel que soit n,

$$y_{4n+2}^2(\alpha) - (\alpha^2 - 2)\, z_{4n+2}^2(\alpha) = 2, \tag{22}$$

parce que cette formule est évidente pour $n = 0$, et la formule générale est donc une conséquence immédiate du théorème I de l'article II; c'est-à-dire que nous aurons

$$Z_{2n+1}(\alpha) = y_{4n+2}(\alpha), \quad H_{2n+1}(\alpha) = z_{4n+2}(\alpha). \tag{22 bis}$$

7° Étudions maintenant les fonctions

$$f_n(\alpha) = \varphi_n\left(\alpha + \frac{1}{2}\right), \quad g_n(\alpha) = \frac{1}{2}\psi_n\left(\alpha + \frac{1}{2}\right), \tag{23}$$

puis remarquons que

$$f_3(\alpha) = 4\alpha^3 + 6\alpha^2 + 6\alpha + 2, \quad g_3(\alpha) = 2\alpha^2 + \alpha + 1$$

sont les premières de ces fonctions qui aient toutes deux des coefficients entiers; il est évident que la solution complète, en polynomes entiers, de l'identité algébrique

$$h_n^2(\alpha) - (4\alpha^2 + 4\alpha + 5)\, k_n^2(\alpha) = (-1)^n \tag{24}$$

est représentée par les fonctions

$$h_n(\alpha) = \varphi_{3n}\left(\alpha + \frac{1}{2}\right), \quad k_n(\alpha) = \frac{1}{2}\psi_{3n}\left(\alpha + \frac{1}{2}\right). \tag{24 bis}$$

La fraction continue dont il s'agit ici, savoir

$$\sqrt{4\alpha^2 + 4\alpha + 5} = \left[2\alpha + 1, (\alpha, 1, 1, \alpha, 4\alpha + 2)\right], \quad \alpha \geqq 1, \tag{25}$$

ayant, pour $n = 1, 2, 3, 4, 5, \ldots$, les réduites

$$\left\{\begin{aligned} \frac{y_n(\alpha)}{z_n(\alpha)} = \frac{2\alpha + 1}{1}, \quad \frac{2\alpha^2 + \alpha + 1}{\alpha}, \quad \frac{2\alpha^2 + 3\alpha + 2}{\alpha + 1}, \\ \frac{4\alpha^2 + 4\alpha + 3}{2\alpha + 1}, \quad \frac{4\alpha^3 + 6\alpha^2 + 6\alpha + 2}{2\alpha^2 + 2\alpha + 1}, \ldots, \end{aligned}\right. \tag{25 bis}$$

on aura, quel que soit l'indice n,

$$y_{5n}(\alpha) = \varphi_{3n}\left(\alpha + \frac{1}{2}\right), \quad z_{5n}(\alpha) = \frac{1}{2}\psi_{3n}\left(\alpha + \frac{1}{2}\right). \tag{26}$$

Remarquons ensuite que le procédé ordinaire donnera ici, quel que soit l'indice n,

$$(27)\quad y_{5n\pm1}^2(\alpha) - (4\alpha^2+4\alpha+5)\,z_{5n\pm1}^2(\alpha) = (-1)^{n-1}4,$$

nous aurons de même

$$(27\text{ bis})\quad y_{5n\pm1}(\alpha) = 2\varphi_{3n\pm1}\left(\alpha+\frac{1}{2}\right),\ z_{5n\pm1}(\alpha) = \psi_{3n\pm1}\left(\alpha+\frac{1}{2}\right).$$

Quant aux équations indéterminées

$$(28)\qquad x^2 \mp (4p+2)\,xy - 4y^2 = \pm 1,$$

elles conduisent à l'équation de FERMAT

$$x^2 - (4p^2+4p+5)\,y^2 = \pm 1,$$

et l'on aura donc

$$(28\text{ bis})\quad y = k_n(p),\ x = h_n(p) \pm (2p+1)\,k_n(p).$$

8° En dernier lieu, les fonctions

$$(29)\qquad f_n(\alpha) = \zeta_{3n}\left(\alpha+\frac{1}{2}\right),\ g_n(\alpha) = \frac{1}{2}\eta_{3n}\left(\alpha+\frac{1}{2}\right).$$

représentent la solution complète, en polynomes entiers, de l'identité algébrique

$$(30)\qquad f_n^2(\alpha) - (4\alpha^2+4\alpha-3)\,g_n^2(\alpha) = 1.$$

La fraction continue correspondante, savoir

$$(31)\quad \sqrt{4\alpha^2+4\alpha-3} = \left[2\alpha, (1, \alpha-1, 2, \alpha-1, 1, 4\alpha)\right],\ \alpha \geqq 2$$

ayant, pour $n = 1, 2, 3, \ldots$, les réduites

$$(31\text{ bis})\quad \begin{cases} \dfrac{2\alpha}{1},\ \dfrac{2\alpha+1}{1},\ \dfrac{2\alpha^2+\alpha-1}{\alpha},\ \dfrac{4\alpha^2+3\alpha-1}{2\alpha+1}, \\ \dfrac{4\alpha^3+2\alpha^2-4\alpha}{2\alpha^2-1},\ \dfrac{4\alpha^3+6\alpha-1}{2\alpha^2+6\alpha},\ \ldots, \end{cases}$$

on aura, quel que soit l'indice n,

$$(32) \qquad y_{6n} = \zeta_{3n}\left(\alpha + \frac{1}{2}\right), \quad z_{6n}(\alpha) = \frac{1}{2}\eta_{3n}\left(\alpha + \frac{1}{2}\right).$$

De plus, le procédé ordinaire donnera ici

$$(33) \qquad y^2_{6n\pm 2}(\alpha) - (4\alpha^2 + 4\alpha - 3)\, z^2_{6n\pm 2}(\alpha) = 4,$$

donc on aura, quel que soit l'indice n,

$$(33\text{ bis}) \quad y_{6n\pm 2}(\alpha) = 2\zeta_{3n\pm 1}\left(\alpha + \frac{1}{2}\right), \quad z_{6n\pm 2}(\alpha) = \eta_{3n\pm 1}(\alpha).$$

Quant à l'équation indéterminée

$$(34) \qquad x^2 \pm (4p + 2)\, xy + 4y^2 = 1,$$

elle conduira à l'équation de FERMAT

$$z^2 - (4p^2 + 4p - 3)\, y^2 = 1,$$

et l'on aura donc

$$(34\text{ bis}) \qquad y = g_n(p), \quad x = f_n(p) \pm (2p + 1)\, g_n(p).$$

Il est évident, du reste, que les polynomes entiers, étudiés dans cet article, donnent des éclaircissements sur la nature de certaines bases d'une forme spéciale. On aura, en effet, les deux propositions suivantes, qui présentent un certain intérêt:

II. Soit n un nombre entier, les nombres

$$(35) \qquad n^2 + 1, \quad 4n^2 + 4n + 5$$

sont, pour $n \geqq 1$, respectivement $n \geqq 0$, toujours des bases de première espèce.

On voit par exemple que les nombres

$$(35\text{ bis}) \qquad (10\nu \pm 1)^2 + 4,$$

divisibles par 5, sont des bases de première espèce, bien qu'ils ne soient pas, pour $\nu \geqq 1$, des nombres premiers; les premiers de ces nombres deviennent

$$85, \ 125, \ 365, \ 445, \ \ldots.$$

Quant au deuxième de ces nombres, le théorème V de l'article X montre que les puissances $5^{2\varrho+1}$ sont toujours des bases de première espèce.

Remarquons, en passant, que les réduites de la fraction continue

$$\sqrt{10} = [3, (6)]$$

deviennent

$$\frac{3}{1}, \frac{19}{6}, \frac{117}{37}, \frac{721}{228}, \frac{4443}{1405}, \ldots,$$

il est évident que le nombre 5 est, pour la base 10, du rang 5; c'est-à-dire que les nombres $2 \cdot 5^{2\varrho+1}$ sont toujours des bases de première espèce.

Dans l'article XVIII, nous avons à démontrer que les nombres $2 \cdot 5^{2\varrho}$ sont aussi des bases de première espèce.

Chose curieuse, le nombre

$$5 \cdot 521 = 51^2 + 4,$$

de la forme (35 bis), ne satisfait pas aux conditions suffisantes que Lejeune Dirichlet[1] a données, afin que le produit de deux nombres premiers de la forme $4\nu + 1$ soit une base de première espèce.

III. *Soit n un positif entier, les nombres*

$$n^2 \pm 2, \quad n(n+1), \quad n(n+2), \quad n(n+4), \quad 4n \tag{36}$$

sont toujours des bases de seconde espèce, abstraction faite peut-être des petites valeurs de n.

On voit par exemple que les produits

$$13 \cdot 17, \quad 37 \cdot 41, \quad 97 \cdot 101, \quad 109 \cdot 113$$

sont des bases de seconde espèce, bien que les huit nombres premiers en question soient tous de la forme $4\nu + 1$.

[1] Abhandlungen der Königlich Preussischen Akademie der Wissenschaften 1834. Werke, t. I, p. 230.

Quant à la base 2 qui est de première espèce, on voit que les nombres

$$(36\,\text{bis})\quad 2\cdot 17 = 6^2 - 2,\ 2\cdot 73 = 12^2 + 2,\ 2\cdot 97 = 14^2 - 2$$

sont des bases de seconde espèce, bien que les trois nombres premiers 17, 73, 97 soient tous de la forme $4\nu + 1$.

Dans l'article XXII, nous avons à étudier plus amplement les nombres de la forme (36 bis).

Remarquons, en passant, que les bases spéciales que nous venons d'étudier sont bien connues. En effet, EULER[1] en a considéré les quatre qui se présentent sous la forme $\alpha^2 \pm 1$ et $\alpha^2 \pm 2$, auxquelles WERTHEIM[2] a ajouté $\alpha^2 + \alpha$, tandis que M. F. TANO[3] a étudié $\alpha^2 \pm 4$, et M. E. DE JONQUIÈRES[4] remarque que les nombres $(2\alpha + 1)^2 + 4$ sont toujours des bases de première espèce. De plus, ce dernier géomètre indique que les nombres

$$(\alpha^2 + 1)\,\psi^2_{2n+1}(\alpha) = \varphi^2_{2n+1}(\alpha) + 1$$

sont toujours des bases de première espèce, ce qui est, du reste, un cas très spécial du théorème IV de l'article X.

Quant aux nombres $\alpha^2 \pm 1$, le théorème II de l'article IV donnera la proposition curieuse:

IV. *Soit* $a = (4\nu + 3)^{2\varrho+1}$, *où* $4\nu + 3$ *est un nombre premier, tous les nombres* $A_{2n+1}(a)$ *sont des bases de première ou de seconde espèce, selon que* ν *est pair ou impair.*

[1] Algebra, herausgegeben von J. P. GRÜSON, t. II, p. 249—251; Berlin 1797.

[2] Anfangsgründe der Zahlenlehre, p. 223; Brunswick 1902.

[3] Bulletin de Darboux (2), t. 4, p. 215—218; 1890.

[4] Comptes rendus, t. 126, p. 1837—1843; 1898.

XIV. De la base $a = \alpha^2 + 2$.

Revenons maintenant aux polynomes $\Phi_m(\alpha)$ et $\Psi_m(\alpha)$, définis par les formules (17) de l'article précédent et satisfaisant aux identités algébriques

$$(1)\quad \begin{cases} \Phi_{2n}^2(\alpha) - (\alpha^2+2)\,\Psi_{2n}^2(\alpha) = 1 \\ \Phi_{2n+1}^2(\alpha) - (\alpha^2+2)\,\Psi_{2n+1}^2(\alpha) = -2, \end{cases}$$

la fraction continue correspondante, savoir

$$(2)\quad \sqrt{\alpha^2+2} = \left[\alpha, (\alpha, 2\alpha)\right],$$

a les réduites

$$(2\text{ bis})\quad \begin{cases} \dfrac{\alpha}{1}, \ \dfrac{\alpha^2+1}{\alpha}, \ \dfrac{2\alpha^3+3\alpha}{2\alpha^2+1}, \ \dfrac{2\alpha^4+4\alpha^2+1}{2\alpha^3+2\alpha}, \\ \dfrac{4\alpha^5+10\alpha^3+5\alpha}{4\alpha^4+6\alpha^2+1}, \ \dfrac{4\alpha^6+12\alpha^4+9\alpha^2+1}{4\alpha^5+8\alpha^3+3\alpha}, \ldots, \end{cases}$$

ce qui donnera les formules récursives

$$(3)\quad \begin{cases} \Phi_{2n}(\alpha) = \alpha\,\Phi_{2n-1}(\alpha) + \Phi_{2n-2}(\alpha) \\ \Psi_{2n}(\alpha) = \alpha\,\Psi_{2n-1}(\alpha) + \Psi_{2n-2}(\alpha) \end{cases}$$

$$(3\text{ bis})\quad \begin{cases} \Phi_{2n+1}(\alpha) = 2\alpha\,\Phi_{2n}(\alpha) + \Phi_{2n-1}(\alpha) \\ \Psi_{2n+1}(\alpha) = 2\alpha\,\Psi_{2n}(\alpha) + \Psi_{2n-1}(\alpha). \end{cases}$$

Appliquons ensuite les définitions (17) de l'article précédent, il résulte, en vertu des formules (7), (8), (9), (10) de l'article XI,

$$(4)\quad \begin{cases} \Psi_{2n}(\alpha) + \Psi_{2n+2}(\alpha) = \Phi_{2n-1}(\alpha) \\ \Psi_{2n+1}(\alpha) + \Psi_{2n-1}(\alpha) = 2\,\Psi_{2n}(\alpha) \end{cases}$$

$$(5)\quad \Phi_{2n}(\alpha) \pm \alpha\,\Psi_{2n}(\alpha) = \Psi_{2n\pm 1}(\alpha)$$

$$(6)\quad \begin{cases} \Phi_{2n+1}(\alpha) + \alpha\,\Psi_{2n+1}(\alpha) = 2\,\Psi_{2n+2}(\alpha) \\ \Phi_{2n+1}(\alpha) - \alpha\,\Psi_{2n+1}(\alpha) = 2\,\Psi_{2n}(\alpha) \end{cases}$$

$$(7) \quad \begin{cases} \Phi_{4n}(\alpha) = 2\,\Phi_{2n}^2(\alpha) - 1 \\ \Phi_{4n+2}(\alpha) = \Phi_{2n+1}^2(\alpha) - 1 \end{cases}$$

$$(8) \quad \begin{cases} \Psi_{4n}(\alpha) = 2\,\Phi_{2n}(\alpha)\,\Psi_{2n}(\alpha) \\ \Psi_{4n+2}(\alpha) = \Phi_{2n+1}(\alpha)\,\Psi_{2n+1}(\alpha). \end{cases}$$

Remarquons, en passant, que la dernière des formules (4) donnera, en vertu de (5), les relations curieuses

$$(9) \quad \Psi_{2n+1}(\alpha) - \Phi_{2n}(\alpha) = \Phi_{2n}(\alpha) - \Psi_{2n-1}(\alpha) = \alpha\,\Psi_{2n}(\alpha).$$

Quant à la dernière des formules (12) de l'article XI, elle donne

$$(10) \quad \Psi_{4n\pm1}(\alpha) = \Psi_{2n\pm1}^2(\alpha) + 2\,\Psi_{2n}^2(\alpha),$$

tandis qu'il résulte, en vertu de la formule (14) de l'article susdit,

$$(11) \quad \begin{cases} 2\,\alpha\,\Psi_{4n}(\alpha) = \Psi_{2n+1}^2(\alpha) - \Psi_{2n-1}^2(\alpha) \\ \alpha\,\Psi_{4n+2}(\alpha) = \Psi_{2n+2}^2(\alpha) - \Psi_{2n}^2(\alpha). \end{cases}$$

Nous avons encore à appliquer la formule (15) de l'article XI, ce qui donnera les relations intéressantes

$$(12) \quad \begin{cases} 2\,\Psi_{2n}^2(\alpha) + 1 = \Psi_{2n-1}(\alpha)\,\Psi_{2n+1}(\alpha) \\ \Psi_{2n+1}^2(\alpha) - 1 = 2\,\Psi_{2n}(\alpha)\,\Psi_{2n+2}\,\alpha(). \end{cases}$$

Cela posé, il saute aux yeux que l'expression de $\Psi_{2m+1}(\alpha)$ indiquée dans la formule (10), est très intéressante, parce que $\Psi_{2m+1}(\alpha)$ est, en vertu des formules (1) et (12), diviseur des deux polynomes

$$(13) \quad \Phi_{2m+1}^2(\alpha) + 2, \quad 2\,\Psi_{2m}^2(\alpha) + 1$$

qui sont tous deux de la même forme que le second membre de (10), mais un des deux polynomes qui figurent dans les expressions (13) est réduit à l'unité.

Cette propriété des $\Psi_{2m+1}(\alpha)$ est très intéressante, au point de vue historique, nous le verrons dans l'article XVI, en démontrant deux propositions de Fermat.

Du reste, nous avons, dans l'article XVII, à donner une nouvelle démonstration de la formule (10).

Remarquons maintenant que la fraction continue (2) appartient à celles considérées par Seeling; la formule (18) de l'article II donnera immédiatement

$$(14)\quad \Phi_n(\alpha)\,\Phi_{n-1}(\alpha)-(\alpha^2+2)\,\Psi_n(\alpha)\,\Psi_{n-1}(\alpha)=(-1)^n\alpha,$$

tandis que la définition même des $\Phi_m(\alpha)$ et des $\Psi_m(\alpha)$, comme étant, pour $m = 1, 2, 3, \ldots$, les numérateurs respectivement les dénominateurs des réduites (2 bis), donne cette autre identité

$$(15)\quad \Phi_n(\alpha)\,\Psi_{n-1}(\alpha)-\Psi_n(\alpha)\,\Phi_{n-1}(\alpha) = (-1)^{n-1}.$$

Éliminons ensuite, en vertu de (5), les fonctions $\Phi_n(\alpha)$ et $\Phi_{n-1}(\alpha)$, il résulte

$$(16)\quad \Psi^2_{2n\pm 1}(\alpha)\mp 2\alpha\,\Psi_{2n}(\alpha)\,\Psi_{2n\pm 1}(\alpha)-2\,\Psi^2_{2n}(\alpha) = 1,$$

où les trois signes doubles correspondent entre eux.

Cela posé, on aura immédiatement la proposition:

I. Soit p un positif entier quelconque, les valeurs

$$(17)\quad x = \Psi_{2n\pm 1}(p),\quad y = \Psi_{2n}(p)$$

représentent l'ensemble des solutions en positifs entiers de l'équation indéterminée

$$(18)\quad x^2 \mp 2pxy - 2y^2 = 1.$$

Remarquons, en passant, que les polynomes $Z_n(\alpha)$ et $H_n(\alpha)$, définis par les formules (19) de l'article précédent, se présentent aussi sous la forme

$$Z_n(\alpha) = i^{-n}\,\Phi_n(i\alpha); \quad H_n(\alpha) = i^{1-n}\,\Psi_n(i\alpha), \tag{19}$$

il est évident que ces polynomes satisfont à une suite de relations analogues à celles que nous venons de démontrer pour les $\Phi_n(\alpha)$ et les $\Psi_n(\alpha)$.

Or, ces identités étant, en vertu de (19), des conséquences immédiates des précédentes, nous nous bornerons à cette indication de leur existence.

CHAPITRE IV

Des nombres $x^2 + ay^2$.

XV. Formules générales.

Dans plusieurs équations indéterminées, les nombres de la forme

$$p^2 + aq^2,$$

où a est un positif entier, jouent un rôle fondamental; c'est pourquoi il nous semble utile de développer une suite de formules fondamentales et de résoudre certains problèmes, qui se rattachent aux nombres susdits.

A cet effet, prenons pour point de départ l'identité algébrique

$$(1) \qquad (p^2 + aq^2)(r^2 + as^2) = (pr \pm aqs)^2 + a(ps \mp rq)^2,$$

nous avons tout d'abord à résoudre deux problèmes qui correspondent à des formes spéciales du produit, développé dans la formule (1), savoir:

I. Déterminer les positifs entiers x, y, z qui satisfassent à l'équation indéterminée

$$(2) \qquad (p^2 + aq^2)(x^2 + ay^2) = z^2 + a,$$

où p et q sont des positifs entiers donnés, premiers entre eux.

Il résulte immédiatement, en vertu de (1),

$$(3) \qquad px \mp qy = \pm 1,$$

équation indéterminée du premier degré qui est toujours résoluble en nombres entiers, et qui représente la condition suffisante et nécessaire pour l'existence de l'equation (2).

II. Déterminer les positifs entiers x, y, z qui satisfassent à l'équation indéterminée

$$(4) \qquad (p^2 + aq^2)(x^2 + ay^2) = az^2 + 1,$$

où p et q sont des positifs entiers donnés, tels que p et aq sont premiers entre eux.

Dans ce cas, nous avons à résoudre l'équation indéterminée

$$(5) \qquad px \pm aqy = \pm 1,$$

ce qui est toujours possible, parce que p est supposé premier avec le produit aq.

III. Déterminer les positifs entiers x, y, z qui satisfassent à l'équation indéterminée

$$(6) \qquad (x^2 + ay^2)^2 = az^2 + 1,$$

où a est un positif entier donné, n'étant pas un carré exact.

En remarquant que la formule (1) se présente, dans ce cas, sous la forme

$$(7) \qquad (x^2 + ay^2)^2 = (x^2 - ay^2)^2 + a(2xy)^2,$$

on aura ici à résoudre l'équation de FERMAT

$$(8) \qquad x^2 - ay^2 = \pm 1,$$

ce qu donnera

$$(9) \qquad x = A_n, \quad y = B_n, \quad z = B_{2n},$$

de sorte que l'équation (6) n'est autre chose que celle-ci

$$A_{2n}^2 - aB_{2n}^2 = 1.$$

Multiplions maintenant par $\alpha^2 + a\beta^2$ les deux membres de (7), il résulte, en vertu de (1), cette autre identité

$$(10) \left\{ \begin{aligned} & (\alpha^2 + a\beta^2)(x^2 + ay^2)^2 = \\ & = \left[(x^2 - ay^2)\alpha \pm 2a\beta xy\right]^2 + a\left[(x^2 - ay^2)\beta \mp 2\alpha xy\right]^2, \end{aligned} \right.$$

essentielle et dans la théorie de l'équation de FERMAT et dans la théorie des nombres $x^2 + ay^2$, nous le verrons, en résolvant des problèmes convenables.

IV. Déterminer les positifs entiers x, y, z qui satisfassent à l'équation indéterminée

$$(\alpha^2 + a)(x^2 + ay^2)^2 = z^2 + a, \tag{11}$$

où a et α sont des positifs entiers donnés, tels que $\alpha^2 + a$ n'est pas un carré exact.

Soit, dans (10), $\beta = 1$, il résulte, en vertu de (11),

$$x^2 - ay^2 \mp 2\alpha xy = \pm 1,$$

ce qui donnera

$$x = \pm \alpha y \pm \sqrt{(\alpha^2 + a)y^2 \pm 1},$$

de sorte qu'il s'agit de résoudre l'équation de FERMAT

$$t^2 - (\alpha^2 + a)y^2 = \pm 1, \tag{12}$$

et l'on aura donc

$$y = B_n,\ x = |A_n \pm \alpha B_n|, \tag{13}$$

tandis que z se présente sous la forme

$$z = |(x^2 - ay^2)\alpha \pm 2axy|, \tag{13 bis}$$

où les signes doubles qui figurent dans x et z sont les mêmes.

V. Déterminer les positifs entiers x, y, z qui satisfassent à l'équation indéterminée

$$(a\alpha^2 + 1)(x^2 + ay^2)^2 = az^2 + 1, \tag{14}$$

où a et α sont des positifs entiers donnés, tels que la somme $a^2\alpha^2 + a$ n'est pas un carré exact.

Posons, dans (10), $\alpha = 1$, puis remplaçons β par α, il résulte, en vertu de (14),

$$x^2 - ay^2 \pm 2a\alpha xy = \pm 1,$$

savoir

$$x = \mp a\alpha y \pm \sqrt{(a^2\alpha^2 + a)y^2 \pm 1},$$

ce qui conduira à l'équation de FERMAT

(15) $$t^2 - (a^2\alpha^2 + a)y^2 = \pm 1,$$

de sorte que nous aurons

(16) $$y = B_n, \quad x = |A_n \mp a\alpha B_n|,$$

tandis que z se présente sous la forme

(16 bis) $$z = |(x^2 - ay^2)\alpha \mp 2xy|,$$

où les signes doubles qui figurent dans x et z sont les mêmes.

Quant aux nombres $x^2 + ay^2$, nous avons encore à démontrer quelques propriétés fondamentales des positifs entiers X_n et Y_n, définis par l'identité

(17) $$(x^2 + ay^2)^n = X_n^2 + aY_n^2.$$

A cet effet, multiplions par $x^2 + ay^2$ les deux membres de (17), il résulte immédiatement, en vertu de (1), les formules récursives

$$\pm X_{n+1} = xX_n \pm ayY_n$$
$$\pm Y_{n+1} = xY_n \mp yX_n,$$

et la conclusion de m à $m+1$ donnera la congruence

(18) $$Y_n \equiv 0 \pmod{y},$$

donc nous aurons la proposition:

VI. *Une équation de la forme*

(19) $$(x^2 + ay^2)^n = X_n^2 + a$$

n'est possible, à moins que $y = 1$.

En second lieu, multiplions par

$$(x^2 + ay^2)^2 = (x^2 - ay^2)^2 + a(2xy)^2$$

les deux membres de (17), il résulte les deux autres formules récursives

$$\pm X_{n+2} = (x^2 - ay^2) X_n \pm 2\,axy\,Y_n$$
$$\pm Y_{n+2} = (x^2 - ay^2) Y_n \mp 2\,xy\,X_n,$$

ce qui donnera, par la conclusion de m à $m+1$, les deux congruences

$$X_{2n+1} \equiv 0 \pmod{x} \tag{20}$$
$$Y_{2n} \equiv 0 \pmod{2xy}. \tag{21}$$

Remarquons ensuite que Y_{2n} est toujours un nombre pair, nous aurons les deux propositions analogues à VI:

VII. Une équation de la forme

$$(x^2 + ay^2)^{2n} = X_{2n}^2 + a \tag{22}$$

est toujours impossible.

VIII. Une équation de la forme

$$(x^2 + ay^2)^{2n+1} = a\,Y_{2n+1}^2 + 1 \tag{23}$$

est impossible, à moins que $x = 1$.

XVI. Des cubes. Propositions de Fermat.

Revenons maintenant à la formule (10) de l'article précédent, puis posons $x = \alpha$, $y = \beta$, il résulte la formule plus spéciale

$$\tag{1} \left\{ \begin{aligned} & (\alpha^2 + a\beta^2)^3 = \\ & = \left[(\alpha^2 - a\beta^2)\,\alpha \pm 2\,a\,\alpha\beta^2\right]^2 + a\left[(\alpha^2 - a\beta^2)\,\beta \mp 2\,\alpha^2\beta\right]^2, \end{aligned} \right.$$

essentielle dans des recherches sur les cubes.

En premier lieu, nous aurons à démontrer le théorème:

I. Soit a un positif entier quelconque, l'équation indéterminée

$$(x^2 + ay^2)^3 = az^2 + 1 \tag{2}$$

n'est jamais résoluble en positifs entiers.

On aura, en effet, conformément à la formule (1),

$$(x^2 - ay^2)x \pm 2axy = \pm 1,$$

ce qui donnera à la fois $x = \pm 1$ et

$$1 - ay^2 \pm 2ay^2 = \pm 1,$$

où les signes doubles sont arbitraires; c'est-à-dire qu'il nous reste à étudier ces deux équations indéterminées

$$ay^2 \pm 2ay^2 = 0$$
$$ay^2 \pm 2ay^2 = \pm 2.$$

Or, il est évident que la première de ces équations est impossible, parce qu'elle donne $y = 0$. Quant à la seconde des équations susdites, elle entraîne nécessairement celle-ci

$$ay^2 = 2,$$

parce que les autres combinaisons des signes doubles ne sont pas admissibles; c'est-à-dire que nous aurons, comme seule possibilité

$$a = 2, \quad y = 1,$$

et il résulte donc, en vertu de (2),

$$26 = 2z^2,$$

ce qui est impossible.

Comme supplément au théorème I, nous aurons à démontrer celui-ci:

II. Soit a un positif entier, l'équation indéterminée

$$(x^2 + ay^2)^3 = z^2 + a \tag{3}$$

n'est jamais résoluble en positifs entiers, à moins que a ne se présente sous la forme

$$a = 3\alpha^2 \pm 1, \tag{4}$$

où α est un positif entier quelconque. Dans ce cas, l'équation susdite n'admet qu'une seule solution en positifs entiers, savoir

$$x = \alpha, \quad y = 1, \quad z = 8\alpha^3 \pm 3\alpha. \tag{5}$$

La formule (1) donnera ici

$$(x^2 - ay^2)\, y \mp 2x^2 y = \pm 1,$$

ce qui exige $y = \pm 1$, et l'on aura donc

$$x^2 - a \mp 2x^2 = \pm 1,$$

où les signes sont arbitraires; c'est-à-dire que l'hypothèse

$$a = 3x^2 \pm 1 \tag{6}$$

est la seule possible, et a est par conséquent de la forme (4).

Soit maintenant α un positif entier quelconque, et soit a déterminé par l'expression (4), il résulte, en vertu de (6),

$$x = \alpha,$$

de sorte qu'il nous reste à déterminer l'inconnue z.

A cet effet, on aura, en vertu de (1),

$$\pm z = -\alpha(2\alpha^2 \pm 1) \pm 2\alpha(3\alpha^2 \pm 1),$$

où ± 1 a la même valeur dans les deux parenthèses qui figurent au second membre, tandis que les autres signes sont arbitraires.

Cela posé, il ne nous reste évidemment que ces deux valeurs

$$z = 8\alpha^3 \pm 3\alpha \tag{8}$$

$$z = 4\alpha^3 \pm \alpha, \tag{8 bis}$$

et l'identité algébrique

$$(4\alpha^2 \pm 1)^3 = (8\alpha^3 \pm 3\alpha)^2 + 3\alpha^2 \pm 1$$

montre clairement que la valeur (8) est appliquable, quel que soit le positif entier α.

Quant à la valeur (8 bis), on aura, en vertu de (3),

$$6\alpha^4 \pm 5\alpha^2 + 1 = 0,$$

ce qui est impossible, et l'équation (3) n'a donc que la seule solution indiquée par les formules (5).

Quant au théorème II, je ne me rappelle pas l'avoir vu dans la littérature qui traite, plus ou moins habilement, les équations indéterminées

$$x^3 = y^2 \pm a, \tag{9}$$

où a est un positif entier, littérature de laquelle nous citons ici les publications de M. M. E. de Jonquières[1], S. Réalis[2], Fauquembergue[3] et le P. Th. Pepin S. J.[4]

Remarquons encore que Le Besgue[5] et Gerono[6] ont démontré l'impossibilité de l'équation (9), où le second membre est $y^2 - 7$ respectivement $y^2 + 17$.

Revenons maintenant aux deux théorèmes que nous venons de démontrer, il est évident qu'ils donnent une suite de résultats intéressants concernant les cubes, résultats parmi lesquels nous aurons à étudier plus amplement ceux qui suivent.

III. Soit

$$a = 1, 2, 3, 4, \tag{10}$$

l'équation indéterminée

[1] Nouvelles Annales (2) t. 7, pp. 374—381, 514—516; 1878.

[2] Ibid. (3) t. 2, p. 289—297; 1883.

[3] Ibid. (3) t. 4, p. 379—380; 1885.

[4] Annales de la Société Scientifique de Bruxelles, t. VI B, p. 86—100; 1882. Comptes rendus, t. 119, p. 397—399; 1894, t. 120, p. 1254—1256; 1895.

[5] Nouvelles Annales (2) t. 8, p. 455; 1869.

[6] Ibid. (2) t. 16, p. 325—326; 1877.

$$x^3 = ay^2 + 1 \tag{11}$$

n'est jamais résoluble en positifs entiers.

Considérons tout d'abord les valeurs 1, 2, 3, nous aurons, d'après Fermat, que x est nécessairement un nombre de la forme

$$x = \alpha^2 + a\beta^2, \quad a = 1, 2, 3,$$

où α et β sont des positifs entiers, et le théorème I montre que cette hypothèse est inadmissible.

Quant à la valeur $a = 4$, l'équation (11) se présente sous la forme

$$x^3 = (2y)^2 + 1,$$

de sorte que x est aussi une somme de deux carrés, savoir

$$x = \alpha^2 + (2\beta)^2,$$

ce qui est impossible.

IV. L'équation indéterminée

$$x^3 = y^2 + 3 \tag{12}$$

n'est pas résoluble en positifs entiers.

En effet, on aura, aussi dans ce cas,

$$x = \alpha^2 + 3\beta^2,$$

et le théorème II montre clairement qu'une telle valeur de x est inadmissible.

Soit maintenant, dans le théorème II, $\alpha = 1$, $a = 2$, x se présente sous la forme

$$x = \alpha^2 + 2\beta^2,$$

donc nous aurons la proposition:

V. L'équation indéterminée

$$x^3 = y^2 + 2 \tag{13}$$

n'admet qu'une seule solution en positifs entiers, savoir

(13 bis) $$x = 3, \quad y = 5.$$

Quant aux valeurs $\alpha = 1$, $a = 4$, nous aurons à démontrer cette autre proposition:

VI. L'équation indéterminée

(14) $$x^3 = y^2 + 4$$

admet deux solutions en positifs entiers, savoir

(14 bis) $$\begin{cases} x = 5, \quad y = 11 \\ x = 2, \quad y = 2. \end{cases}$$

Soit tout d'abord y impair, x aura la même propriété; de plus, x est une somme de deux carrés, savoir

$$x = \alpha^2 + 4\beta^2,$$

et la première des solutions (14 bis) est une conséquence immédiate du théorème II.

Soit ensuite, dans (14), y un nombre pair, x aura la même propriété; posons donc $2x$ et $2y$ au lieu de x et y, il nous reste à démontrer cette autre proposition:

VII. L'équation indéterminée

(15) $$2x^3 = y^2 + 1$$

n'admet qu'une seule solution en positifs entiers, savoir

(15 bis) $$x = y = 1.$$

Remarquons que x se présente sous la forme

$$x = \alpha^2 + \beta^2,$$

puis appliquons la formule

$$2(p^2 + q^2) = (p + q)^2 + (p - q)^2,$$

il résulte, en vertu de (1), que α et β satisfont à une de ces deux conditions:

$$(\alpha+\beta)\left((\alpha-\beta)^2 \pm 2\alpha\beta\right) = \pm 1$$
$$(\alpha-\beta)\left((\alpha+\beta)^2 \pm 2\alpha\beta\right) = \pm 1,$$

savoir

$$\alpha+\beta = \pm 1, \quad (\alpha-\beta)^2 \pm 2\alpha\beta = \pm 1$$
$$\alpha-\beta = \pm 1, \quad (\alpha+\beta)^2 \pm 2\alpha\beta = \pm 1.$$

Cela posé, on aura une seule condition de la forme

$$4\alpha\beta \pm 2\alpha\beta = 1 \pm 1,$$

ce qui exige nécessairement $\alpha\beta = 0$, savoir $\alpha = 0$, $\beta = \pm 1$, parce que l'hypothèse $\alpha\beta = 1$, $\alpha = \beta = 1$ est inadmissible; car x est, en vertu de (15) un nombre impair; c'est-à-dire que nous aurons précisément la solution (15 bis), ce qui donnera la seconde des solutions (14 bis).

Les deux théorèmes V et VI sont dus à Fermat[1], et le premier de ces propositions n'est autre chose que l'observation XLII sur Diophante[2]. Plus tard Fermat a communiqué cette proposition remarquable à Frenicle, et c'est ce dernier géomètre que Fermat a en vue quand il écrit, dans une lettre, datée mercredi 15 août 1657 et adressée à Digby[3]:

»Je lui avois écrit qu'il n'y a qu'un seul nombre quarré en entiers qui, joint au binaire, fasse un cube, et que ledit quarré est 25, auquel si vous ajoutez 2, il se fait 27, qui est cube. Il a peine à croire cette proposition négative et la trouve un peu hardie et trop générale.

Mais, pour augmenter son étonnement, je dis que, si on cherche un quarré qui, ajouté à 4, fasse un cube, il

[1] Œuvres, t. II, pp. 345, 375.
[2] Ibid. t. I, p. 333.
[3] Ibid. t. II, p. 345.

n'en trouvera jamais que deux en nombres entiers, savoir 4 et 121. Car 4 ajouté à 4 fait 8 qui est cube, et 121 ajouté à 4 fait 125 qui est aussi cube. Mais, après cela, toute l'infinité des nombres n'en sauroit fournir un troisième qui ait la même propriété!«

Le P. TH. PEPIN[1] remarque, avec raison, que la démonstration des deux théorèmes susdits, communiquée par LEGENDRE[2], n'est pas rigoureuse, parce qu'elle suppose $x = p^2 + 2$ au lieu de $x = p^2 + 2q^2$, faute que le savant géomètre a redressée, dans son Mémoire que nous venons de citer.

Du reste, la faute susdite est très curieuse, comparée avec les formules (1), (12), (13) de l'article XIV.

XVII. D'autres applications.

Il est intéressant, ce me semble, que les formules générales que nous venons de développer permettent de donner une nouvelle démonstration de l'identité (10) de l'article XIV, identité qui est la conséquence immédiate du théorème:

I. L'identité algébrique

$$(1) \qquad \left(f^2(x) + 2g^2(x)\right)^2 (x^2 + 2) = h^2(x) + 2$$

admet, comme seules solutions, les polynomes

$$(2) \quad f(x) = \Phi_{2n\pm 1}(x), \; g(x) = \Psi_{2n}(x), \; h(x) = \Psi_{4n\pm 1}(x).$$

A cet effet, remarquons que la formule (10) de l'article XV donnera

$$(3) \left\{ \begin{aligned} &(\alpha^2 + 2b^2)^2 (\alpha^2 + 2) = \\ &= \left[(a^2 - 2b^2)\,\alpha \pm 4ab\right]^2 + 2\left[a^2 - 2b^2 \mp 2ab\,\alpha\right]^2, \end{aligned} \right.$$

[1] Journal de Mathématiques (3) t. 1, p. 345; 1875.
[2] Théorie des Nombres, t. II, p. 14; 3e édition, Paris 1830.

nous aurons à déterminer a et b, de sorte que cette formule se présente sous la forme

$$(a^2 + 2b^2)^2 (\alpha^2 + 2) = c^2 + 2. \tag{4}$$

Cela posé, il résulte, en vertu de (3),

$$a^2 - 2b^2 \mp 2\alpha ab = \pm 1, \tag{5}$$

savoir

$$a = \pm \alpha b \pm \sqrt{(\alpha^2 + 2) b^2 \pm 1},$$

et l'on aura donc à déterminer b sous forme d'un polynome entier de α, tel que la racine carrée devienne aussi un polynome entier de α.

A cet effet, il faut évidemment supprimer, dans (5), le signe inférieur qui figure au second membre, donc on aura

$$b = \Psi_{2n}(\alpha), \quad \sqrt{(\alpha^2 + 2) b^2 + 1} = \Phi_{2n}(\alpha), \tag{6}$$

de sorte que a se présente sous la forme

$$a = \Phi_{2n}(\alpha) \pm \alpha \Psi_{2n}(\alpha) = \Psi_{2n \pm 1}(\alpha), \tag{6 bis}$$

d'où il résulte, en vertu de (3) et (4),

$$c = (a^2 - 2b^2)\alpha \pm 4ab,$$

savoir

$$c = \alpha \Phi_{2n}^2(\alpha) \pm 2\alpha^2 \Phi_{2n}(\alpha) \Psi_{2n}(\alpha) +$$
$$+ (\alpha^3 + 2\alpha) \Psi_{2n}^2(\alpha) \pm 4 \Phi_{2n}(\alpha) \Psi_{2n}(\alpha),$$

ce qui donnera, après un simple calcul,

$$c = \alpha \left(2\Phi_{2n}^2(\alpha) - 1\right) \pm (\alpha^2 + 2) \Psi_{4n}(\alpha),$$

ou, ce qui est la même chose,

$$c = \alpha \Phi_{4n}(\alpha) \pm (\alpha^2 + 2) \Psi_{4n}(\alpha),$$

de sorte que les formules récursives de Lagrange donnent

$$c = \Phi_{4n \pm 1}(\alpha). \tag{7}$$

Cela posé, il est évident que les formules (6) et (7) donnent immédiatement les solutions (2), savoir la démonstration du théorème I, mais ces deux formules conduiront plus loin encore.

En effet, remarquons que l'équation (1) n'est autre chose que la première des formules (1) de l'article XIV, savoir l'équation de FERMAT qui correspond à la base x^2+2, il résulte, en vertu de la valeur de $h(x)$,

$$\psi_{4n\pm1}(x) = \psi^2_{2n\pm1}(x) + 2\,\psi^2_{2n}(x), \tag{8}$$

savoir la formule (10) de l'article XIV.

Étudions maintenant la formule

$$\left\{\begin{aligned} &(a^2+2\,b^2)^2\,(2\,\alpha^2+1) = \\ &= \left[a^2-2\,b^2 \pm 4\,ab\,\alpha\right]^2 + 2\left[(a^2-2\,b^2)\,\alpha \mp 2\,ab\right]^2, \end{aligned}\right. \tag{9}$$

analogue à (3), nous avons à déterminer a et b, de sorte que cette formule se présente sous la forme

$$(a^2+2\,b^2)^2\,(2\,\alpha^2+1) = 2\,c^2+1, \tag{10}$$

ce qui donnera

$$\left\{\begin{aligned} a^2-2\,b^2 \pm 4\,ab\,\alpha &= \pm 1 \\ (a^2-2\,b^2)\,\alpha \mp 2\,ab &= \pm c. \end{aligned}\right. \tag{10 bis}$$

Or, il est évident que l'équation (10) n'est autre chose que celle-ci

$$(a^2+2\,b^2)^2\left((2\,\alpha)^2+2\right) = (2\,c)^2+2,$$

savoir l'équation (4), de sorte que nous aurons

$$a = \psi_{2n\pm1}(2\,\alpha), \quad b = \psi_{2n}(2\,\alpha), \quad c = \frac{1}{2}\,\Phi_{4n\pm1}(\alpha). \tag{11}$$

Nous avons encore à citer ici le théorème, analogue à I:

II. L'identité algébrique

$$(f^2(x) + g^2(x))^2 (x^2 + 1) = h^2(x) + 1 \tag{12}$$

admet, comme seules solutions, les polynomes

$$f(x) = \varphi_{n\pm 1}(x), \;\; g(x) = \psi_n(x), \;\; h(x) = \psi_{2n\pm 1}(x). \tag{13}$$

La démonstration est analogue à la précédente, et les formules (12) et (13) donnent l'identité (12) de l'article XI, savoir

$$\psi_{2n+1}(x) = \psi_{n+1}^2(x) + \psi_n^2(x). \tag{14}$$

CHAPITRE V

L'équation de Théon de Smyrne.

XVIII. Formules générales.

Il est évident que le nombre 2 est la plus petite de toutes les bases, mais cette base est aussi une des plus intéressantes, parce que les nombres A_n et B_n, déterminés par l'équation correspondante de FERMAT

$$A_n^2 - 2B_n^2 = (-1)^n, \tag{1}$$

jouent un rôle fondamental dans la théorie de l'équation générale de FERMAT, nous le verrons dans ce qui suit.

Remarquons que les A_n et les B_n sont les numérateurs, respectivement les dénominateurs des réduites de la fraction continue

$$\sqrt{2} = [1, (2)], \tag{2}$$

savoir

$$\begin{cases} \frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \frac{239}{169}, \frac{577}{408}, \frac{1393}{985}, \\ \frac{3363}{2378}, \frac{8119}{5741}, \frac{19601}{13860}, \frac{47321}{33461}, \ldots, \end{cases} \tag{3}$$

il résulte les formules récursives

$$\begin{cases} A_n = 2A_{n-1} + A_{n-2} \\ B_n = 2B_{n-1} + B_{n-2}. \end{cases} \tag{4}$$

Il est très intéressant que THÉON DE SMYRNE[1] (Theon

[1] Jahrbuch über die Fortschritte der Mathematik, t. 14 (1882), p. 132—133.

Smyrnaeus) a connu les relations numériques

$$2\cdot 1^2-1^2=1^2,\ 2\cdot 5^2-1=7^2,\ 2\cdot 29^2-1=41^2,\ 2\cdot 169^2-1=239^2;$$

c'est pourquoi nous avons rattaché à son nom l'équation de Fermat dont il s'agit ici.

Remarquons encore, en passant, que M. E. Lemoine[1] a donné la résolution complète de l'équation (1), sans »appliquer la fraction continue«, mais en cherchant la valeur générale de x_n, déterminée par les formules récursives

$$x_n = 2x_{n-1}+x_{n-2},\quad x_0 = a,\quad x_1 = b,$$

savoir précisément les formules récursives (4). Or, je ne vois ni la différence entre cette méthode et la méthode ordinaire ni l'avantage de la méthode »nouvelle«.

Revenons maintenant aux nombres A_n et B_n, puis remarquons qu'ils se présentent aussi sous la forme

$$A_n = \varphi_n(1),\quad B_n = \psi_n(1), \tag{5}$$

il résulte immédiatement, en vertu des développements de l'article XI, une suite de relations linéaires, que nous pouvons déduire aussi immédiatement des formules récursives (4), en appliquant la conclusion de m à $m+1$, savoir:

$$A_n = B_n+B_{n-1},\quad B_n = A_{n-1}+B_{n-1} \tag{5}$$

$$A_n = \frac{A_{n+1}-A_{n-1}}{2} = \frac{B_{n+1}+B_{n-1}}{2} \tag{6}$$

$$B_n = \frac{A_n+A_{n-1}}{2} = \frac{A_{n+1}-A_n}{2} = \frac{B_{n+1}-B_{n-1}}{2}. \tag{7}$$

On voit, du reste, que les formules (5) se présentent aussi sous cette autre forme

[1] Journal de Sciencias Mathematicas et Astronomicas publicado pelo Dr. F. Gomes Teixeira, t. 21, p. 68—76; 1892. Citation d'après Jahrbuch über die Fortschritte der Mathematik, t. 24 (1892), p. 179.

(8) $$A_n \pm B_n = B_{n\pm 1}.$$

Quant aux formules non-linéaires, nous citons d'abord celles-ci:

(9) $$B_{n+1} B_{n-1} = B_n^2 + (-1)^n$$

(10) $$4 B_n^4 + A_n^4 = B_{2n}^2 + 1$$

(11) $$B_{n+1}^2 - B_n^2 - 2 B_n B_{n+1} = (-1)^n,$$

tirées directement des identités, démontrées dans l'article XI, et c'est la même chose pour ces deux autres formules

(12) $$\left\{\begin{aligned} B_{2n+1} &= B_n^2 + B_{n-1}^2 \\ 2 B_{2n} &= B_{n+1}^2 - B_{n-1}^2. \end{aligned}\right.$$

Appliquons ensuite l'équation (1), les formules (12) se présentent aussi sous cette autre forme

(12 bis) $$\left\{\begin{aligned} 2 B_{2n+1} &= A_n^2 + A_{n+1}^2 \\ 4 B_{2n} &= A_{n+1}^2 - A_{n-1}^2. \end{aligned}\right.$$

Les formules récursives de Lagrange donnent ici

(13) $$B_{2n} = 2 A_n B_n$$

(14) $$A_{2n} = A_{2n}^2 + 2 B_{2n}^2,$$

d'où, en vertu de l'équation (1),

(15) $$A_{2n} = 2 A_n^2 - (-1)^n = 4 B_n^2 + (-1)^n,$$

de sorte que la première des formules (6) donnera

(16) $$A_{2n+1} = A_{n+1}^2 - A_n^2 + (-1)^n = 2 B_{n+1}^2 - 2 B_n^2 - (-1)^n;$$

de plus, nous aurons, en vertu de (11),

(17) $$A_{2n+1} = 4 B_n B_{n+1} + (-1)^n.$$

Quant aux formules (15), posons pour abréger

$$B_{2n} = 2 \nu_n, \quad B_{2n+1} = 2 \varrho_n + 1,$$

nous aurons

$$(18) \qquad A_{4n} = 16\nu_n^2 + 1, \quad A_{4n+2} = 16\varrho_n(\varrho_n + 1) + 3.$$

Soit maintenant p un facteur premier de A_{2n}, on voit, en vertu de (14), que le nombre -2 est résidu quadratique de p, ce qui donnera, en vertu de la dernière des formules (15):

I. Les facteurs premiers des A_{4n} sont tous de la forme $8\nu + 1$, tandis que les facteurs premiers des A_{4n+2} sont ou de la forme $8\nu + 1$ ou de la forme $8\nu + 3$.

On voit, en vertu de (3), que le nombre premier 3 est du rang 4; c'est-à-dire que les B_{4n} et les A_{4n+2} représentent l'ensemble des B_m et des A_m qui sont divisibles par 3.

On voit de même que le nombre premier 5 est du rang 3, de sorte qu'une puissance quelconque de 5 est du rang impair, et il résulte donc, en vertu des remarques faites sur les nombres (35 bis) de l'article XIII:

II. Les nombres $5^{2\varrho+1}$ et $2 \cdot 5^{\varrho}$ sont toujours des bases de première espèce.

Quant au nombre premier 2, il est du rang 2, ce qui donnera la proposition:

III. Soit l'indice n de la forme $2^{\nu}(2\varrho + 1)$, B_n est précisément divisible par 2^{ν}.

De plus, nous aurons à démontrer cette autre proposition:

IV. Soit n un entier, égal à 3 au moins, on aura toujours

$$(19) \qquad B_{2^n} = 3 \cdot 2^n (a^2 + b^2),$$

où a et b sont de parité différente.

En effet, prenons pour point de départ les valeurs

$$B_4 = 3 \cdot 2^2, \quad A_4 = 4^2 + 1,$$

nous aurons

$$B_8 = 3 \cdot 2^3 (4^2 + 1),$$

savoir une expression de la forme (19), et la conclusion de m à $m+1$ est évidente, parce que A_{2^n} se présente toujours sous la forme

$$A_{2^n} = p^2 + q^2.$$

Quant aux facteurs premiers des nombres B_{2n+1}, qui sont tous de la forme $4\nu + 1$, M. J. PEROTT[1], en étudiant l'équation

$$x^2 - 2q^2y^2 = 1,$$

où q est un nombre premier de la forme susdite, a essayé, avec un certain succès, de déterminer la forme de q, de sorte que l'équation susdite soit résoluble en positifs entiers. C'est-à-dire que M. PEROTT a essayé de déterminer la forme des facteurs premiers des nombres B_{2n+1}, ou, ce qui est la même chose, la forme des nombres premiers du rang impair, pour la base $a = 2$.

Revenons maintenant aux nombres A_n et B_n, il est évident que plusieurs des résultats que nous venons d'obtenir sont intimement liés à l'équation indéterminée

$$x^2 + y^2 = 2z^2, \tag{20}$$

équation qui a, comme solutions générales,

$$\begin{aligned} \pm x &= \alpha^2 - \beta^2 \pm 2\alpha\beta = (\alpha \pm \beta)^2 - 2\beta^2 \\ \pm y &= \alpha^2 - \beta^2 \mp 2\alpha\beta = (\alpha \mp \beta)^2 - 2\beta^2 \\ z &= \alpha^2 + \beta^2, \end{aligned}$$

où α et β sont premiers entre eux et de parité différente.

Soit maintenant, dans (20), $y = 1$, on aura

$$x = A_{2n+1}, \quad z = B_{2n+1}, \tag{21}$$

[1] Journal de Crelle, t. 102, p. 185—223; 1887.

tandis qu'il résulte, en vertu de l'expression de y,

$$(\alpha \mp \beta)^2 - 2\beta^2 = (-1)^\nu,$$

ce qui donnera

$$\alpha \mp \beta = A_\nu, \quad \beta = B_\nu,$$

savoir

$$\alpha = A_\nu \pm B_\nu = B_{\nu \pm 1}$$

$$\alpha \pm \beta = B_{\nu \pm 1} \pm B_\nu = \pm A_{\nu \pm 1}.$$

Cela posé, la valeur de x deviendra

$$\pm x = A_{\nu \pm 1}^2 - 2B_\nu^2 = A_{\nu \pm 1}^2 - A_\nu^2 + (-1)^\nu,$$

ce qui donnera, en vertu de (16) et (21),

$$\nu = n \quad \text{ou} \quad \nu = n + 1,$$

et l'on aura donc

$$z = B_{2n+1} = B_n^2 + B_{n+1}^2,$$

savoir la formule (12).

XIX. Des puissances biquadratiques.

Parmi les problèmes qui se rattachent à l'équation de FERMAT

$$x^2 - ay^2 = \pm 1$$

un des plus intéressants est la question si un des nombres x et y peut être un carré exact.

Quant à l'équation de THÉON DE SMYRNE

$$A_n^2 - 2B_n^2 = (-1)^n, \tag{1}$$

il est très facile de démontrer la proposition:

I. Le nombre $A_1 = 1$ représente la seule solution possible de l'équation

$$A_n = p^2. \tag{2}$$

En effet, EULER[1] a démontré que l'équation indéterminée

[1] Commentarii Academiæ Petropolitanæ, t. 10 (1738), p. 130—139; 1747.

$$x^4 + 1 = 2y^2,$$

qui correspond à (1) et (2), pour n impair, n'admet qu'une seule solution en nombres entiers, savoir $x = y = 1$, tandis que l'équation

$$x^4 - 1 = 2y^2,$$

qui correspond à (1) et (2), pour n pair, n'admet que la seule solution en nombres entiers $x = 1$, $y = 0$.

Quant aux B_m, on aura de même:

II. Aucun des nombres B_{2n} ne peut être un carré, savoir l'équation

$$B_{2n} = p^2 \tag{3}$$

est impossible.

Remarquons que l'équation (3) n'est autre chose que celle-ci

$$2A_nB_n = p^2,$$

nous aurons, parce que A_n est toujours impair,

$$A_n = r^2, \ B_n = 2s^2, \ p = 2rs. \tag{4}$$

Or, la première de ces équations n'est possible que pour $n = 1$, ce qui donnera $B_1 = 1$, et la valeur $2s^2$, indiquée par la seconde des formules (5), n'a aucun sens.

Quant à l'équation

$$B_{2n+1} = p^2, \tag{5}$$

supplémentaire à (3), elle admet des solutions. On aura, en effet,

$$B_1 = 1^2, \ B_7 = 13^2, \tag{5 bis}$$

mais j'ignore s'il y a d'autres solutions de l'équation (5), équivalente à celle-ci

$$x^2 + 1 = 2y^4. \tag{6}$$

La dernière des valeurs spéciales, indiquées dans (5 bis), est assez singulière. En effet, il résulte, en vertu de (1),

$$(7) \qquad B_{2n+1}^2 = \left(\frac{A_{2n+1}+1}{2}\right)^2 + \left(\frac{A_{2n+1}-1}{2}\right)^2,$$

ce qui donnera la proposition:

III. Le carré de B_{2n+1} est toujours la somme des carrés de deux nombres consécutifs.

Inversement, l'équation indéterminée

$$(8) \qquad y^2 = x^2 + (x+1)^2$$

donnera immédiatement

$$(2x+1)^2 - 2y^2 = -1,$$

savoir

$$(8 \text{ bis}) \qquad y = B_{2n+1}, \quad x = \frac{A_{2n+1}-1}{2}.$$

Cela posé, les valeurs numériques $B_7 = 169$, $A_7 = 239$ donnent

$$13 = 2^2 + 3^2, \quad 13^4 = 119^2 + 120^2;$$

c'est-à-dire que les deux équations indéterminées simultanées

$$(9) \qquad x = y^2 + (y+1)^2, \quad x^4 = z^2 + (z+1)^2$$

admettent les solutions en positifs entiers

$$x = 13, \quad y = 2, \quad z = 119,$$

mais y en a-t-il d'autres?

M. E. de Jonquières[1] a postulé que les deux équations indéterminées simultanées

$$(10) \qquad x = y^2 + (y+1)^2, \quad x^2 = z^2 + (z+1)^2$$

n'admettent, abstraction faite de la solution triviale $x = 1$, $y = z = 0$, qu'une seule solution en positifs entiers, savoir:

$$x = 5, \quad y = 1, \quad z = 3;$$

c'est-à-dire que les nombres

[1] Nouvelles Annales (2) t. 17, pp. 241—247, 289—310; 1878.

$$B_1 = 1, \ B_3 = 5$$

représentent les seules solutions possibles de l'équation

$$(11) \qquad B_{2n+1} = p^2 + (p+1)^2,$$

ou, ce qui est la même chose,

$$(11 \text{ bis}) \qquad 2B_{2n+1} = (2p+1)^2 + 1,$$

mais, malheureusement la démonstration de M. DE JONQUIÈRES est fausse.

En effet, B_{2n+1} étant la somme de deux carrés, il est possible de déterminer une expression de la forme

$$B_{2n+1} = x^2 + y^2,$$

de sorte que nous aurons, en vertu de (7),

$$x^2 - y^2 = \frac{A_{2n+1} \pm 1}{2}, \ 2xy = \frac{A_{2n+1} \mp 1}{2},$$

mais le géomètre distingué suppose que x et y soient les valeurs déterminées par la formule (11), ce qui est naturellement inadmissible.

On voit que cette faute est analogue à celle mentionnée dans l'article XVI, concernant la démonstration des propositions de FERMAT.

Du reste, la démonstration de M. DE JONQUIÈRES serait rigoureuse, pourvu que la représentation de B_{2n+1} sous forme d'une somme de deux carrés n'admette qu'une seule solution, ce qui n'a cependant pas lieu, nous le verrons dans l'article XXXI.

Or, on n'a pas encore réussi, que je sache, à démontrer ce fameux postulat de M. DE JONQUIÈRES; c'est-à-dire que les résultats, qu'en ont tirés LUCAS[1] et GERONO[2] ne sont point démontrés jusqu'ici.

[1] Nouvelles Annales (2) t. 18, p. 74—77; 1879.
[2] Ibid. (2) t. 17. p. 381—383; 1878.

Revenons maintenant à l'équation (5), il résulte, en vertu de la formule (12) de l'article précédent,

$$p^2 = B_n^2 + B_{n+1}^2, \tag{12}$$

ce qui donnera

$$p = \alpha^2 + \beta^2, \quad B_{2\nu} = 2\alpha\beta, \quad B_{2\nu\pm1} = \alpha^2 - \beta^2, \tag{12 bis}$$

où il faut supposer $2\nu = n$ ou $2\nu = n+1$, selon que n est pair ou impair, mais comment déterminer ces deux positifs entiers α et β?

Chose curieuse, l'équation (11) se présente aussi dans cet autre théorème:

IV. Soit p un nombre premier, et soit

$$A_{4n+2} = px^2, \tag{13}$$

p est nécessairement de la forme $8\nu + 3$, et B_{2n+1} se présente sous forme d'une somme des carrés de deux nombres consécutifs.

En effet, la formule (13) donnera, en vertu de la formule (15) de l'article précédent,

$$px^2 = (2B_{2n+1} + 1)(2B_{2n+1} - 1). \tag{14}$$

Or, le premier des facteurs qui figurent au second membre de (14) étant de la forme $4\nu + 3$, le second, au contraire, de la forme $4\nu + 1$, il est évident que p est de la forme $8\nu + 3$, parce que A_{4n+2} n'est jamais, en vertu de la proposition I de l'article précédent, divisible par un nombre premier de la forme $8\nu + 7$.

Cela posé, il résulte, en vertu de (14)

$$2B_{2n+1} \pm 1 = pt^2, \quad 2B_{2n+1} \mp 1 = u^2, \quad x = tu,$$

ce qui donnera

$$pt^2 = u^2 \pm 2, \quad 4B_{2n+1} = pt^2 + u^2,$$

où il faut lire, au second membre de la première de ces formules, u^2+2, parce que 2 n'est pas résidu quadratique du nombre premier $p = 8\nu + 3$, de sorte que nous aurons

$$(15) \qquad pt^2 = u^2 + 2, \quad 4B_{2n+1} = pt^2 + u^2$$

savoir

$$(16) \qquad 2B_{2n+1} = u^2 + 1, \quad B_{2n+1} = \left(\frac{u+1}{2}\right)^2 + \left(\frac{u-1}{2}\right)^2,$$

ce qui est précisément la formule (11), mais il faut remarquer que le nombre u est ici une solution de la première des formules (15), savoir d'une forme particulière.

Quant à la formule (15) en question, nous la connaissons déjà du théorème IV de l'article IV, et nous la retrouvons encore une fois, dans l'article XXIII.

Revenons maintenant aux formules (16), nous connaissons deux solutions de ces équations, savoir

$$B_1 = 1, \quad u = 1; \quad B_3 = 5, \quad u = 3,$$

ce qui donnera, comme solutions de (13),

$$(17) \qquad A_2 = 3\cdot 1^2; \quad A_6 = 11\cdot 3^2.$$

Or, supposons vrai le postulat de M. E. DE JONQUIÈRES, ces deux valeurs représentent les seules solutions possibles de l'équation (13).

Quant aux nombres B_{2n}, nous avons à démontrer le théorème:

V. Soit p un nombre premier, l'équation

$$(18) \qquad B_{2n} = px^2$$

n'admet que deux solutions, savoir

$$(18 \text{ bis}) \quad \begin{cases} p = 2, & n = 1, & x = 1, & B_2 = 2\cdot 1^2 \\ p = 3, & n = 2, & x = 2, & B_4 = 3\cdot 2^2. \end{cases}$$

Soit tout d'abord $p = 2$, on aura, en vertu de (18),

$$A_n B_n = x^2,$$

ce qui donnera

$$A_n = r^2, \ B_n = s^2, \ x = rs.$$

Or, la première de ces expressions n'étant admissible que pour $n = 1$, on aura $r = s = x = 1$, savoir la première des solutions (18 bis).

Soit ensuite, dans (18), p un nombre premier impair, x est nécessairement un nombre pair, de sorte que B_{2n} est divisible par 4, ce qui exige que n soit un nombre pair, savoir $n = 2\nu$. Posons ensuite $x = 2z$, l'équation (18) se présente sous la forme

$$(19) \qquad 2pz^2 = A_{2\nu} B_{2\nu}.$$

Supposons maintenant $A_{2\nu}$ divisible par le nombre premier p, nous aurons

$$A_{2\nu} = pr^2, \ B_{2\nu} = 2s^2, \ z = rs, \ x = 2rs,$$

et la valeur de $B_{2\nu}$ est précisément celle que nous venons de déterminer, savoir la première des solutions (18 bis), de sorte que nous aurons

$$\nu = s = 1, \ A_2 = pr^2 = 3,$$

ce qui donnera

$$p = 3, \ r = s = 1, \ x = 2,$$

savoir la seconde des solutions (18 bis).

Supposons, en second lieu, p et A_{2n} premiers entre eux, il résulte, en vertu de (18),

$$A_{2\nu} = r^2, \ B_{2\nu} = 2ps^2, \ z = rs, \ x = 2rs,$$

ce qui est impossible, parce que $A_{2\nu}$ ne peut jamais être un carré.

Cela posé, la première des solutions (18 bis) donnera:

VI. L'équation indéterminée

(20) $$x^2 - 8y^4 = 1$$

n'admet qu'une seule solution en positifs entiers, savoir

(20 bis) $$x = 3, \quad y = 1.$$

On voit que ce corollaire n'est autre chose que la célèbre proposition de FERMAT[1]:

VII. Le nombre 1 est le seul nombre trigone qui soit une puissance biquadratique.

En effet, l'équation

$$x(x+1) = 2y^4,$$

savoir

$$(2x+1)^2 = 8y^2 + 1,$$

n'est autre chose que l'équation (20), donc nous aurons, comme la seule solution possible de l'équation proposée, $x = y = 1$.

Cette proposition de FERMAT a été retrouvée par EULER[2] et LEGENDRE[3], néanmoins elle est parfois attribuée à ce dernier géomètre[4].

Comme application de la proposition VI, nous avons à démontrer cette autre:

VIII. L'équation indéterminée

(21) $$x^4 - 8x^2y^2 + 8y^4 = 1$$

n'admet qu'une seule solution en positifs entiers, savoir

(21 bis) $$x = y = 1.$$

On aura, en effet, en vertu de (21),

[1] Œuvres, t. II, p. 402.

[2] Commentarii Academiæ Petropolitanæ, t. 10 (1738), p. 140—141; 1747.

[3] Théorie des Nombres, t. p. 7.

[4] Voir par exemple GERONO: Nouvelles Annales (2) t. 16, p. 230—234; 1877.

$$x^2 = 4y^2 \pm \sqrt{8y^4+1},$$

ce qui donnera, en vertu de (20), le résultat susdit.

Remarquons, en passant, que le P. Th. Pepin[1] a étudié l'équation

$$x^4 - 8x^2y^2 + 8y^4 = z^4,$$

de laquelle (21) est un cas très spécial.

Quant à la seconde des solutions (18 bis), elle donnera le corollaire:

IX. L'équation indéterminée

$$x^2 - 18y^4 = 1 \tag{22}$$

n'admet qu'une seule solution en positifs entiers, savoir

$$x = 17, \quad y = 2. \tag{22 bis}$$

En terminant cet article, nous avons encore à donner la proposition:

X. Soit p un positif entier, sans facteurs quadratiques, une expression de la forme

$$A_{2n}(2) = px^2 \tag{23}$$

est impossible, à moins que

$$x = B_\nu(p), \quad 2B_n(2) = A_\nu(p). \tag{23 bis}$$

La formule (23) donnera, en effet, en vertu de la dernière des expressions (15) de l'article XVIII,

$$4B_n^2(2) + (-1)^n = px^2,$$

savoir

$$\left(2B_n(2)\right)^2 - px^2 = (-1)^{n-1},$$

ce qui donnera immédiatement les relations (23 bis).

[1] Memoire della Accademia Pontificia dei Nuovi Lincei, t. 14, p. 71—85; 1898. Citation d'après Jahrbuch über die Fortschritte der Mathematik, t. 29 (1898). p. 158—159.

Soit n un nombre pair, on voit que p est nécessairement une base de première espèce.

XX. Des nombres A_n.

Dans l'article XVIII, nous avons démontré que A_{2n} est toujours un nombre de la forme $2p^2 \pm 1$. Quant aux nombres A_{2n+1} nous avons à démontrer les deux théorèmes:

I. Le nombre

(1) $$A_1 = 1$$

représente la seule solution possible de l'équation

(2) $$A_{2n+1} = 2p^2 + 1.$$

II. Les nombres

(3) $$A_1 = 1, \quad A_3 = 7$$

représentent les seules solutions possibles de l'équation

(4) $$A_{2n+1} = 2p^2 - 1.$$

Ces deux théorèmes sont, en effet, des conséquences immédiates des formules (16) de l'article XVIII, savoir

(5) $$A_{2n+1} = A_{n+1}^2 - A_n^2 + (-1)^n = 2B_{n+1}^2 - 2B_n^2 - (-1)^n,$$

car les formules (2) et (4) donnent toujours, quelle que soit la parité de n, une des deux équations

$$B_{n+1}^2 - B_n^2 = p^2$$
$$A_{n+1}^2 - A_n^2 = 2p^2,$$

d'où il résulte, en vertu des formules (5) et (7) de l'article XVIII,

(6) $$A_n A_{n+1} = p^2$$

(7) $$2B_n B_{n-1} = p^2.$$

Cela posé, il résulte, en vertu du théorème I de l'article précédent, que la formule (6) n'est possible que pour

$p = 1$, ce qui donnera la première des solutions (3). Quant à l'équation (7), on aura

$$B_{2\nu} = 2r^2, \quad B_{2\nu\pm 1} = s^2, \quad p = 2rs, \tag{8}$$

où $2\nu = n$ ou $2\nu = n - 1$, selon que n est pair ou impair, ce qui donnera, en vertu du théorème V de l'article précédent, $\nu = 1$, $r = 1$.

Or, $B_3 = 5$ n'étant pas un carré, la seconde des équations (8) donnera $B_1 = 1$, $s = 1$, savoir $p = 2$, et l'on trouve donc la seconde des solutions (3). Remarquons encore que l'hypothèse $\nu = 0$ donnera, en vertu de (8), $r = 0$, $s = 1$, $p = 1$, savoir la solution (1).

Introduisons maintenant, dans l'équation de Théon,

$$A_{2n+1} = 2x^2 \pm 1, \quad B_{2n+1} = y,$$

il résulte, en vertu des deux théorèmes I et II, le corollaire:

III. L'équation indéterminée

$$x^4 + (x^2 + 1)^2 = y^2 \tag{9}$$

n'est pas résoluble en nombres entiers, abstraction faite de la solution triviale $x = 0$, $y = 1$, tandis que l'équation analogue

$$x^4 + (x^2 - 1) = y^2 \tag{9 bis}$$

admet deux solutions en positifs entiers, savoir

$$x = y = 1; \quad x = 2, \quad y = 5.$$

Dans l'article XVIII, nous avons aussi démontré que les A_{2n} se présentent toujours sous la forme $4p^2 \pm 1$. Quant aux nombres A_{2n+1}, nous avons à démontrer les deux théorèmes:

IV. Le nombre $A_1 = 1$ représente la seule solution possible de l'équation

(10) $$A_{2n+1} = 4p^2 + 1.$$

V. Aucun des nombres A_{2n+1} ne se présente sous la forme

(11) $$A_{2n+1} = 4p^2 - 1.$$

En effet, les formules (5) donnent ici une de ces deux équations
$$B_{n+1}B_n = 2p^2$$
$$A_nA_{n-1} = 4p^2.$$

Or, la dernière de ces équations est impossible, parce que les A_{2n} sont des nombres impairs, tandis que la première n'est possible que pour la valeur triviale $n = 0$, ce qui donnera $p = 0$, savoir la solution $A_1 = 1$ de l'équation (10).

Cela posé, on aura ici le corollaire:

VI. L'équation indéterminée

(12) $$(2x^2)^2 + (2x^2 \pm 1)^2 = y^2$$

n'est pas résoluble en positifs entiers, abstraction faite de la solution triviale $x = 0$, $y = 1$.

On voit que le théorème II n'est autre chose qu'une proposition fameuse, indiquée par Fermat[1], dans une lettre adressée à Frenicle, savoir:

VII. Les équations indéterminées simultanées

(13) $$x = 2y^2 - 1, \quad x^2 = 2z^2 - 1$$

admettent seulement deux solutions en positifs entiers, savoir

(13 bis) $$x = y = z = 1; \quad x = 7, \quad y = 2, \quad z = 5.$$

Cette proposition de Fermat est très intéressante, et il

[1] Œuvres, t. II, p. 434.

semble que le grand géomètre en a communiqué sa démonstration, ce qui est très rare.

En effet, d'après LUCAS[1], on lit dans les manuscrits de BOUILLIOU (Bullialdus):

»M. Fermat a envoyé à M. Frenicle la démonstration par laquelle il preuve qu'il n'y a aucun autre nombre que le seul 7 qui, estant le double d'un carré —1, soit la racine quarrée de la mesme nature (c'est-à-dire qui soit le double d'un carré —1).

7 est double du quarré 4, —1, c'est-à-dire, 8—1, et son quarré 49 est le double du quarré 25, —1, c'est-à-dire 50—1.«

Or, la lettre de FERMAT et la réponse de FRENICLE semblent toutes deux perdues, et la proposition susdite de FERMAT a causé beaucoup de difficultés aux géomètres qui ont cherché de la démontrer, mais en vain[2]. Le P. PEPIN[3] a par exemple indiqué que, si les équations indéterminées simultanées (13) ont d'autres solutions que celles indiquées par FERMAT, savoir les nombres (13 bis), ces solutions contiennent au moins 3849 chiffres.

Or, au moment où le P. PEPIN a publié sa Note susdite, deux géomètres ont déjà réussi à résoudre le problème difficile dont il s'agit.

[1] Nouvelles Annal. (2), t. 18, p. 75; 1879.

[2] Voir par exemple la Note de LUCAS dans les Nouvelles Annales, (2) t. 18, p. 74—77; 1879.

[3] Jahrbuch über die Fortschritte der Mathematik, t. 15 (1883), p. 195; t. 16 (1884), p. 154. La Note du P. PEPIN est publiée dans les Atti della Accademia Pontificia dei Nuovi Lincei t. 26 (ou t. 36) p. 23—33; 1884. Les indications du Jahrbuch concernant les numéros des tomes de la publication périodique susdite sont, aux environs de l'année 1884, très confuses. De plus, dans le premier lieu cité, on lit 3848 chiffres, dans le second 3849!

En effet, GERONO[1] a démontré que les seules solutions en positifs entiers de l'équation indéterminée

$$(14) \qquad 1 + x + x^2 + x^3 = (x+1)(x^2+1) = y^2$$

sont

$$x = 1, \ y = 2; \ x = 7, \ y = 20,$$

et l'on voit que l'équation (14) se décompose en celles-ci

$$x + 1 = 2m^2, \ x^2 + 1 = 2n^2, \ y = 2mn,$$

dont les deux premiers sont identiques à (13).

Or, ni le Jahrbuch über die Fortschritte der Mathematik[2], ni LUCAS, dans sa Note susdite sur la proposition de FERMAT, n'ont remarqué que GERONO a résolu le problème en question.

Plus tard, GENOCCHI[3] a trouvé une solution presque identique à celle de GERONO.

XXI. Des nombres B_n.

Il est très intéressant, ce me semble, que les nombres B_{2n+1} ont des propriétés analogues à celles que nous venons de démontrer pour les A_{2n+1}, savoir:

I. Les nombres

$$(1) \qquad B_1 = 1, \ B_3 = 5$$

représentent les seules solutions possibles de l'équation

$$(1 \text{ bis}) \qquad B_{2n+1} = 4p^2 + 1.$$

En effet, appliquons le théorème II de l'article XVIII, il s'agit de résoudre les deux équations indéterminées simultanées

[1] Nouvelles Annales (2) t. 16, p. 230—234; 1877.

[2] Voir t. 9 (1877), p. 137.

[3] Jahrbuch, t. 15 (1883), p. 145. La démonstration est reproduite, sans commentaires, dans les Nouvelles Annales (3) t. 2, p. 306—310; 1885.

(2) $$x = 4p^2 + 1, \quad x^2 = y^2 + (y+1)^2.$$

Soit tout d'abord y un nombre pair, on aura donc

(3) $$y = 2\alpha\beta, \quad y + 1 = \alpha^2 - \beta^2, \quad x = \alpha^2 + \beta^2,$$

ce qui donnera

$$\alpha^2 - 2\alpha\beta - \beta^2 = 1, \quad x = 2\beta^2 + 2\alpha\beta + 1,$$

ou, ce qui est la même chose,

(3 bis) $$(\alpha - \beta)^2 - 2\beta^2 = 1, \quad \alpha - \beta = A_{2\nu}, \quad \beta = B_{2\nu}.$$

Cela posé, il résulte, en vertu des deux expressions de x,

(4) $$2p^2 = \beta(\beta + \alpha) = B_{2\nu} A_{2\nu+1},$$

équation qui n'est pas résoluble en positifs entiers, de sorte qu'il ne nous reste que la solution triviale de (3 bis), savoir $\alpha = 1$, $\beta = 0$, ce qui donnera

$$y = p = 0, \quad x = 1 = B_1.$$

Soit, en second lieu, dans (2), y un nombre impair, on aura

$$y + 1 = 2\alpha\beta, \quad y = \alpha^2 - \beta^2, \quad x = \alpha^2 + \beta^2,$$

savoir

$$(\beta + \alpha)^2 - 2\alpha^2 = 1, \quad x = 2\alpha^2 - 2\alpha\beta + 1,$$

ce qui donnera

(4 bis) $$\beta + \alpha = A_{2\nu}, \quad \alpha = B_{2\nu}, \quad 2p^2 = B_{2\nu} A_{2\nu-1},$$

et cette dernière équation n'étant possible que pour $\nu = 1$, on aura donc

$$p = 1, \quad x = 5 = B_3.$$

Gerono[1] a résolu les deux equations indéterminées simultanées (2), sans remarquer qu'elles se rattachent à l'équation de Théon.

II. Le nombre $B_1 = 1$ représente la seule solution possible de l'équation

[1] Nouvelles Annales (2) t. 17, p. 521—523; 1878.

(5) $$B_{2n+1} = 2p^2 + 1.$$

Il est évident que la démonstration de ce théorème est analogue à celle que nous venons d'établir pour le théorème précédent. Il faut simplement remplacer les équations (4) et (4 bis) par celles-ci

$$p^2 = B_{2\nu} A_{2\nu+1}, \quad p^2 = B_{2\nu} A_{2\nu-1},$$

équations qui sont impossibles pour une valeur positive de l'indice ν, de sorte qu'il ne nous reste que la solution triviale $p = 0$, $x = 1 = B_1$.

III. L'équation

(6) $$B_{2n+1} = 4p^2 - 1$$

est impossible.

En effet, soit y un nombre pair, la dernière des équations (2) donnera

$$\beta^2 = \alpha^2 - 2\alpha\beta - 1, \quad x = 2\alpha^2 - 2\alpha\beta - 1,$$

de sorte que nous aurons

$$\alpha - \beta = A_{2\nu}, \quad \beta = B_{2\nu}, \quad 2p^2 = A_{2\nu} B_{2\nu+1},$$

ce qui est impossible.

L'hypothèse y impair donnera de même

$$\alpha^2 = \beta^2 + 2\alpha\beta - 1, \quad x = 2\beta^2 + 2\alpha\beta - 1,$$

savoir

$$\beta + \alpha = A_{2\nu}, \quad \alpha = B_{2\nu}, \quad 2p^2 = B_{2\nu-1} B_{2\nu},$$

ce qui est également impossible.

IV. Le nombre $B_1 = 1$ représente la seule solution possible de l'équation

(7) $$B_{2n+1} = 2p^2 - 1.$$

La démonstration est tellement analogue aux précédentes qu'il nous semble inutile de l'établir plus amplement.

XXII. Résolution de problèmes diverses.

Les nombres A_n et B_n, étudiés dans les articles précédents, jouent un rôle essentiel dans la Théorie des Nombres, parce qu'ils permettent de résoudre plusieurs problèmes d'une forme simple, problèmes parmi lesquels nous avons à considérer quelques-uns, pour la plupart bien connus.

I. Déterminer un nombre trigone qui soit un carré exact.

L'équation indéterminée dont il s'agit, savoir

$$x(x+1) = 2y^2, \tag{1}$$

se transforme en celle-ci

$$(2x+1)^2 = 8y^2 + 1,$$

ce qui donnera

$$x = \frac{A_{2n} - 1}{2}, \quad y = \frac{B_{2n}}{2}, \tag{1 bis}$$

et ces nombres donnent aussi la solution complète de ces deux autres équations indéterminées

$$\left\{ \begin{aligned} 1 + 2 + 3 + \dots + x &= y^2 \\ 1^3 + 3^3 + 3^3 + \dots + x^3 &= y^4. \end{aligned} \right. \tag{3}$$

II. Déterminer deux nombres trigones, dont le premier soit le double du second.

Dans ce cas, il s'agit de résoudre l'équation indéterminée

$$x(x+1) = 2y(y+1), \tag{3}$$

ou, ce qui est la même chose,

$$(2x+1)^2 = 2(2y+1)^2 - 1,$$

de sorte que nous aurons

$$x = \frac{A_{2n+1} - 1}{2}, \quad y = \frac{B_{2n+1} - 1}{2}, \tag{3 bis}$$

et il est évident que ces nombres donnent aussi la solution complète de ces deux autres équations indéterminées

$$(4)\quad \begin{cases} 1+2+3+\ldots+x = 2(1+2+3+\ldots+y). \\ 1^3+2^3+3^3+\ldots+x^3 = 4(1^3+2^3+3^3+\ldots+y^3). \end{cases}$$

Dans l'»Educational Times«[1] on a traité le problème plus général

$$x(x+1) = ny(y+1),$$

où n est un positif entier; cependant la solution donnée de ce problème ne me paraît pas complète, et je me réserve de revenir à l'équation susdite, dans une autre occasion.

III. *Déterminer un nombre x qui soit un carré plus ou moins un, tel que $2x$ ait la même propriété.*

Les équations indéterminées simultanées

$$(5)\qquad x = y^2 \pm 1, \quad 2x = z^2 \pm 1$$

donnent immédiatement

$$z^2 - 2y^2 = \pm 1,$$

savoir

$$(5\text{ bis})\quad z = A_n, \; y = B_n, \; x = B_n^2 + (-1)^n = B_{n+1}B_{n-1}.$$

IV. *Déterminer un nombre x qui soit un carré plus ou moins un, tandis que $2x$ soit un carré moins ou plus 2.*

Ici nous avons à résoudre les équations indéterminées simultanées

$$x = y^2 \pm 1, \quad 2x = z^2 \mp 2,$$

savoir

$$2y^2 = z^2 \mp 4,$$

de sorte que y et z sont tous deux des nombres pairs. Posons $y = 2\beta$, $z = 2\alpha$, il résulte

[1] Jahrbuch über die Fortschritte der Mathematik, t. 32 (1901), p. 197.

$$2\beta^2 = \alpha^2 \mp 1,$$

et nous aurons donc

$$\alpha = A_n, \quad \beta = B_n, \quad y = 2B_n, \quad z = 2A_n,$$

d'où il résulte finalement

(6 bis) $$x = 4B_n^2 + (-1)^n = A_{2n}.$$

V. Déterminer un carré, dont le double soit un carré plus ou moins 4.

L'équation indéterminée

(7) $$2x^2 = y^2 \pm 4$$

montre clairement que x et y sont tous deux des nombres pairs. Posons $x = 2\alpha$, $y = 2\beta$, nous aurons

$$\beta^2 - 2\alpha^2 = \mp 1,$$

ce qui donnera

(7 bis) $$x = 2B_n, \quad y = 2A_n.$$

VI. Déterminer deux carrés consécutifs, dont la somme soit un carré.

L'équation indéterminée

(8) $$x^2 + (x+1)^2 = y^2,$$

savoir

$$(2x+1)^2 - 2y^2 = -1$$

est déjà résolue, dans l'article XIX; on aura

(8 bis) $$x = \frac{A_{2n+1} - 1}{2}, \quad x + 1 = \frac{A_{2n+1} + 1}{2}, \quad y = B_{2n+1}.$$

Considérons maintenant un triangle rectangulaire, dont les côtés sont exprimés par des nombres entiers, il est évident que l'équation (8) détermine de tels triangles, dont les cathètes ont la différence un.

Posons pour abréger

$$a_n = \frac{A_{2n-1} - 1}{2}, \quad b_n = B_{2n-1}, \quad n \geqq 1, \tag{9}$$

la solution complète de l'équation indéterminée (8) est représentée par les valeurs

$$x = a_n, \quad y = b_n. \tag{10}$$

Or, les formules récursives de LAGRANGE

$$A_{2n+1} = 3A_{2n-1} + 4B_{2n-1}$$
$$B_{2n+1} = 2A_{2n-1} + 3B_{2n-1}$$

donnent, en vertu de (9), ces autres formules récursives

$$\left\{ \begin{aligned} a_{n+1} &= 3a_n + 2b_n + 1 \\ b_{n+1} &= 4a_n + 3b_n + 2 \end{aligned} \right. \tag{11}$$

qui permettent de déterminer successivement les nombres a_m et b_m, à l'aide de la solution triviale $a_0 = 0$, $b_1 = 1$.

La première des formules (11) est due à M. TH. MUIR[1]; quant à la seconde, elle montre que l'équation indéterminée

$$3x + 4y + 2 = u^2 + v^2 \tag{12}$$

est résoluble en positifs entiers. Mais il me semble un problème très difficile de déterminer toutes les valeurs positives entières de x, y, u, v qui satisfont à cette équation, ce qui exige, en effet, de déterminer toutes les représentations de la forme

$$B_{2n+1} = u^2 + v^2,$$

et je ne crois pas que la solution de l'équation (12), donnée dans l'»Educational Times«[2] soit complète.

[1] Proceedings of the Royal Society of Edinburgh, t. 23, p. 264—267; 1901.

[2] Jahrbuch über die Fortschritte der Mathematik, t. 35 (1904), p. 206—207.

VII. Démontrer que $x = 1$, $x = 5$ sont les seuls positifs entiers qui satisfassent aux deux conditions

$$x = y^2 + 1, \quad 2x^2 = u^2 + 1. \tag{13}$$

On aura

$$u = A_{2n+1}, \quad x = B_{2n+1},$$

et le théorème I de l'article précédent montre que la première des équations (13) n'est possible que pour $n = 0$ et $n = 1$, ce qui donnera précisément $x = 1$, $x = 5$.

Cela posé, il résulte, en vertu de (5), que $x = 1$ et $x = 5$ sont les seuls positifs entiers qui satisfassent aux trois conditions

$$x = y^2 + 1, \quad 2x = z^2 + 1, \quad 2x^2 = t^2 + 1, \tag{14}$$

et l'on voit que les deux premières de ces équations donnent une infinité de solutions, tandis que la première et la dernière ne donnent que les deux solutions susdites.

Quant aux deux dernières des équations (14), il est évident que z et t sont tous deux des nombres impairs. Posons $z = 2\alpha + 1$, $t = 2\beta + 1$, il résulte

$$x = \alpha^2 + (\alpha + 1)^2, \quad x^2 = \beta^2 + (\beta + 1)^2,$$

savoir le problème de M. E. de Jonquières, problème qui se présente par conséquent aussi sous cette autre forme

$$x = \frac{z^2 + 1}{2}, \quad x^2 = \frac{t^2 + 1}{2}. \tag{15}$$

Enfin, nous avons à résoudre un problème, régardé mais pas résolu par Moret-Blanc[1] et par Lucas[2], savoir:

VIII. Démontrer que les équations indéterminées simultanées

$$x = 6y^2, \quad x + 1 = z^2, \quad 2x + 1 = u^2 \tag{16}$$

[1] Nouvelles Annales (2) t. 15, p. 46—48; 1875.
[2] Ibid. (2) t. 17, p. 381; 1877.

n'admettent qu'une seule solution en positifs entiers, savoir

(16 bis) $x = 24, \ y = 2, \ z = 5, \ u = 7.$

On voit, en éliminant x, que le système (16) est équivalent à deux des trois équations suivantes, prises arbitrairement,

(17) $$u^2 - 2z^2 = -1$$

(18) $$u^2 - 3(2y)^2 = 1$$

(19) $$z^2 - 6y^2 = 1$$

Étudions tout d'abord les deux premières de ces équations, il résulte, en vertu de (17),

(20) $$u = A_{2n+1}(2), \quad z = B_{2n+1}(2),$$

tandis que la seconde donnera

(21) $$u \pm 1 = 2\alpha^2, \quad u \mp 1 = 3\beta^2, \quad y = \alpha\beta.$$

Or, la première de ces expressions n'est, en vertu des théorèmes I et II de l'article XX, possible que pour

$$u = 1, \quad \alpha = 0, \quad 1 = 3\beta^2$$
$$u = \alpha = 1, \quad \beta = 0$$
$$u = 7, \quad \alpha = 2, \quad \beta = 1,$$

et l'on voit que le premier de ces systèmes est inadmissible, que le second donnera la solution triviale $x = y = 0$, $z = u = 1$, tandis que le troisième conduira à la solution indiquée par les formules (16 bis).

Lucas, en étudiant les équations (16), donne seulement $u + 1 = 2\alpha^2$ au lieu de la première des formules (21).

Remarquons encore que les équations (17) et (18) donnent immédiatement la proposition:

IX. L'équation

(22) $$A_{2n+1}(2) = A_{2\nu}(3)$$

n'admet qu'une seule solution, savoir

$$n = \nu = 1,\quad A_3(2) = A_2(3) = 7 \tag{22 bis}$$

En second lieu, les équations (18) et (19) donnent cette autre proposition:

X. L'équation

$$B_n(6) = B_\nu(12) = \frac{1}{2} B_{2\varrho}(3) \tag{23}$$

ne donne que la seule solution

$$n = \nu = \varrho = 1,\quad B_1(6) = B_1(12) = \frac{1}{2} B_2(3) = 2. \tag{23 bis}$$

Moret-Blanc, dans son essai maladroit de résoudre les équations (16) indique empiriquement la proposition X.

Quant aux équations (17) et (19), elles donnent la proposition:

XI. L'équation

$$B_{2n+1}(2) = A_\nu(6) \tag{24}$$

n'admet qu'une seule solution, savoir

$$n = \nu = 1,\quad B_3(2) = A_1(6) = 5. \tag{24 bis}$$

Enfin, nous aurons, en multipliant les deux premières des équations (16), puis appliquant la troisième, cette autre proposition que nous avons à étudier plus amplement dans les articles XXVI et XXVIII:

XII. L'équation indéterminée

$$u^4 - 24t^2 = 1 \tag{25}$$

n'a qu'une seule solution en positifs entiers, savoir

$$u = 7,\quad t = 10. \tag{25 bis}$$

CHAPITRE VI

Des puissances d'un nombre premier.

XXIII. De la base $a = (2\nu + 1)^{2\varrho+1}$.

Dans les articles VIII et X, nous avons déjà mentionné un théorème concernant les nombres premiers de la forme $4\nu + 1$, théorème que nous avons à démontrer ici, à un autre point de vue, savoir:

I. Soit $4\nu + 1$ un nombre premier, la puissance impaire $(4\nu + 1)^{2\varrho+1}$ est toujours une base de première espèce, donc l'équation de Fermat

$$x^2 - (4\nu + 1)^{2\varrho+1} y^2 = -1 \tag{1}$$

est résoluble en positifs entiers.

A cet effet, nous désignons par $2\sigma + 1$ un nombre premier impair quelconque, il est évident que l'équation de Fermat

$$x^2 - ay^2 = 1, \quad a = (2\sigma + 1)^{2\varrho+1}, \quad \varrho \geqq 0, \tag{2}$$

est toujours résoluble en positifs entiers.

Cela posé, nous désignons par x et y les plus petites des solutions de l'équation (2), ou, ce qui est la même chose,

$$(x + 1)(x - 1) = ay^2. \tag{3}$$

Soit maintenant x un nombre pair, les deux facteurs $x + 1$ et $x - 1$ sont premiers entre eux, donc on aura, en vertu de (3),

$$x \pm 1 = ap^2, \quad x \mp 1 = q^2, \quad y = pq, \tag{4}$$

ce qui donnera

$$2x = ap^2 + q^2, \quad q^2 - ap^2 = \mp 2, \tag{5}$$

d'où

$$x = q^2 \pm 1 = ap^2 \mp 1. \tag{6}$$

Soit, au contraire, x un nombre impair, les deux facteurs $x+1$ et $x-1$ ont le plus grand commun diviseur 2, et l'on aura, en vertu de (3),

$$x \pm 1 = 2ap^2, \quad x \mp 1 = 2q^2, \quad y = 2pq \tag{7}$$

ce qui donnera

$$x = 2q^2 \pm 1 = 2ap^2 \mp 1, \tag{8}$$

d'où

$$x = ap^2 + q^2, \quad q^2 - ap^2 = \mp 1. \tag{9}$$

Cela posé, nous avons à étudier séparément les deux hypothèses σ pair et σ impair.

Soit tout d'abord σ un nombre pair, le nombre premier en question est de la forme $4\nu + 1$, et il est évident que la dernière des équations (5) est impossible, parce que son premier membre est multiple de 4; c'est-à-dire qu'il ne nous reste, dans ce cas, que les formules (7).

Or, x et y étant les plus petites solutions en positifs entiers de l'équation (2), on aura nécessairement, en vertu de la dernière des formules (9),

$$q^2 - ap^2 = -1; \tag{10}$$

c'est-à-dire que l'équation (1) est résoluble en positifs entiers, et a est par conséquent une base de première espèce.

Remarquons, en passant, que la formule (10) donnera

$$q = A_1, \quad p = B_1,$$

de sorte que nous aurons, en vertu de (7) et (8),

$$y = 2A_1 B_1 = B_2, \quad x = 2A_1^2 + 1 = A_2.$$

Soit ensuite σ un nombre impair, le nombre premier est de la forme $4\nu+3$, et la puissance $(4\nu+3)^{2\varrho+1}$ est une base de seconde espèce, ce qui exclut la dernière des formules (9), parce que x et y sont les plus petites solutions de l'équation (2); c'est-à-dire qu'il ne nous reste que les équations (5).

Cela posé, nous retrouvons évidemment les formules de l'article IV, mais la méthode que nous venons d'appliquer ici ne donne aucun éclaircissement sur la nature des nombres p et q, qui figurent dans les expressions de x et y, savoir de A_1 et B_1, indiquées dans les formules (4) et (6).

Remarquons, en passant, que la dernière des formules (5) se rattache au théorème IV de l'article XIX.

Du reste, notre démonstration du théorème I n'est qu'une légère modification de celle que Legendre[1] a appliquée pour établir le cas spécial du théorème susdit qui correspond à $\varrho = 0$.

Revenons maintenant au cas général, nous aurons à démontrer quelques autres théorèmes concernant l'équation de Fermat

$$x^2 - ay^2 = \pm 1, \quad a = (2\nu+1)^{2\varrho+1}, \tag{11}$$

où $2\nu+1$ est un nombre premier.

II. Une équation de la forme

$$A_m(a) = 2\alpha^2 \pm 1 \tag{12}$$

n'est jamais possible pour m impair.

Étudions tout d'abord l'équation (11) qui correspond à la valeur -1 au second membre, a est une base de première espèce, et l'indice m de $A_m(a)$ est nécessairement un nombre impair. Introduisons ensuite, dans (11), la valeur (12) de $A_m(a)$, il résulte

[1] Théorie des Nombres, t. I, p. 65, 3e édition, Paris 1830.

$$4\alpha^2(\alpha^2 \pm 1) = ay^2 - 2,$$

ce qui est impossible et pour y pair et pour y impair.

Quant à la valeur $+1$ au second membre de (11), on aura, en vertu de (12),

$$4\alpha^2(\alpha^2 \pm 1) = ay^2, \tag{13}$$

et il est évident que α ne peut pas être divisible par le nombre premier $2\nu+1$, parce que le premier membre de (13) est, dans ce cas, divisible par une puissance paire du nombre premier susdit, tandis que le second membre est divisible par une puissance impaire.

Cela posé, il est évident que y est divisible par 2α, savoir

$$y = 2\alpha z, \tag{14}$$

ce qui donnera, en vertu de (13),

$$\alpha^2 \pm 1 = az^2,$$

ou, ce qui est la même chose,

$$\alpha = A_p(a), \quad z = B_p(a),$$

donc on aura, en vertu de (14)

$$y = B_{2p}(a), \quad x = A_{2p}(a). \tag{15}$$

Soit le nombre premier de la forme $4\nu+3$, il résulte de la formule (23) de l'article IV que les A_{2n+1}, tirés de (11), sont toujours un carré plus ou moins un. Quant aux nombres premiers de la forme $4\nu+1$, nous aurons à démontrer le théorème:

III. Soit, dans l'équation (11), ν un nombre pair, l'équation

$$A_m(a) = \alpha^2 \pm 1, \quad a = (4\nu+1)^{2\varrho+1}, \tag{16}$$

n'est possible pour aucune valeur paire de l'indice m.

Soit, en effet, m un nombre pair, il faut supprimer la valeur -1 au second membre de (11), et l'on aura, en introduisant, au lieu de x, la valeur (16),

$$\alpha^2(\alpha^2 \pm 2) = ay^2.$$

On voit, comme dans la démonstration précédente, que α ne peut pas être divisible par le nombre premier $4\nu + 1$, de sorte que l'on aura nécessairement $y = \alpha z$, ce qui donnera

$$\alpha^2 \pm z = az^2,$$

et cette équation est impossible, parce que son premier membre est de la forme $4\sigma - 1$, le second, au contraire, de la forme $4\tau + 1$.

XXIV. De l'équation $x^4 - ay^2 = 1$.

Soit $2\nu + 1$ un nombre premier, on connaît des équations de FERMAT

$$x^2 - ay^2 = \pm 1, \quad a = (2\nu + 1)^{2\varrho+1},$$

où le nombre x est un carré, ce qui a lieu par exemple pour $a = 5$.

Dans ce cas, on aura en effet

$$9^2 - 5 \cdot 4^2 = 1, \quad A_2(5) = 3^2, \quad B_2(5) = 2^2,$$

de sorte que x et y sont tous deux des carrés.

Or, il est très intéressant, ce me semble, que les équations indéterminées de la forme

$$(1) \qquad x^4 - ay^2 = 1, \quad a = (2\nu + 1)^{2\varrho+1},$$

où $2\nu + 1$ est un nombre premier, se rattachent intimement à l'équation de THÉON DE SMYRNE.

En effet, soit, dans (1), x un nombre pair, on aura

$$x^2 \pm 1 = ap^2, \quad x^2 \mp 1 = q^2, \quad y = pq,$$

et la deuxième de ces équations est impossible; c'est-à-dire que x est nécessairement un nombre impair.

Cela posé, il est évident que x^2+1 est toujours un nombre de la forme $4\sigma+2$, tandis que x^2-1 est multiple de 8, de sorte que nous avons à étudier deux systèmes d'équations indéterminées, savoir

$$x^2+1 = 2q^2, \quad x^2-1 = 8ar^2, \quad y = 4qr \tag{2}$$

$$x^2+1 = 2aq^2, \quad x^2-1 = 8r^2, \quad y = 4qr. \tag{3}$$

Or, il résulte de la première des équations (2)

$$x = A_{2n+1}(2), \quad q = B_{2n+1}(2),$$

tandis que la seconde des équations susdites donnera

$$x \pm 1 = 4\alpha^2, \quad x \mp 1 = 2a\beta^2, \quad r = \alpha\beta \tag{4}$$

$$x \pm 1 = 4a\alpha^2, \quad x \mp 1 = 2\beta^2, \quad r = \alpha\beta. \tag{5}$$

Quant aux équations (4), il résulte

$$x = 2\alpha^2 + a\beta^2, \quad 2\alpha^2 - a\beta^2 = \pm 1,$$

ce qui donnera

$$x = A_{2n+1}(2) = 4\alpha^2 \mp 1;$$

mais, dans l'article XX, nous avons démontré que la valeur $4\alpha^2-1$ est inadmissible, tandis que la valeur $4\alpha^2+1$ exige

$$\alpha = 0, \quad x = 1,$$

ce qui donnera, en vertu de (4), la condition impossible

$$a\beta^2 = 1.$$

Étudions maintenant les équations (5), nous aurons

$$x = \beta^2 + 2a\alpha^2, \quad \beta^2 - 2a\alpha^2 = \mp 1,$$

et, comme dans le cas précédent, en vertu de la première des équations (2),

$$x = A_{2n+1}(2), \quad q = B_{2n+1}(2),$$

ce qui donnera

$$x = A_{2n+1}(2) = 2\beta^2 \pm 1.$$

Or, il résulte des recherches de l'article XX que ces expressions de x ne sont possibles que pour

$$x = 1,\ \beta = 0; \quad x = 7,\ \beta = 1,$$

ce qui n'est pas admissible.

Cela posé, il nous reste seulement les équations (3) qui représentent par conséquent la condition nécessaire et suffisante pour l'existence de l'équation (1).

Remarquons maintenant que la première des équations (3) n'est autre chose que celle-ci

$$x^2 - 2aq^2 = -1, \tag{6}$$

nous aurons la proposition essentielle:

I. *Supposons résoluble en positifs entiers l'équation (1), l'équation (6) aura nécessairement la même propriété, de sorte que la base a est toujours de la forme*

$$a = (4\nu + 1)^{2\varrho+1}, \tag{7}$$

où $4\nu + 1$ est un nombre premier.

On voit donc que cette condition nécessaire exclut dès à présent toutes les bases de la forme

$$a = (4\nu + 3)^{2\varrho+1}, \tag{8}$$

où $4\nu + 3$ est un premier, mais c'est la même chose pour d'autres valeurs de a.

Soit par exemple $a = 17$, on aura $34 = 6^2 - 2$, ce qui est une base de seconde espèce, et l'équation correspondante (6) n'est pas résoluble en positifs entiers.

On voit du reste que

$$A_{4n}(2) = 4B_{2n}^2(2) + 1$$

est toujours une base de première espèce, tandis que

$$2A_{4n}(2) = 4A_{2n}^2(2) - 2$$

est toujours de seconde espèce.

Revenons maintenant à l'équation (6), nous aurons

$$x = A_{2n+1}(2a), \quad q = B_{2n+1}(2a), \tag{9}$$

tandis que la deuxième des équations (3) donnera

$$x = A_{2k}(2), \quad r = \frac{1}{2}B_{2k}(2), \tag{9 bis}$$

donc nous avons démontré le théorème:

II. Soit $4\nu + 1$ un nombre premier, l'égalité

$$x = A_{2n+1}(2a) = A_{2k}(2), \quad a = (4\nu + 1)^{2\varrho+1}, \tag{10}$$

où les indices n et k sont à déterminer convenablement, représente la condition nécessaire et suffisante pour la résolution en positifs entiers de l'équation proposée (1).

Supposons maintenant remplie la condition (10), puis supposons déterminés les indices n et k, la valeur correspondante de y se détermine, en vertu de la dernière des équations (3), par l'expression

$$y = 4qr = 2B_{2k}(2)\,B_{2n+1}(2a). \tag{11}$$

Soit particulièrement $a = 5$, la fraction continue

$$\sqrt{10} = \left[3, (6)\right]$$

donnera

$$A_1(10) = A_2(2) = 3; \quad B_1(10) = 1, \quad B_2(2) = 2,$$

d'où il résulte

$$x = 3,\ y = 4,\quad 3^4 - 5 \cdot 2^4 = 1.$$

Remarquons encore que la proposition I donnera immédiatement cette autre:

III. Soit $4\nu + 3$ un nombre premier, l'équation indéterminée

$$(12) \qquad x^2 - 4ay^4 = 1,\ a = (4\nu + 3)^{2\varrho+1},$$

n'est pas résoluble en positifs entiers, ou, ce qui est la même chose, une expression de la forme

$$(13) \qquad B_n(a) = 2p^2$$

n'est pas admissible.

Remarquons que, dans (12), x est impair, nous aurons

$$x \pm 1 = 2a\alpha^4,\ x \mp 1 = 2\beta^4,\ y = \alpha\beta,$$

ce qui donnera

$$(14) \qquad \beta^4 - a\alpha^4 = \mp 1,$$

où il faut par conséquent supprimer le signe supérieur qui figure au second membre, parce que a est une base de seconde espèce, et la proposition I montre clairement que l'équation (14), ainsi obtenue, n'est pas résoluble en positifs entiers.

XXV. De la base $2a = 2(2\nu + 1)^{2\varrho+1}$.

Dans les recherches de l'article précédent, nous avons appliqué l'équation de Fermat

$$(1) \qquad x^2 - 2ay^2 = 1,\ a = (2\nu + 1)^{2\varrho+1},$$

où $2\nu + 1$ est un nombre premier, c'est pourquoi nous nous sommes proposé d'étudier plus amplement une telle équation, et nous avons tout d'abord à démontrer le théorème:

I. Soit, avec la définition susdite, $2a$ une base de seconde espèce, l'équation indéterminée

$$2q^2 - ap^2 = \mp 1 \tag{2}$$

est résoluble, et il existe de telles solutions p et q de (2) que les nombres $A_1(2a)$ et $B_1(2a)$ se présentent sous la forme

$$A_1(2a) = 4q^2 \pm 1, \quad B_1(2a) = 2pq, \tag{3}$$

et inversement. Soit $A_1(2a)$ de la forme susdite, $2a$ est toujours une base de seconde espèce.

En effet, remarquons que, dans (1), x est toujours impair, nous aurons à regarder ces deux systèmes d'équations indéterminées

$$x \pm 1 = 2ap^2, \quad x \mp 1 = 4q^2, \quad y = 2pq \tag{4}$$

$$x \pm 1 = 4ap^2, \quad x \mp 1 = 2q^2, \quad y = 2pq. \tag{5}$$

Étudions tout d'abord les équations (4), il résulte

$$x = ap^2 + 2q^2, \quad 2q^2 - ap^2 = \mp 1, \quad x = 4q^2 \pm 1. \tag{6}$$

Quant au système (5), on aura

$$x = q^2 + 2ap^2, \quad q^2 - 2ap^2 = \mp 1, \tag{7}$$

mais la seconde de ces équations est impossible. En premier lieu, il faut supprimer la valeur -1, parce que $2a$ est une base de seconde espèce, et nous aurons en outre, en vertu de la première des équations (7),

$$x = A_1(2a) > q,$$

ce qui exclut la valeur $+1$ au second membre de la dernière des équations susdites.

Cela posé, il nous reste seulement le système (4), ce qui entraîne précisément les expressions (3) de $A_1(2a)$ et $B_1(2a)$.

Inversement, soit $A_1(2a)$ de la forme (3), il résulte, en vertu de (1),

$$16q^4 \pm 8q^2 = 2ay^2,$$

de sorte que y est un nombre pair, et l'on aura donc

$$q^2(2q^2 \pm 1) = ay_1^2, \quad y = 2y_1. \tag{8}$$

Or, il est évident que les deux facteurs qui figurent au premier membre de (8) sont premiers entre eux, ce qui entraîne que q ne peut pas être divisible par le nombre premier $2\nu + 1$, parce que le premier membre est, dans ce cas, divisible par une puissance paire de ce premier, le second par une puissance impaire.

Cela posé, y_1 est nécessairement divisible par q, savoir $y_1 = qz$, et l'on aura donc

$$2q^2 \pm 1 = az^2,$$

savoir la seconde des équations (6), de sorte que le système (5) est exclu, et $2a$ est par conséquent une base de seconde espèce.

Il est évident que le théorème I est appliquable à tous les nombres premiers de la forme $4\nu + 3$, mais c'est la même chose pour les nombres premiers de la forme $4\nu + 1$, comme nous l'avons remarqué dans l'article précédent.

Du reste, je me réserve de revenir, dans une autre occasion, au problème que nous venons d'étudier ici.

XXVI. Résolution de l'équation $x^4 - 2(2\nu+1)^{2\varrho+1}y^2 = 1$.

Il est très intéressant, ce me semble, qu'il est possible de résoudre complètement l'équation indéterminée

$$x^4 - 2ay^2 = 1, \quad a = (2\nu + 1)^{2\varrho+1}, \tag{1}$$

où $2\nu + 1$ est un nombre premier impair quelconque.

Remarquons tout d'abord que x est impair, il est évident que x^2+1 est de la forme $8\varrho+2$, tandis que x^2-1 est de la forme 8σ; de plus, aucun de ces deux nombres ne peut être un carré.

Cela posé, il est évident que l'équation (1) est équivalente au système

$$(2) \qquad x^2+1 = 2r^2, \quad x^2-1 = 4as^2, \quad y = 2rs,$$

où r est par conséquent impair, s pair.

Or, la première des équations (2) donnera

$$(3) \qquad x = A_{2n+1}(2), \quad r = B_{2n+1}(2),$$

tandis qu'il résulte, en vertu de la deuxième,

$$(4) \qquad x \mp 1 = 2a\alpha^2, \quad x \mp 1 = 2\beta^2, \quad s = \alpha\beta,$$

donc on aura

$$(4\text{ bis}) \qquad x = 2\beta^2 \pm 1, \quad \beta^2 - a\alpha^2 = \mp 1,$$

d'où, en vertu des théorèmes I et II de l'article XX,

$$x = 1, \quad x = 7.$$

On voit que la première de ces valeurs est inadm ssible, tandis que la seconde donnera $\beta = 2$, de sorte qu'il résulte, en vertu de la première des équations (4),

$$a\alpha^2 = 3, \quad a = 3, \quad \alpha = 1,$$

ce qui donnera

$$s = 2, \quad r = 5, \quad y = 20,$$

et nous avons donc démontré le théorème curieux:

I. Soit $2\nu+1$ un nombre premier, l'équation indéterminée

$$(5) \qquad x^4 - 2ay^2 = 1, \quad a = (2\nu+1)^{2\varrho+1}, \quad \varrho \geqq 0,$$

n'est jamais résoluble en positifs entiers, à moins que

(5 bis) $$\varrho = 0, \ \ \nu = 1, \ \ 2\nu + 1 = 3;$$

dans ce cas on aura la seule solution possible

(6) $$x = 7, \ \ y = 20.$$

On voit que ce théorème représente une généralisation très étendue du théorème XII de l'article XXII; du reste, il conduira immédiatement à ces deux autres théorèmes:

II. Soit $2\nu + 1$ un nombre premier, une équation de la forme

(7) $$B_{2n}(2a) = p^2, \ \ a = (2\nu + 1)^{2\varrho+1}$$

n'est jamais possible.

En effet, dans l'équation de Fermat

(8) $$x^2 - 2ay^2 = \pm 1,$$

dont il s'agit ici, x est toujours un nombre impair; c'est-à-dire que l'équation

$$2 A_n B_n = p^2,$$

équivalente à (7), donnera

$$A_n = \alpha^2, \ \ B_n = 2\beta^2, \ \ p = \alpha\beta,$$

de sorte que nous aurons

(9) $$\alpha^4 - 2a(2\beta^2)^2 = \pm 1.$$

Or, $\alpha^4 + 1$ étant de la forme $8\sigma + 2$, l'équation (9) est de la forme (5), de sorte qu'il résulte, en vertu du théorème I,

$$a = 3, \ \ \alpha = 7, \ \ 2\beta^2 = 20,$$

ce qui est impossible.

III. Soit, dans (8), ν un nombre impair, une équation de la forme

$$B_{2n}(2a) = 2p^2, \quad a = (4\nu + 3)^{2\varrho+1} \tag{10}$$

n'est jamais possible.

On aura, dans ce cas, en vertu de (10),

$$A_n = \alpha^2, \quad B_n = \beta^2, \quad p = \alpha\beta,$$

ce qui donnera

$$\alpha^4 - 2a\beta^4 = 1,$$

équation qui est, en vertu du théorème I, impossible.

CHAPITRE VII

D'autres bases spéciales.

XXVII. L'équation d'Archimède.

Il est évident que le nombre $3 = 1^2 + 2$ est la plus simple des bases étudiées dans l'article XIV. Posons

$$A_n = \Phi_{2n}(1), \qquad B_n = \Psi_{2n}(1)$$
$$a_n = \Phi_{2n+1}(1), \quad b_n = \Psi_{2n+1}(1),$$

les solutions complètes des deux équations indéterminées

(1) $$x^2 - 3y^2 = 1$$

(2) $$3v^2 = u^2 + 2$$

deviennent

(1 bis) $$x = A_n, \ \ y = B_n$$

(2 bis) $$u = a_n, \ \ v = b_n.$$

Appliquons maintenant la fraction continue

$$\sqrt{3} = \left[1, \ (1, 2)\right],$$

les A_n et les B_n sont les numérateurs, respectivement les dénominateurs des réduites aux indices impairs, en commençant par l'indice 0, savoir

$$\frac{2}{1}, \ \frac{7}{4}, \ \frac{26}{15}, \ \frac{97}{56}, \ \frac{362}{209}, \ldots,$$

tandis que les a_n et les b_n sont les numérateurs, respectivement les dénominateurs des réduites aux indices pairs, savoir

$$\frac{1}{1}, \ \frac{5}{3}, \ \frac{19}{11}, \ \frac{71}{41}, \ \frac{265}{153}, \ldots,$$

Il semble que déjà Archimède[1] a connu une méthode pour la détermination successive des solutions de (1); c'est pourquoi nous rattachons à l'équation susdite le nom du plus grand géomètre de l'Antiquité.

Introduisons maintenant, dans les formules de l'article XIV, la valeur $\alpha = 1$, nous aurons une suite de relations entre les nombres A_n et B_n, a_n et b_n. Or, nous nous bornerons à indiquer ici les plus intéressantes de ces formules nombreuses, savoir

$$A_{2n} = 6B_n^2 + 1, \quad A_{2n+1} = a_{2n+1}^2 + 1 \tag{3}$$

$$B_{2n} = 2A_n B_n, \qquad B_{2n+1} = a_{n+1} b_{n+1} \tag{4}$$

$$2B_n^2 + 1 = b_n b_{n+1}, \quad b_n^2 - 1 = 2B_n B_{n-1} \tag{5}$$

$$2B_{2n} = b_{n+1}^2 - b_n^2, \; B_{2n+1} = B_{n+1}^2 - B_n^2 \tag{6}$$

$$b_{2n\pm 1} = b_{n\pm 1}^2 + 2B_n^2. \tag{7}$$

La formule (7) est bien curieuse, parce que b_{2n+1} est diviseur des deux nombres

$$2B_{2n}^2 + 1, \quad a_{2n+1}^2 + 2$$

qui sont de la forme $x^2 + 2y^2$, mais un des carrés est réduit à un.

Remarquons encore que la première des formules (5) donnera, en vertu de (1) et (3),

$$2A_n^2 + 1 = 3b_n b_{n+1}, \tag{8}$$

formule qui nous permet de démontrer la proposition:

I. L'équation indéterminée

$$3x^2 + 2y^2 = 6xy - 1 \tag{9}$$

[1] Jahrbuch über die Fortschritte der Mathematik, t. 14 (1882), p. 133.

admet une infinité de solutions en positifs entiers, savoir

(9 bis) $$y = A_n, \quad x = \begin{cases} b_n \\ b_{n+1}. \end{cases}$$

On aura, en effet,

$$x = y \pm \sqrt{\frac{y^2 - 1}{3}},$$

savoir

$$y = A_n, \quad x = A_n \pm B_n = \begin{cases} b_{n+1} \\ b_n. \end{cases}$$

Introduisons ensuite, dans (9), les valeurs susdites, puis soustrayons les deux équations ainsi obtenues, il résulte

$$3\,b_n(2\,A_n - b_n) = 2\,A_n^2 + 1 = 3\,b_{n+1}(2\,A_n - b_{n+1}),$$

et nous aurons donc

(10) $$2\,A_n = b_n + b_{n+1}.$$

Remarquons encore que les quatre nombres A_n et B_n, a_n et b_n se déterminent tous à l'aide de la même formule récursive, savoir

(11) $$\alpha_n = 4\,\alpha_{n-1} - \alpha_{n-2}$$

et que les formules récursives de Lagrange

(12) $$\begin{cases} A_n = 2\,A_{n-1} + 3\,B_{n-1} \\ B_n = 2\,B_{n-1} + A_{n-1} \end{cases}$$

donnent

(12 bis) $$\begin{cases} 2\,B_n - A_n = B_{n-1} \\ 2\,A_n - 3\,B_n = A_{n-1} \end{cases}$$

de sorte que nous aurons toujours, pour $n > 1$,

(13) $$2\,B_n > A_n > \frac{3}{2}B_n.$$

Quant à la base 3, le nombre premier 3 est du rang 3, tandis que 7 est du rang 4, de sorte que les nombres A_{4n+2} et B_{4n} représentent l'ensemble des nombres A_m et B_m qui sont divisibles par 7. Mais, y a-t-il d'autres solutions de l'équation

$$(14) \qquad A_{4n+2} = 7p^2$$

que $A_2 = 7$? Problème qui est d'un certain intérêt, nous le verrons dans ce qui suit.

Étudions maintenant les nombres A_n, la proposition I de l'article XXIV donnera immédiatement cette autre:

II. Aucun des nombres A_n ne peut être un carré; car l'équation indéterminée

$$(15) \qquad x^4 - 3y^2 = 1$$

n'est pas résoluble en positifs entiers.

De plus, nous avons à démontrer le théorème:

III. Le nombre $A_1 = 2$ représente la seule solution possible de l'équation

$$(16) \qquad A_n = 2p^2;$$

c'est-à-dire que l'équation indéterminée

$$(27) \qquad 4x^4 - 3y^2 = 1$$

n'admet qu'une seule solution en positifs entiers, savoir

$$x = y = 1.$$

Remarquons tout d'abord que y est impair, de sorte que $3y^2 + 1$ est un nombre de la forme $8\sigma + 4$, il est évident que x est aussi un nombre impair, de sorte que $2x^2 + 1$ est de la forme $8\sigma + 3$, tandis que $2x^2 - 1$ est de la forme $8\sigma + 1$.

Cela posé, il résulte, en vertu de (17),

$$(18) \qquad 2x^2 + 1 = 3u^2, \quad 2x^2 - 1 = v^2, \quad y = uv,$$

car $2x^2 + 1$ et $2x^2 - 1$ sont premiers entre eux, et l'on aura, en vertu de (18), (18 bis) $$4x^2 = 3u^2 + v^2,\ \ 2 = 3u^2 - v^2,$$

ce qui donnera

(19) $$2x \pm v = 3p^2,\ \ 2x \mp v = q^2,\ \ u = pq,$$

parce que $2x$ et v sont, en vertu de la dernière des équations (18), premiers entre eux.

Introduisons ensuite, dans la seconde des formules (18 bis), les valeurs

$$u = pq,\ \ v = \frac{3p^2 - q^2}{2},$$

tirées de (19), il résulte

$$2 = 3p^2q^2 - \left(\frac{3p^2 - p^2}{2}\right),$$

ou, ce qui est la même chose,

$$8 = 12p^2q^2 - (3p^2 - q^2)^2 = 18p^2q^2 - 9p^4 - q^4,$$

savoir

$$8 = 8q^4 - 9(p^2 - q^2)^2,$$

de sorte que nous aurons finalement

$$q^4 - 2\left(\frac{3}{4}(p^2 - q^2)\right)^2 = 1,$$

équation qui n'admet que la seule solution en nombres entiers $p = q = 1$, ce qui donnera $u = v = x = y = 1$.

On voit, que les deux premières des formules (18) donnent, comme corollaire, la proposition:

IV. *L'équation*

(20) $$a_n = A_{2\nu+1}(2)$$

n'admet qu'une seule solution, savoir

(20 bis) $$n = 1,\ \ \nu = 0,\ \ a_1 = A_1(2) = 1.$$

Quant aux nombres B_m, il est facile de démontrer des théorèmes analogues aux précédents, savoir:

V. *Le nombre $B_2 = 4$ représente la seule solution possible de l'équation*

$$B_{2n} = p^2; \tag{21}$$

c'est-à-dire que l'équation indéterminée

$$x^2 - 48y^4 = 1 \tag{21 bis}$$

n'admet qu'une seule solution en positifs entiers, savoir

$$x = 7, \quad y = 1.$$

En effet, il résulte, en vertu de (21),

$$2A_nB_n = p^2.$$

Or, A_n n'étant jamais un carré, $2A_n$ aura nécessairement cette propriété, ce qui n'est possible que pour $n = 1$, savoir $B_2 = 4$.

Mais j'ignore, si l'equation

$$B_{2n+1} = p^2, \tag{22}$$

supplémentaire à (21), admet d'autres solutions que $B_1 = 1$.

VI. Aucun des nombres B_n ne peut être le double d'un carré, car l'équation indéterminée

$$x^2 - 12y^4 = 1 \tag{23}$$

n'est pas résoluble en positifs entiers.

Remarquons que les B_{2n+1} sont tous impairs, il nous reste seulement à étudier l'équation

$$B_{2n} = 2A_nB_n = 2p^2,$$

ce qui exige que A_n et B_n soient tous deux des carrés, ce qui est impossible.

Quant aux nombres B_n, nous avons encore à démontrer ici un théorème qui nous sera utile dans l'article qui suit, savoir:

VII. Le nombre $B_1 = 1$ représente la seule solution de l'équation

$$B_{2n+1} = 2p^2 - 1. \tag{24}$$

En effet, soit, dans l'équation

$$x^2 - 3y^2 = 1,$$

y un nombre impair, x est pair et se présente sous la forme $x = 6q \pm 2$, ce qui donnera, en vertu de (24),

$$(4q \pm 1)^2 = (2p^2 - 1)^2 + 4q^2,$$

de sorte que nous aurons

$$4q \pm 1 = \alpha^2 + \beta^2, \quad 2p^2 - 1 = \alpha^2 - \beta^2, \quad q = \alpha\beta,$$

où α et β sont premiers entre eux et de parité différente.

Cela posé, la première et la dernière de ces équations donnent

$$(\alpha - 2\beta)^2 - 3\beta^2 = \pm 1,$$

de sorte qu'il faut supprimer, dans l'expression $x = 6q \pm 2$, le signe inférieur, donc on aura

$$\beta = B_\nu, \quad \alpha - 2\beta = \pm A_\nu, \quad \alpha = 2B_\nu \pm A_\nu,$$

ce qui donnera

$$2p^2 - 1 = 3B_\nu^2 + A_\nu^2 \pm 4A_\nu B_\nu = 2A_\nu^2 \pm 4A_\nu B_\nu - 1,$$

savoir

$$p^2 = A_\nu(A_\nu + 2B_\nu), \tag{25}$$

car $A_\nu - 2B_\nu$ est, en vertu des inégalités (13), un nombre négatif.

Soit maintenant, dans (25), ν un nombre pair, A_ν est de la forme $4\sigma + 2$, parce que le nombre 2 est du rang 2; c'est-à-dire que 2 est le plus grand commun diviseur de A_ν et de $A_\nu + 2B_\nu$, de sorte que nous aurons

$$A_\nu = 2r^2, \quad A_\nu + 2B_\nu = 2s^2, \quad p = 2rs.$$

Or, la première de ces équations n'est, en vertu du théorème III, possible que pour $\nu = r = 1$, ce qui donnera

$$A_\nu + 2B_\nu = 4 = 2s^2,$$

supposition qui n'est pas admissible.

Soit donc ν un nombre pair, A_ν est impair, et les deux facteurs qui figurent au second membre de (25) sont premiers entre eux, de sorte que nous aurons

$$A_\nu = r^2, \quad A_\nu + 2B_\nu = s^2, \quad p = rs,$$

ce qui n'est possible pour aucune valeur positive de ν, de sorte qu'il ne nous reste que la solution triviale $\nu = 0$, savoir $r = s = p = 1$.

XXVIII. Applications diverses.

Le dernier résultat que nous venons d'obtenir, dans l'article précédent, nous permet de démontrer la proposition curieuse:

I. L'équation indéterminée

$$x^3 + 1 = y^2 \tag{1}$$

n'admet qu'une seule solution en positifs entiers, savoir

$$x = 2, \quad y = 3. \tag{2}$$

En effet, remarquons tout d'abord que les deux nombres $x+1$ et $x^2 - x + 1$ sont ou premiers entre eux ou ils ont le plus grand commun diviseur 3. Or $x^2 - x + 1$ n'étant jamais un carré, il résulte donc, en vertu de (1),

$$x + 1 = 3p^2, \quad x^2 - x + 1 = 3q^2, \quad y = 3pq, \tag{3}$$

où p et q sont premiers entre eux, et la deuxième de ces formules se présente sous la forme

$$(2x - 1)^2 + 3 = 3(2q)^2,$$

ce qui donnera, en vertu de la première des formules susdites,

$$(2q)^2 - 3(2p^2 - 1)^2 = 1. \tag{4}$$

Cela posé, il résulte, en vertu du théorème VII de l'article précédent, que l'équation (4) n'est possible que pour $p = q = 1$, ce qui donnera précisément la solution (2).

Quant au théorème que nous venons de démontrer, remarquons, en passant, que CATALAN[1] a énoncé, sans démonstration, le théorème général:

Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes.

C'est-à-dire que l'équation indéterminée

$$x^m = y^n + 1 \tag{5}$$

n'est résoluble en positifs entiers que pour $x = 3$, $y = 2$, $m = 2$, $n = 3$, ce qui est précisément notre équation (1).

LE BESGUE[2] a démontré l'impossibilité de l'équation (5) pour $n = 2$, mais il dit que le théorème général est difficile à démontrer. Plus tard, GERONO[3] a démontré l'impossibilité de l'équation (5), dans le cas où y est un nombre premier.

Quant à notre théorème I, je ne me rappelle pas l'avoir vu complètement démontré, dans la littérature qui mentionne, plus ou moins légèrement, l'équation (1), littérature de laquelle nous citons, outre un auteur anonyme[4], MM. GERONO[5], MEYL[6] et MORET-BLANC[7].

Écrivons maintenant sous la forme

$$x^3 = (y+1)(y-1)$$

l'équation (1), puis remarquons que l'hypothèse

[1] Nouvelles Annales t. 1, p. 520; 1842.
[2] Ibid. t. 9, p. 178—181; 1850.
[3] Ibid. (2) t. 9, p. 469—471; 1870.
[4] Ibid. (2) t. 9, p. 204—206; 1870.
[5] Ibid. (2) t. 9, p. 452; 1870.
[6] Ibid. (2) t. 15, p. 545; 1876.
[7] Ibid. (2) t. 15, p. 44—46; 1876.

$$y+1 = p^3, \quad y-1 = q^3$$

est inadmissible, nous aurons nécessairement

$$y \pm 1 = 2p^3, \quad y \mp 1 = 4q^3, \quad x = 2pq,$$

ce qui donnera

$$p^3 - 2q^3 = \pm 1. \tag{6}$$

Or, cette équation indéterminée étant équivalente à l'équation (1), elle n'admet que la seule solution en positifs entiers $x = y = 1$, qui correspond au signe inférieur au second membre.

Il est très singulier, ce me semble, qu'aucun des auteurs susdits n'ait remarqué que la résolution de l'équation (6), communiquée par Legendre[1], entraîne celle de l'équation (1).

Dans le problème I de l'article XXII, nous avons déterminé les valeurs de n, pour lesquelles la somme des n premiers nombres devient un carré. Or, la proposition I nous permet de résoudre un problème analogue concernant la somme des n premiers nombres carrés, c'est-à-dire de démontrer la proposition:

II. L'équation indéterminée

$$1^2 + 2^2 + 3^2 + \ldots + x^2 = y^3, \tag{7}$$

ou, ce qui est la même chose,

$$x(x+1)(2x+1) = 6y^3, \tag{7 bis}$$

n'admet qu'une seule solution en positifs entiers, savoir

$$x = y = 1. \tag{8}$$

A cet effet, remarquons que les deux nombres

$$x(x+1), \quad 2x+1$$

[1] Théorie des Nombres, t. II, p. 13; 3e édition; Paris 1830.

sont premiers entre eux, puis remarquons que le premier de ces nombres ne peut pas être une puissance, plus élevée que la première, d'un positif entier, il est évident que l'équation (7) conduira à ces deux systèmes d'équations indéterminées simultaneés

$$(9) \qquad x(x+1) = 2t^3, \quad 2x+1 = 3u^3, \quad y = tu$$

$$(10) \qquad x(x+1) = 6t^3, \quad 2x+1 = u^3, \quad y = tu.$$

Or, la première des équations (9) se présentant sous la forme

$$(2x+1)^2 = (2t)^3 + 1,$$

savoir l'équation (1), on aura $x = t = u = y = 1$, ce qui est précisément la solution (8).

Quant aux équations (10), on aura

$$(2x+1)^2 = u^6 = 24t^3 + 1,$$

ou, ce qui est la même chose,

$$(11) \qquad (u^2-1)(u^4+u^2+1) = 24t^3,$$

et il résulte donc, conformément aux remarques faites relativement aux équations (1) et (3), des expressions de la forme

$$(11 \text{ bis}) \qquad u^2-1 = 3^\alpha(2p)^3, \quad u^4+u^2+1 = 3^\beta q^3.$$

Cela posé, je dis que l'on aura nécessairement $\beta = 1$. En effet, les équations (11 bis) donnent immédiatement

$$3u^2 = 3^\beta q^3 - 3^{2\alpha}(2p)^6,$$

ce qui exige $\beta = 1$, parce que u n'est pas divisible par 3. Posons donc, dans (11 bis), $\beta = 1$, il résulte, en vertu de (11),

$$3^\alpha p^3 q^3 = t^3,$$

c'est-à-dire que α est divisible par 3, de sorte que la première des équations (11 bis) se présente sous la forme

$$u^2 - 1 = (6p)^3,$$

équation qui n'est pas résoluble en positifs entiers.

Quant aux premiers membres des formules (7), il est facile de démontrer cette autre proposition:

III. La somme des n premiers nombres carrés ne peut jamais être le double d'un carré.

Conformément aux remarques faites relativement à l'équation (7 bis), l'équation indéterminée dont il s'agit ici, savoir

$$x(x+1)(2x+1) = 12y^2 \tag{12}$$

conduira à ces autres

$$x(x+1) = 12z^2, \quad 2x+1 = u^2, \quad y = zu,$$

et les deux premières de ces équations donnent l'équation d'Archimède

$$u^4 - 3(4z)^2 = 1, \tag{13}$$

qui n'est pas résoluble en positifs entiers.

Remarquons, en passant, que cette autre équation

$$x(x+1)(2x+1) = 18y^2 \tag{14}$$

a la même propriété que (12), celle de ne pas être résoluble en positifs entiers, parce qu'elle entraîne nécessairement que $2x+1$ soit un carré, de sorte que nous aurons une équation de la forme

$$p^4 - (2q)^2 = 1.$$

équation qui n'est pas résoluble en positifs entiers.

Cela posé, il est curieux, ce me semble, que l'équation indéterminée

$$1^4 + 2^4 + 3^4 + \ldots + x^4 = 2y^2, \tag{15}$$

ou, ce qui est la même chose,

$$x(x+1)(2x+1)(3x^2+3x-1) = 60y^2 \tag{15 bis}$$

soit résoluble en positifs entiers.

En effet, remarquons que les deux nombres

$$x(x+1)(2x+1), \quad 3x(x+1)-1$$

sont premiers entre eux, à moins que

$$2x+1, \quad 3x(x+1)-1$$

n'aient le plus grand commun diviseur 7, puis remarquons qu'une équation de la forme

$$3x(x+1)-1 = ap^2$$

n'est possible que pour $a = 3\mu - 1$, l'équation (15 bis) conduira à celles-ci

$$(16) \quad \begin{cases} x(x+1) = 12r^2, & 2x+1 = 7q^2 \\ 3x(x+1)-1 = 35p^2, & y = 7pqr. \end{cases}$$

Or, les deux premières de ces équations donnent

$$(17) \qquad 49q^4 - 48r^2 = 1,$$

de sorte que le problème qui nous occupe ici se rattache à l'équation

$$A_{4n+1}(3) = 7q^2,$$

savoir l'équation (14) de l'article précédent.

Il est évident que l'équation (17) a la solution $q = r = 1$, ce qui donnera $x = 3$, $p = 7$, $y = 49$, et l'on aura donc

$$1^4 + 2^4 + 3^4 = 2 \cdot 7^2,$$

mais y a-t-il d'autres solutions de l'équation (15)?

XXIX. De la base $a = 6$.

Nous avons encore à étudier la base $6 = 2^2 + 2$; posons

$$A_n = \Phi_{2n}(2), \qquad B_n = \Psi_{2n}(2)$$

$$a_n = \frac{1}{2}\Phi_{2n+1}(2), \quad b_n = \Psi_{2n+1}(2),$$

les valeurs

$$x = A_n, \quad y = B_n$$
$$u = a_n, \quad v = b_n$$

représentent l'ensemble des positifs entiers qui satisfont aux équations

$$(1) \qquad x^2 - 6y^2 = 1$$

$$(2) \qquad 3v^2 = 2u^2 + 1.$$

De plus, il est évident que les A_n et les B_n sont les numérateurs respectivement les dénominateurs des réduites aux indices impairs, en commençant par l'indice 0, de la fraction continue

$$\sqrt{6} = \left[2, (2, 4)\right],$$

savoir

$$\frac{5}{2}, \frac{49}{20}, \frac{485}{198}, \frac{4801}{1960}, \ldots,$$

tandis que les a_n et les b_n sont la moitié des numérateurs, respectivemeut les dénominateurs des autres réduites, savoir

$$\frac{1}{1}, \frac{11}{9}, \frac{109}{89}, \frac{1079}{881}, \ldots,$$

Introduisons, dans l'article XIV, $\alpha = 2$, nous aurons une suite de relations concernant les nombres que nous venons d'introduire ici, formules parmi lesquelles nous nous bornerons à citer celles-ci

$$(3) \qquad A_{2n} = 12B_n^2 + 1, \quad A_{2n+1} = 4a_{n+1}^2 + 1$$

$$(4) \qquad B_{2n} = 2A_nB_n, \quad B_{2n+1} = 2a_{n+1}b_{n+1}$$

$$(5) \qquad 4B_{2n} = b_{n+1}^2 - b_n^2, \quad 2b_{2n+1} = B_{n+1}^2 - B_n^2$$

$$(6) \qquad 2B_n^2 + 1 = b_nb_{n+1}, \quad b_n^2 - 1 = 2B_nB_{n-1}$$

$$(7) \qquad b_{2n\pm1} = b_{n\pm1}^2 + 2B_n^2.$$

De plus, les quatre nombres A_n et B_n, a_n et b_n se déterminent par la même formule récursive, savoir

$$\alpha_n = 10\,\alpha_{n-1} - \alpha_{n-2}. \tag{8}$$

Remarquons encore que la base 6 est de la forme $2\cdot 3$, il résulte, en vertu du théorème I de l'article XXVI,

I. Le nombre $A_2 = 49$ représente la seule solution possible de l'équation

$$A_n = p^2; \tag{9}$$

c'est-à-dire que l'équation indéterminée

$$x^4 - 6\,y^2 = 1 \tag{10}$$

n'admet qu'une seule solution en positifs entiers, savoir

$$x = 7, \quad y = 20. \tag{11}$$

Remarquons, en passant, que l'équation (14) de l'article XX donnera la proposition curieuse:

II. L'équation indéterminée

$$x^4 - (x-1)\,y^2 = 1 \tag{12}$$

admet, abstraction faite du cas trivial $x = 1$, précisément la même solution en positifs entiers que l'équation (10).

De plus, le théorème II de l'article XXV donnera:

III. Une équation de la forme

$$A_{2n+1} = 2\,p^2 \pm 1 \tag{13}$$

est impossible.

Appliquons ensuite la dernière des formules (3), il résulte de même:

IV. Une équation de la forme

$$B_{2\nu}(2) = a_n \tag{14}$$

est impossible quels que soient les indices ν et n.

Quant aux nombres B_m, il est évident que B_{2n+1}, étant de la forme $4\varrho + 2$, ne peut jamais être un carré, de sorte qu'il résulte, en vertu du théorème II de l'article XXVI:

V. Le nombre B_n ne peut jamais être un carré, donc l'équation indéterminée

$$x^2 - 6y^4 = 1 \tag{15}$$

n'est pas résoluble en positifs entiers.

De plus, le théorème III de l'article XXVI donnera:

VI. Le nombre B_{2n} ne peut jamais être le double d'un carré, donc l'équation indéterminée

$$x^2 - 96y^4 = 1 \tag{16}$$

n'est pas résoluble en positifs entiers.

La valeur $A_2 = 49$ montre que les A_{4n+2} et les B_{4n} sont tous divisibles par 49, tandis qu'aucun autre des nombres A_m et B_m n'est divisible par 7.

Quant aux nombres A_{4n+2}, on aura:

VII. Le nombre $A_2 = 49$ représente la seule solution possible de l'équation

$$A_{4n+2} = 49p^2, \tag{17}$$

tandis qu'une équation de la forme

$$A_{4n+2} = 7p^2 \tag{17 bis}$$

est impossible.

Remarquons que le second membre de (17) est un carré, il ne nous reste, en vertu du théorème I, que l'équation (17 bis), ou, ce qui est la même chose,

$$49p^4 - 24y^2 = 1. \tag{18}$$

Or, $7p^2 + 1$ n'étant jamais divisible par 3, et $7p^2 - 1$ étant de la forme $4\sigma + 2$, on aura, en vertu de (18),

$$7p^2+1 = 4u^2, \quad 7p^2-1 = 6t^2, \quad y = tu,$$

savoir

$$1 = 2u^2 - 3t^2,$$

ce qui est impossible, parce que le second membre est de la forme $3\sigma+2$.

Il nous reste encore à démontrer que l'équation

$$B_{2n+1}(6) = 2p^2 \tag{19}$$

se rattache à celle-ci

$$B_{2\nu+2}(3) = k^2. \tag{20}$$

En effet, introduisons, dans l'équation (1), $y = 2p^2$, il résulte ces deux systèmes d'équations indéterminées simultanées

$$x \pm 1 = 12r^4, \quad x \mp 1 = 2s^4, \quad p = rs \tag{21}$$

$$x \pm 1 = 6r^4, \quad x \mp 1 = 4s^4, \quad p = rs. \tag{21 bis}$$

Or, le système (21) n'est pas admissible, parce qu'il donne

$$s^4 - 6r^4 = \pm 1$$

équation qui n'admet aucune solution en positifs entiers.

Quant aux équations (21 bis), elle donnent

$$3r^4 - 2s^4 = \pm 1,$$

et il faut donc supprimer la valeur -1 au second membre; c'est-à-dire qu'il existe, l'équation (19) supposée possible, un indice ν tel que

$$a_{\nu+1}(3) = s^2, \quad b_{\nu+1}(3) = r^2, \tag{22}$$

ce qui conduira précisément à une équation de la forme (20), où $k = rs = p$, de sorte que nous aurons

$$B_{2n+1}(6) = 2B_{2\nu+1}(3). \tag{23}$$

Cela posé, il est bien curieux que l'équation plus générale

$$B_n = pq^2, \tag{24}$$

où p est un nombre prémier impair, conduise aussi à l'équation (20).

Remarquons tout d'abord que, B_n étant un nombre pair, q est pair aussi, et il s'agit donc de l'équation indéterminée

$$(x+1)(x-1) = 96p^2q^4, \tag{25}$$

ce qui donnera ces quatre systèmes d'équations indéterminées simultanées

$$\begin{array}{llll} \text{(a)} & x \pm 1 = 2p^2r^4, & x \mp 1 = 48s^4, & q = rs \\ \text{(b)} & x \pm 1 = 6p^2r^4, & x \mp 1 = 16s^4, & q = rs \\ \text{(c)} & x \pm 1 = 2r^4, & x \mp 1 = 48p^2s^4, & q = rs \\ \text{(d)} & x \pm 1 = 6r^4, & x \mp 1 = 16p^2s^4, & q = rs. \end{array}$$

Or, le système (a) donnera, après la suppression de la valeur inadmissible -1,

$$1 = p^2r^4 - 24s^4,$$

ce qui est précisément une équation de la forme (1), et l'on aura donc

$$A_\nu = pr^2, \quad B_\nu = 2s^2, \tag{26}$$

où ν doit nécessairement être un nombre impair, ce qui est une conséquence directe du théorème VI; c'est-à-dire que la dernière des équations (26) est précisément de la forme (19).

Quant au système (b), il résulte

$$1 = 3(pr^2)^2 - 2(2s^2)^2,$$

ce qui est impossible, parce que les $a_\nu(3)$ sont tous impairs.

On voit que le système (c) donnera

$$r^4 - 6(2ps^2)^2 = 1,$$

savoir, en vertu du théorème VII, $r = 7$, $ps^2 = 10$, ce qui est impossible, tandis que l'on aura, en vertu du système (d), l'équation impossible

$$1 = 3r^4 - 2(2ps^2)^2.$$

Cela posé, il nous reste seulement le système (a), savoir les équations (26), où ν est impair; de plus, il résulte, en vertu de (24) et (26),

$$B_n = 4pr^2s^2 = B_{2\nu},$$

ce qui donnera la proposition curieuse:

VIII. Une équation de la forme (24) est impossible, à moins que n ne soit de la forme $4\nu + 2$ et qu'il n'existe un indice ϱ tel que

$$B_{2\nu+1}(6) = 2B_{2\varrho+1}(3), \tag{27}$$

où $B_{2\varrho+1}(3)$ est un carré.

On voit que la valeur

$$B_2(6) = 5 \cdot 2^2$$

provient de (26), pour $p = 5$, $r = s = 1$, ce qui donnera

$$B_1(6) = 2B_1(3) = 2.$$

XXX. Problème de Lucas.

Édouard Lucas, dans un livre publié en 1873[1], a énoncé, sans démonstration, le théorème intéressant:

I. L'équation indéterminée

$$1^2 + 2^2 + 3^2 + \ldots + x^2 = y^2, \tag{1}$$

ou, ce qui est la même chose,

$$x(x+1)(2x+1) = 6y^2 \tag{1 bis}$$

a seulement deux solutions en positifs entiers, savoir

[1] Recherches sur l'Analyse indéterminée et l'Arithmétique de Diophante; Moulins 1873. Citation de Lucas, dans les Nouvelles Annales (2) t. 18, p. 74—77; 1879.

(2) $$x = y = 1;\; x = 24,\; y = 70.$$

Après l'essai maladroit qu'a fait Moret Blanc[1] de démontrer le théorème susdit, Lucas[2] a cherché lui-même à établir une démonstration, en étudiant les neuf systèmes possibles de la forme

$$x = \alpha_1 t^2,\; x + 1 = \alpha_2 u^2,\; 2x + 1 = \alpha_3 v^2$$
$$\alpha_1 \alpha_2 \alpha_3 = 6,\; tuv = y,$$

provenus de l'équation (1 bis).

Or, sa résolution du système

$$x = 6t^2,\; x + 1 = u^2,\; 2x + 1 = v^2$$

est incomplète, comme nous l'avons déjà remarqué dans l'article XXIV, où nous avons aussi démontré que cette insuffisance est sans influence sur le résultat final. Mais c'est une chose très grave que Lucas se contente d'une remarque futile concernant le système

(3) $$x = t^2,\; x + 1 = 2u^2,\; 2x + 1 = 3v^2,$$

afin d'établir que ce système n'admet qu'une seule solution en positifs entiers, savoir

(3 bis) $$x = t = u = v = 1.$$

En effet, la résolution du système (3) représente toute la difficulté du problème proposée.

Gerono[3] a essayé de combler cette lacune du développement de Lucas, mais sa démonstration est fondée sur »le remarquable théorème« démontré par M. E. de Jonquières, et par conséquent elle est sans valeur.

[1] Nouvelles Annales (2) t. 15, p. 46—48; 1876.
[2] Ibid. (2) t. 16, p. 429—432; 1877.
[3] Ibid. (2) t. 17, p. 381—382; 1878.

Plus tard, le P. TH. PEPIN[1] S. J. a étudié l'équation indéterminée (1), »deren Lösung ebenfalls vervollständigt wird«[2], mais j'ignore et les résultats et la méthode de ce géomètre distingué.

Quant au problème de LUCAS, savoir les équations (1), il résulte, conformément aux remarques faites concernant l'équation (7) de l'article XXVIII, ces deux systèmes d'équations indéterminées simultanées

$$x(x+1) = 6y^2, \quad 2x+1 = u^2, \quad y = tu \tag{a}$$

$$x(x+1) = 2t^2, \quad 2x+1 = 3u^2, \quad y = tu. \tag{b}$$

Quant au système (a), on aura

$$u^4 - 24t^2 = 1,$$

savoir $u = 7$, $t = 10$, ce qui donnera $x = 24$, $y = 70$, savoir la seconde des solutions (2).

Étudions ensuite le système (b), il résulte

$$9u^4 - 8t^2 = 1, \tag{4}$$

ce qui donnera la proposition curieuse:

II. Le postulat de LUCAS exige que l'équation

$$A_{4n+2}(2) = 3p^2 \tag{5}$$

n'ait que la seule solution

$$A_2(2) = 3, \tag{5 bis}$$

ce qui est certainement le cas, pourvu que le postulat de M. E. DE JONQUIÈRES soit vrai.

[1] Atti della Accademia Pontificia dei Nuovi Lincei, t. 35, p. 281—302; 1879.

[2] Jahrbuch über die Fortschritte der Mathematik, t. (11), 1879, p. 135. Le Jahrbuch, t. 10 (1878), p. 145 indique faussement que LUCAS ait démontré le résultat (3 bis).

En effet, supposons que l'équation (4) n'ait que la seule solution $u = t = 1$, nous aurons $x = y = 1$, savoir la première des solutions (2).

Remarquons, en passant, que la démonstration exacte du postulat de Lucas n'entraîne pas le postulat de M. E. de Jonquières, comme le montre clairement la démonstration du théorème IV de l'article XIX.

Or, il est très curieux, ce me semble, que les résultats indiqués, supposés vrais, permettent de résoudre complètement cette autre équation indéterminée

$$1^4 + 2^4 + 3^4 + \dots + x^4 = y^2, \tag{6}$$

ou, ce qui est la même chose,

$$x(x+1)(2x+1)(3x^2+3x-1) = 30y^2. \tag{6 bis}$$

En effet, l'équation (6 bis) donne, en vertu des remarques faites relativement à l'équation (15 bis) de l'article XXVIII, ces trois systèmes d'équations indéterminées

(a) $x(x+1)(2x+1) = 6z^2, \ 3x^2+3x-1 = 5u^2, \ \ y = zuv$

(b) $x(x+1) = 6t^2, \ 2x+1 = 7u^2, \ 3x^2+3x-1 = 35v^2, \ y = 7zuv$

(c) $x(x+1) = 2t^2, \ 2x+1 = 21u^2, \ 3x^2+3x-1 = 35v^2, \ y = 7zuv.$

Quant aux équations (a), on aura $x = z = u = y = 1$, tandis que les valeurs $x = 24$, $y = 70$ sont inadmissibles, parce que $3x(x+1)$ est multiple de 5.

Étudions maintenant le système (b), les deux premières équations donnent

$$(2x+1)^2 - 24t^2 = 1, \ \ 2x+1 = 7u^2,$$

et il résulte du théorème VII de l'article précédent que ces équations ne sont pas résolubles en positifs entiers.

Enfin, les équations (c) donnent

$$(2x+1)^2 - 2(2t)^2 = 1, \ \ 2x+1 = 21u^2,$$

ce qui est impossible, parce que $A_{2\nu}(2)$ ne peut pas être multiple de 7.

Cela posé, nous venons de démontrer la proposition curieuse:

III. Supposons vrai le postulat de Lucas, l'équation indéterminée (6) n'admet que la solution triviale $x = y = 1$.

CHAPITRE VIII

Des bases de première espèce.

XXXI. La base a et les nombres $\omega_{\mu-1}$ et $p_{\mu-1}$.

Soit a une base quelconque de première espèce, l'équation

$$A_{2n+1}^2 + 1 = aB_{2n+1}^2 \tag{1}$$

montre clairement que a et B_{2n+1} sont tous deux une somme de deux carrés, savoir

$$a = p^2 + q^2 \tag{2}$$

$$B_{2n+1} = x^2 + y^2 \tag{3}$$

Or, le premier membre de (1) étant ou impair ou de la forme $4\sigma + 2$, il est évident que B_{2n+1} est toujours impair, tandis que a est ou impair ou de la forme $4\sigma + 2$; c'est-à-dire que, dans (2), au moins un des nombres p et q est impair.

Appliquons ensuite la formule générale (10) de l'article XV, il résulte, en vertu de (1), (2), (3),

$$A_{2n+1}^2 + 1 = \left[p(x^2 - y^2) \pm 2qxy\right]^2 + \left[q(x^2 - y^2) \mp 2pxy\right]^2, \tag{4}$$

donc il est possible de choisir, dans (2), les nombres p et q, de sorte qu'il soit possible de déterminer x et y tels qu'un des deux carrés qui figurent au second membre de (4) ait la valeur 1.

A cet égard, nous avons à revenir aux nombres ω_r et p_r, définis dans les articles III et VI par les formules

$$y_r^2 - a z_r^2 = (-1)^{r-1} \omega_r$$

$$y_r y_{r+1} - a z_r z_{r+1} = (-1)^{r+1} p_r,$$

il résulte, en combinant la dernière de ces formules et celle-ci

$$y_r z_{r+1} - z_r y_{r+1} = (-1)^{r+1},$$

puis cherchant y_r et z_r,

$$(5) \quad \left\{ \begin{aligned} \omega_{r+1} y_r &= a z_{r+1} - p_r y_{r+1} \\ \omega_{r+1} z_r &= y_{r+1} - p_r z_{r+1}, \end{aligned} \right.$$

tandis que nous aurons de même

$$(6) \quad \left\{ \begin{aligned} \omega_r y_{r+1} &= a z_r + p_r y_r \\ \omega_r z_{r+1} &= p_r z_r + y_r, \end{aligned} \right.$$

formules qui sont déjà indiquées dans l'article VI.

Appliquons ensuite la formule (12) de l'article susdit, savoir

$$\omega_r \omega_{r+1} = a - p_r^2,$$

il est facile de démontrer le théorème:

I. Soit a une base de première espèce ayant le nombre caractéristique $2\mu + 1$, on aura toujours

$$(7) \qquad a = \omega_{\mu-1}^2 + p_{\mu-1}^2.$$

En effet, la formule fondamentale

$$\omega_r = \omega_{2\mu-r-1}, \quad 0 \leqq r \leqq 2\mu - 1,$$

donnera

$$(8) \qquad \omega_\mu = \omega_{\mu-1},$$

et la formule (7) est évidente.

Cela posé, remarquons que les formules (11) de l'article III donnent,

(9) $$B_1 = z_\mu^2 + z_{\mu-1}^2,$$

je dis que nous aurons, conformément à la formule (4), pour $n = 0$,

(10) $$\omega_{\mu-1}\left(z_\mu^2 - z_{\mu-1}^2\right) - 2p_{\mu-1} z_{\mu-1} z_\mu = (-1)^\mu$$

(11) $$A_1 = p_{\mu-1}\left(z_\mu^2 - z_{\mu-1}^2\right) + 2\omega_{\mu-1} z_{\mu-1} z_\mu.$$

Démontrons tout d'abord la formule (10), qui entraîne nécessairement (11); nous aurons

$$\omega_{\mu-1} z_\mu^2 = z_\mu (p_{\mu-1} z_{\mu-1} + y_{\mu-1})$$
$$\omega_{\mu-1} z_{\mu-1}^2 = \omega_\mu z_{\mu-1}^2 = z_{\mu-1}(y_\mu - p_{\mu-1} z_\mu),$$

ce qui donnera immédiatement la formule (10), donc nous aurons la proposition:

II. Le nombre $\omega_{\mu-1}$ est toujours impair.

Quant à la formule (11), on aura

$$2\omega_{\mu-1} z_{\mu-1} z_\mu = 2\omega_\mu z_{\mu-1} z_\mu = 2z_\mu (y_\mu - p_{\mu-1} z_\mu),$$

ce qui donnera, en vertu de (9)

(12) $$A_1 = 2y_\mu z_\mu - p_{\mu-1} B_1,$$

de sorte que la formule (11) de l'article III

(13) $$A_1 = y_\mu z_\mu + y_{\mu-1} z_{\mu-1}$$

donnera

(14) $$p_{\mu-1} B_1 = y_\mu z_\mu - y_{\mu-1} z_{\mu-1}.$$

Cela posé, on aura immédiatement, en vertu de (13) et (14),

$$A_1^2 - p_{\mu-1}^2 B_1^2 = 4 y_\mu z_\mu y_{\mu-1} z_{\mu-1},$$

et l'équation

$$A_1^2 - \left(p_{\mu-1}^2 + \omega_{\mu-1}^2\right) B_1^2 = -1$$

donnera donc la relation curieuse

$$\omega_{\mu-1}^2 B_1^2 = 4 y_\mu z_\mu y_{\mu-1} z_{\mu-1} + 1, \tag{15}$$

de sorte que le nombre qui figure au second membre est toujours un carré.

Revenons maintenant à la formule (4), puis supposons que p soit impair, ce qui est permis, nous savons que l'équation

$$p(x^2 - y^2) \pm 2qxy = \pm 1 \tag{16}$$

est, pour $p = \omega_{\mu-1}$, résoluble en positifs entiers, ce qui est une conséquence immédiate de l'équation (10); mais y a-t-il d'autres représentations de la forme (2), pour lesquelles l'équation (16) soit résoluble en positifs entiers?

Je n'ai pas réussi à donner une réponse définitive à cette question, mais supposons résoluble en positifs entiers l'équation (16), nous aurons

$$x = \frac{1}{p}\left(\mp qy \pm \sqrt{ay^2 \pm p}\right)$$
$$y = \frac{1}{p}\left(\pm qx \pm \sqrt{ax^2 \mp p}\right);$$

c'est-à-dire que les équations indéterminées

$$u^2 - av^2 = p \tag{17}$$

$$u_1^2 - av_1^2 = -p \tag{18}$$

sont toutes deux résolubles en positifs entiers, et il est possible de déterminer de telles solutions que

$$B_1 = v^2 + v_1^2 \tag{19}$$

$$aB_1 = u^2 + u_1^2. \tag{20}$$

De plus, on aura, dans ce cas

$$pv_1 = \mp qv \pm u$$
$$pv = \pm qv_1 \pm u_1,$$

ce qui donnera, en vertu de (2), (19), (20),

$$qB_1 = \pm(uv \pm u_1 v_1). \tag{21}$$

Quant aux équations (17) et (18), il est facile de démontrer la proposition:

III. Supposons qu'une des équations (17) et (18) ait une seule solution en positifs entiers, les équations ont toutes deux une infinité de telles solutions.

En effet, multiplions une des équations susdites, par exemple la première, par celle-ci

$$A_n^2 - aB_n^2 = (-1)^n,$$

où n est un positif entier quelconque, il résulte

$$(uA_n \pm avB_n)^2 - a(vA_n \pm uB_n)^2 = (-1)^n p.$$

Soit particulièrement a un nombre premier de la forme $4\nu + 1$, il n'existe d'autres représentations que (7), donc il faut admettre, dans (17) et (18)

$$p = \omega_{\mu-1}, \tag{22}$$

et l'on aura par conséquent

$$\left\{\begin{aligned} u &= y_{2n\mu+\mu-1}, & v &= z_{2n\mu+\mu-1} \\ u_1 &= y_{2n\mu+\mu}, & v_1 &= z_{2n\mu+\mu}. \end{aligned}\right. \tag{23}$$

XXXII. Des nombres B_{2nr+r}.

Soit a une base de première espèce, et soit r un indice impair, B_r et B_{2nr+r} sont tous deux la somme de deux carrés, donc il existe une représentation de la forme

$$B_{2nr+r} = B_r(\alpha^2 + \beta^2), \tag{1}$$

et il est très facile de déterminer un système des valeurs de α et β.

En effet, on aura, en vertu de la formule logarithmique générale, savoir la formule (19) de l'article VII,

$$2\,a\,B_r\,B_{2nr+r} = A_{2nr+2r} + A_{2nr},$$

de sorte que la formule

$$A_{2m} = 2\,a\,B_m^2 + (-1)^m \tag{2}$$

donnera immédiatement

$$B_r\,B_{2nr+r} = B_{nr+r}^2 + B_{nr}^2,$$

et il résulte donc

$$B_{2nr+r} = B_r\left(\left(\frac{B_{nr+r}}{B_r}\right)^2 + \left(\frac{B_{nr}}{B_r}\right)^2\right). \tag{3}$$

Cela posé, remarquons que le nombre

$$b = a B_r^2 = A_r^2 + 1 \tag{4}$$

est toujours une base de première espèce, il est évident que la formule (1) se rattache à l'équation de Fermat

$$x^2 - \left(A_r^2 + 1\right) y^2 = \pm\,1,$$

dont les solutions deviennent

$$x = \varphi_m(A_r), \quad y = \psi_m(A_r), \tag{5}$$

et nous aurons donc, en vertu de (4),

$$\varphi_n(A_r) = A_{nr}, \quad \psi_n(A_r) = \frac{1}{B_r} B_{nr}, \tag{6}$$

de sorte que la formule (3) n'est autre chose que celle-ci

$$B_{2nr+r} = B_r\left(\psi_{n+1}^2(A_r) + \psi_n^2(A_r)\right). \tag{7}$$

Or, cette dernière formule montre clairement que l'hypothèse spéciale

$$a = \alpha^2 + 1, \quad a B_r^2 = \beta^2 + 1 \tag{8}$$

conduira à des résultats intéressants.

En effet, soit $r = 2\mu + 1$, on aura

$$\psi_r(\alpha) = \psi_\mu^2(\alpha) + \psi_{\mu+1}^2(\alpha), \tag{9}$$

de sorte que la formule (7) se présente sous la forme

$$\left\{\begin{aligned} \psi_{2nr+r}(\alpha) = \left(\psi_{\mu+1}(\alpha)\,\psi_{n+1}(\beta) \pm \psi_\mu(\alpha)\,\psi_n(\beta)\right)^2 + \\ + \left(\psi_\mu(\alpha)\,\psi_{n+1}(\beta) \mp \psi_n(\beta)\,\psi_{\mu+1}(\alpha)\right)^2. \end{aligned}\right. \tag{10}$$

Cela posé, je dis que nous aurons

$$\left\{\begin{aligned} \psi_{\mu+1}(\alpha)\,\psi_{n+1}(\beta) - (-1)^\mu\,\psi_\mu(\alpha)\,\psi_n(\beta) &= \psi_{nr+\mu+1}(\alpha) \\ \psi_\mu(\alpha)\,\psi_{n+1}(\beta) + (-1)^\mu\,\psi_{\mu+1}(\alpha)\,\psi_n(\beta) &= \psi_{nr+\mu}(\alpha), \end{aligned}\right. \tag{11}$$

de sorte que la formule (10) donnera à la fois l'identité obtenue de (9), en y remplaçant r par $2nr + r$, et cette autre formule

$$\left\{\begin{aligned} \psi_{2nr+r}(\alpha) = \left(\psi_{\mu+1}(\alpha)\,\psi_{n+1}(\beta) + (-1)^\mu\,\psi_\mu(\alpha)\,\psi_n(\beta)\right)^2 + \\ + \left(\psi_\mu(\alpha)\,\psi_{n+1}(\beta) - (-1)^\mu\,\psi_{\mu+1}(\alpha)\,\psi_n(\beta)\right)^2. \end{aligned}\right. \tag{12}$$

Quant à (11), il suffit évidemment de démontrer une seule de ces deux formules, par exemple la première. A cet effet, il s'agit, en vertu de (6), de démontrer l'identité

$$\left\{\begin{aligned} 2(\alpha^2+1)\,\psi_{\mu+1}(\alpha)\,\psi_{nr+r}(\alpha) - (-1)^\mu 2(\alpha^2+1)\,\psi_\mu(\alpha)\,\psi_{nr}(\alpha) = \\ = 2(\alpha^2+1)\,\psi_r(\alpha)\,\psi_{nr+\mu+1}(\alpha). \end{aligned}\right. \tag{13}$$

Or, la formule logarithmique générale, savoir la formule (19) de l'article VII, donnera

$$2(\alpha^2+1)\,\psi_{\mu+1}\,\psi_{nr+r}(\alpha) = \varphi_{nr+r+\mu+1}(\alpha) + (-1)^\mu\,\varphi_{nr+\mu}(\alpha)$$

$$(-1)^\mu\,2(\alpha^2+1)\,\psi_\mu(\alpha)\,\psi_{nr}(\alpha) = (-1)^\mu\,\varphi_{nr+\mu}(\alpha) - \varphi_{nr-\mu}(\alpha)$$

de sorte que le premier membre de la formule (13) aura la valeur

$$\varphi_{nr+r+\mu+1}(\alpha)+\varphi_{nr-\mu}(\alpha)=2(\alpha^2+1)\,\psi_r(\alpha)\,\psi_{nr+\mu+1}(\alpha),$$

ce qui donnera précisément (13) et par conséquent aussi la première des formules (11).

Soit par exemple

$$\alpha=1,\ \ r=3,\ \ B_3=5,$$

on aura

$$2B_3^2=50=7^2+1,\ \ \beta=7,$$

ce qui donnera

$$A_{3\nu}=\varphi_\nu(7),\quad B_{3\nu}=\frac{1}{5}\,\psi_\nu(7),$$

et l'on aura donc, en vertu de (7),

$$B_{6n+3}=5\left(\psi_{n+1}^2(7)+\psi_n^2(7)\right), \tag{14}$$

tandis qu'il résulte, en vertu de (12),

$$B_{6n+3}=\left(2\psi_{n+1}(7)-\psi_n(7)\right)^2+\left(\psi_{n+1}(7)+2\psi_n(7)\right)^2. \tag{15}$$

XXXIII. Des nombres A_{4nr+2r}.

Soit, comme dans les deux articles précédents, a une base de première espèce, on aura quel que soit m,

$$A_{4m+2}=2A_{2m+1}^2+1. \tag{1}$$

De plus, A_{2mp+p} étant toujours divisible par A_p, on aura, pourvu que r soit un indice impair,

$$A_{4nr+2r}=A_{2r}(x^2+2y^2), \tag{2}$$

d'où, en vertu de (1),

$$A_{4nr+2r}=(x\pm 2yA_r)^2+2(xA_r\mp y)^2. \tag{3}$$

Cela posé, il résulte de (1) qu'il est toujours possible de déterminer les nombres entiers x et y, de sorte que

$$(4) \qquad x + (-1)^{\varepsilon} 2 y A_r = \pm 1$$

$$(5) \qquad x A_r - (-1)^{\varepsilon} y = \pm A_{2nr+r}.$$

Quant à l'équation (4), on aura la solution générale

$$(6) \qquad \begin{cases} x = \pm 1 + 2 m A_r \\ y = (-1)^{\varepsilon - 1} m, \end{cases}$$

où m est un entier quelconque, ce qui donnera, en vertu de (5),

$$(7) \qquad \pm A_{2nr+r} = (\pm 1 + 2 m A_r) A_r + m.$$

Or, A_{2nr+r} étant divisible par A_r, m aura évidemment la même propriété; soit donc

$$m = \mu A_r,$$

il résulte, en vertu de (7)

$$(8) \qquad \pm A_{2nr+r} = \left(\pm 1 + 2 \mu A_r^2\right) A_r + \mu A_r.$$

Remarquons ensuite que la formule (3) donnera, en vertu de (4) et (5), cette autre expression

$$A_{4nr+2r} = (x - (-1)^{\varepsilon} 2 y A_r)^2 + 2 (x A_r + (-1)^{\varepsilon} y)^2,$$

il résulte, en vertu de (6),

$$(9) \quad A_{4nr+2r} = \left(\pm 1 + 4 \mu A_r^2\right)^2 + 2 A_r^2 \left(\pm 1 - \mu + 2 \mu A_r^2\right)^2,$$

ce qui donnera la formule curieuse

$$(10) \quad A_{4nr+2r} = 1 + 2 (\mu \pm 1)^2 A_r^2 + 8 \mu (\mu \pm 1) A_r^4 + 8 \mu^2 A_r^6.$$

Soit particulièrement

$$a = 2, \ \ r = 1, \ \ A_2 = 3, \ \ A_1 = 1,$$

on aura, en vertu de (8), une expression de la forme

$$(11) \qquad A_{2n+1} = 3 \varrho_n + (-1)^{\varepsilon n},$$

tandis que la formule (10) donnera

$$(12) \qquad A_{4n+2} = \left(4\varrho_n + (-1)^{\varepsilon_n}\right)^2 + 2\left(\varrho_n + (-1)^{\varepsilon_n}\right)^2.$$

Quant à l'exposant ε_n que nous venons d'introduire, la formule logarithmique (19) de l'article VII donnera ici

$$A_{2n+5} + A_{2n+1} = 6 A_{2n+3},$$

d'où, en vertu de (11),

$$3\varrho_{n+2} + 3\varrho_n + (-1)^{\varepsilon_{n+2}} + (-1)^{\varepsilon_n} = 6 A_{2n+3},$$

savoir

$$\varepsilon_{n+2} + \varepsilon_n = 1,$$

de sorte que nous aurons généralement

$$(12\text{ bis}) \qquad \varepsilon_{4\mu} = \varepsilon_{4\mu+1} = 0, \quad \varepsilon_{4\mu+2} = \varepsilon_{4\mu+3} = 1.$$

Quant à la formule (2), remarquons que B_{4nr} est divisible par B_{4r}, savoir par $2A_{2r}$, tandis que les B_{4nr+2r} ne possèdent pas cette propriété, puis appliquons l'égalité

$$2A_{2r}^2 = 4B_{2r}^2 + 2,$$

l'équation de Fermat

$$(13) \qquad x^2 - 2A_{2r}^2 y^2 = 1$$

a évidemment les solutions générales

$$x = \Phi_{2n}(2B_{2r}), \quad y = \Psi_{2n}(2B_{2r}),$$

et l'on aura donc

$$(14) \qquad A_{4nr} = \Phi_{2n}(2B_{2r}), \quad B_{4nr} = A_{2r}\Psi_{2n}(2B_{2r}).$$

De plus, l'équation (13) donnera

$$\Phi_{2n+1}^2(2B_{2r}) - 2A_{2r}^2\Psi_{2n+1}^2(2B_{2r}) = -2,$$

d'où, en posant

$$\Phi_{2n+1}(2B_{2r}) = 2t_{2n+1},$$

cette autre équation de FERMAT

$$\left(A_{2r}\,\Psi_{2n+1}(2\,B_{2r})\right)^2 - 2\,t_{2n+1}^2 = 1,$$

ce qui donnera

$$(15)\quad A_{4nr+2r} = A_{2r}\,\Psi_{2n+1}(2\,B_{2r}),\quad B_{4nr+2r} = \frac{1}{2}\,\Phi_{2n+1}(2\,B_{2r}),$$

donc la formule (2) se présente aussi sous cette autre forme

$$(16)\qquad A_{8nr\pm 2r} = A_{2r}\left(\Psi_{2n\pm 1}^2(2\,B_{2r}) + 2\,\Psi_{2n}^2(2\,B_{2r})\right).$$

Soit par exemple

$$a = 2,\quad r = 1,\quad A_2 = 3,\quad B_2 = 2,$$

on aura

$$(17)\qquad A_{8n\pm 2} = 3\left(\Psi_{2n\pm 1}^2(4) + 2\,\Psi_{2n}^2(4)\right).$$

TABLE DES MATIÈRES

CHAPITRE VI

Des puissances d'un nombre premier.

CHAPITRE VII

D'autres bases spéciales.

CHAPITRE VIII

Des bases de première espèce.

Forelagt paa Mødet d. 18. Nov. 1921.
Færdig fra Trykkeriet d. 9. Februar 1922.