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

RECHERCHES

SUR LES

ÉQUATIONS DE LAGRANGE

PAR

NIELS NIELSEN

KØBENHAVN
HOVEDKOMMISSIONÆR: ANDR. FRED. HØST & SØN, KGL. HOF-BOGHANDEL
BIANCO LUNOS BOGTRYKKERI
1923

AVANT-PROPOS

LAGRANGE, dans son cinquième supplément à l'Algèbre d'EULER, a developpé une méthode ingénieuse, dont le fondement est la détermination des valeurs rationnelles de x et y qui satisfont à l'équation indéterminée du second degré

$$y^2 = Ax^2 + B, \tag{1}$$

où A et B sont des nombres entiers donnés.

Or, l'illustre géomètre se borne au calcul numérique des valeurs de x et y, sans étudier, à un point de vue général, la nature de ces solutions, problème qui semble être resté inaperçu jusqu'ici.

En effet, HEINRICH WEBER, dans son Mémoire: Theorie der reellen Irrationalzahlen [1], ne cite, outre la Théorie des Nombres de LEGENDRE, que la Table de DEGEN [2] et une petite Note de CAYLEY [3] qui donne des formules et une table numérique concernant les équations spéciales

$$y^2 - ax^2 = \pm 4. \tag{2}$$

Remarquons, en passant, que la Table de Degen a été continuée par CAYLEY [4] et par M. E.-E. WHITFORD [5].

Quant à l'équation (1), on lit, dans le Jahrbuch [6], un compte rendu si curieux qu'il faut le citer textuellement:

[1] Archiv der Mathematik und Physik (3) t. 4, p. 205; 1902.
[2] Canon Pellianus; Copenhague 1817.
[3] Journal de Crelle, t. 53, p. 369—371; 1857.
[4] Report of the British Association for the advancement of Science; 1893.
[5] The Pell Equation; New-York 1912.
[6] Jahrbuch über die Fortschritte der Mathematik, t. 32, p. 197; 1901.

»Sind $T_x = \frac{1}{2}x(x+1)$ und $T_y = \frac{1}{2}y(y+1)$ zwei Triangularzahlen, so soll die Gleichung $T_x = nT_y$ durch ganzzahlige Werte von x und y befreidigt werden. Man setze $X = 2x+1$, $Y = 2y+1$, so kommt die Aufgabe auf die Lösung der diophantischen Gleichung $nY^2 - X^2 = n-1$ zurück. Ist ξ_r, η_r eine Lösung von $\xi^2 - n\eta^2 = 1$, so kann man X und Y in der Form darstellen:

$$X_r = \xi_r X_0 + n\eta_r Y_0\,, \quad Y_r = \xi_r Y_0 + \eta_r X_0\,,$$

wo X_0, Y_0 irgend ein der Gleichung genügendes Wertepaar, z. B. 1,1 ist.«

Les manques de précision et de clarté, que présente cette règle pour la formation des solutions de l'équation indéterminée

$$u^2 - av^2 = -(a-1) \tag{3}$$

sautent aux yeux. En premier lieu, la règle susdite est formulée avec si peu d'exactitude qu'elle donne une infinité de fois chacune des solutions qu'elle peut donner. Et, question plus grave, cette règle peut-elle donner toutes les solutions de l'équation susdite?

A cette question il faut répondre que la règle susdite ne peut donner toutes les solutions de l'équation (3) que dans le seul cas spécial $a = 3$.

En effet, une recherche plus approfondie de l'équation indéterminée du second degré

$$u^2 - av^2 = (-1)^\vartheta \omega\,, \tag{4}$$

où a et ω sont des positifs entiers premiers entre eux, et où a n'est pas un carré exact, montre que les solutions de cette équation forment toujours, pour $\omega > 2$, au moins deux suites différentes. C'est-à-dire que la règle susdite n'est complète que pour $a = 3$.

Or, en se rappelant les nombreux comptes rendus mor-

dants, parfois injustes, des publications qui ne donnent pas des résultats nouveaux, que feu M. LAMPE a donnés dans le Jahrbuch, on peut conclure que, en 1901, les fondements les plus primitifs d'une théorie générale de l'équation (4) étaient inconnus. Et l'on ne trouve rien d'une telle théorie dans la littérature postérieure á 1901.

Mes recherches sur les bases de seconde espèce, dont les facteurs premiers sont tous de la forme $4k+1$, savoir les nombres de la forme $\alpha^2+\beta^2$, où α et β sont premiers entre eux, pour lesquels l'équation

$$x^2-(\alpha^2+\beta^2)y^2=-1 \tag{5}$$

est irrésoluble, m'ont conduit à calculer les solutions des équations résolubles de la forme

$$u^2-34v^2=(-1)^\vartheta\omega\,, \tag{6}$$

parce que 34 est le plus petit des nombres susdits, et à étudier certaines équations de la forme (3) qui s'y rattachent. Or, les résultats ainsi obtenus sont si curieux et bizarres, d'un caractère si étrange que je me suis proposé de calculer une table des solutions des équations résolubles de la forme (4) qui correspondent aux valeurs

$$2\leqq a\leqq 101\,,\quad 2\leqq\omega\leqq 1000\,,$$

parce qu'une telle table donnera beaucoup d'éclaircissements curieux sur l'équation (4).

Je remarque expressément que le calcul de la Table susdite peut être effectué par des artifices spéciaux, sans appliquer la méthode assez compliquée indiquée par LAGRANGE, dans son cinquième supplément à l'Algèbre d'EULER. Néanmoins je propose de désigner comme équation de LAGRANGE une équation de la forme (4).

Dans le Mémoire présent je vais exposer les propriétés

de l'équation de LAGRANGE qui ont été indispensables pour mes calculs. C'est pourquoi je n'ai appliqué que des méthodes purement élémentaires, sans faire usage de la théorie des formes quadratiques, parce qu'il s'agit souvent des indices des solutions, comme éléments dans des suites, et, à ce point de vue, la méthode purement élémentaire est certainement la plus pratique.

Il est possible que la théorie des formes quadratiques donne immédiatement plusieurs des résultats que j'ai obtenus, et j'ai vu que cette théorie donnera facilement des propriétés théoriques de l'équation de LAGRANGE, propriétés qui sont difficiles à obtenir par la méthode purement élémentaire. Dans des publications prochaines j'exposerai des propriétés fondamentales de certaines équations de LAGRANGE des formes spéciales et une méthode pour la résolution numérique de telles équations.

En rédigeant mon Mémoire récent: Recherches sur l'équation de Fermat, je n'ai pas observé que les nombres ω_μ et r_μ sont bien connus, et que DEGEN a calculé les ω_μ qui correspondent à des valeurs de la base a au plus égales à 1000; c'est-à-dire que la plupart des résultats contenus dans le premier Chapitre de mon Mémoire susdit ne sont pas nouveaux.

Copenhague, le 16 octobre 1922.

NIELS NIELSEN.

CHAPITRE PREMIER

Des équations résolubles.

I. Définitions et propriétés fondamentales.

Dans ce qui suit, nous désignons comme équation de LAGRANGE une équation indéterminée de la forme

$$u^2 - av^2 = (-1)^\delta \omega, \tag{1}$$

où le positif entier a, base de l'équation, ne doit pas être un carré exact, tandis que ω, paramètre de l'équation, est un positif entier premier avec a. Quant à l'exposant δ, il est parfaitement déterminé, en vertu de (1), où a et ω sont donnés, pourvu qu'il ne puisse pas rester arbitraire.

De plus, nous disons que l'équation (1) est résoluble, pourvu qu'elle soit satisfaite par des positifs entiers u et v, premiers entre eux.

Ces définitions adoptées, on voit que l'équation de FERMAT est une équation de LAGRANGE au paramètre 1.

De plus, on voit que l'équation indéterminée

$$u^2 - 17v^2 = 4$$

est irrésoluble, bien qu'elle soit satisfaite par une infinité de valeurs paires de u et v, car le premier membre de cette équation est, pour u et v impairs, multiple de 8.

Quant à notre étude de l'équation (1), supposée résoluble, nous avons tout d'abord à indiquer la proposition évidente :

I. Supposons résoluble l'équation (1), $(-1)^{\delta}\omega$ est résidu quadratique d'un facteur quelconque de a; de plus, a est résidu quadratique d'un facteur quelconque de ω.

Soit ensuite, dans (1), $\omega < \sqrt{a}$, Lagrange a démontré que l'équation susdite est toujours irrésoluble, à moins que ω ne soit une des valeurs ω_r, provenues de la fraction continue de $\sqrt{a}$, de sorte que la solution complète de l'équation (1) est formée par les numérateurs et les dénominateurs de certaines réduites de la fraction continue susdite.

Or il est facile de démontrer le théorème général:

II. Soit a une base donnée quelconque, il existe une infinité de paramètres ω, pour lesquels l'équation (1) est résoluble.

En effet, soit r un résidu quadratique de a, il existe un positif entier α, tel que

$$\alpha^2 - aq = r, \tag{2}$$

et α est évidemment premier avec a, parce que r a cette propriété.

Choisissons ensuite deux positifs entiers u et v, premiers entre eux, tels que

$$u = \alpha + am, \quad u^2 = \alpha^2 + a(2\alpha m + am^2)$$
$$v^2 = p + q$$

où m et p sont des nombres entiers, puis posons

$$\omega = r + a(2\alpha m + am^2) - ap,$$

il résulte, en vertu de (2),

$$u^2 - av^2 = \omega, \tag{3}$$

et cette équation est certainement résoluble, parce que u et v, a et ω sont premiers entre eux.

Cela posé, il est évident que la proposition de Lagrange ne donne que la solution d'une partie très mince des équations résolubles qui correspondent à une base donnée a.

Quant au paramètre ω, il est facile de démontrer cette autre proposition, supplémentaire de la précédente :

III. Soit ω un paramètre donné quelconque, il existe une infinité de bases a, pour lesquelles l'équation (1) est résoluble.

En effet, choisissons un positif entier k, plus grand que ω, et premier avec ω, puis posons

$$a = k^2 - (-1)^\delta \omega ,$$

a est certainement un positif entier, premier avec a, qui n'est pas un carré exact; car on aura évidemment

$$(k-1)^2 < a < (k+1)^2.$$

De plus, il est évident que l'équation

$$u^2 - av^2 = (-1)^\delta \omega ,$$

ainsi obtenue, est résoluble, parce qu'elle est satisfaite par $u = k$, $v = 1$.

Ayant ainsi démontré l'existence des équations résolubles qui correspondent à une base donnée ou à un paramètre donné, nous avons à démontrer le théorème fondamental :

IV. Supposons résoluble l'équation (1), cette équation admet une infinité de solutions.

En effet, multiplions l'équation (1) par l'équation correspondante de FERMAT

$$A_n^2 - aB_n^2 = (-1)^{nk},$$

où n est un indice quelconque, il résulte

$$(4) \quad (uA_n \pm avB_n)^2 - a(uB_n \pm vA_n)^2 = (-1)^{nk+\delta}\omega ,$$

de sorte qu'il ne nous reste qu'à démontrer que les deux carrés qui figurent au premier membre de (4) sont premiers entre eux.

Posons par exemple

$$(5) \qquad u_1 = uA_n + avB_n , \quad v_1 = uB_n + vA_n ,$$

il résulte

$$(6)\quad u=(-1)^{nk}(u_1A_n-av_1B_n),\quad v=(-1)^{nk}(v_1A_n-u_1B_n),$$

de sorte que u_1 et v_1 sont premiers entre eux, pourvu que u et v le soient, et inversement.

Remarquons encore que la formule (4) donnera immédiatement cette autre proposition:

V. Soit a une base de première espèce, les deux équations indéterminées

$$(7)\qquad u^2-av^2=+\omega,\quad u^2-av^2=-\omega$$

sont en même temps résolubles ou non.

En effet, k étant un nombre impair, parce que a est une base de première espèce, il est évident que le second membre de (4) a pour n pair ou impair, des signes différents; c'est pourquoi nous écrivons, dans ce cas,

$$u^2-av^2=\pm\omega$$

au lieu des deux équations (7).

Or, cette condition suffisante pour la résolubilité simultanée des équations (7) n'est pas nécessaire, car on aura par exemple

$$7^2-34\cdot 1^2=15,\quad 11^2-34\cdot 2^2=-15,$$

bien que $34=6^2-2$ soit une base de seconde espèce. Dans une publication prochaine, nous avons à revenir aux équations de ce genre.

En terminant ce premier article, nous avons encore à démontrer une proposition qui nous sera souvent utile, dans ce qui suit, savoir:

VI. Supposons résoluble une des quatre équations indéterminées

$$(8)\quad \begin{cases} u^2-av^2=-(4k+2),\quad u^2-av^2=4k+2,\\ u^2-av^2=(-1)^{\delta}(8k+4),\quad u^2-av^2=(-1)^{\varepsilon}8k, \end{cases}$$

les trois autres sont toujours irrésolubles.

En effet, u et v étant tous deux impairs dans chacune des équations en question, u^2 et v^2 sont de la forme $8\sigma+1$, de sorte que la première des équations (8) n'est pas résoluble, à moins que $a=8\nu+3$, tandis que la deuxième des équations susdites exige $a=8\nu+7$; c'est-à-dire que les deux équations en question se présentent sous la forme commune

$$(9) \qquad u^2-av^2=(-1)^{\nu-1}(4k+2), \quad a=4\nu+3.$$

Quant aux deux dernières des équations (8), on aura respectivement $a=8\nu+5$, $a=8\nu+1$.

II. Des suites de solutions.

Revenons maintenant à l'équation générale de LAGRANGE

$$(1) \qquad u^2-av^2=(-1)^{\vartheta}\omega,$$

nous avons tout d'abord à démontrer le théorème:

I. Une solution quelconque de l'équation (1), supposée résoluble, est toujours élément d'une suite infinie de solutions

$$(2) \qquad (u_1, v_1),\ (u_2, v_2),\ \ldots,\ (u_n, v_n),\ \ldots$$

formées successivement à l'aide des formules récursives

$$(3) \qquad u_{n+1}=u_nA_1+av_nB_1, \quad v_{n+1}=u_nB_1+v_nA_1.$$

On voit que ce théorème est une conséquence immédiate de la formule (4) de l'article précédent.

Or, les équations (3) donnent, résolues par rapport à u_n et v_n,

$$(4) \quad (-1)^ku_n=u_{n+1}A_1-av_{n+1}B_1, \quad (-1)^kv_n=v_{n+1}A_1-u_{n+1}B_1,$$

où nous avons posé, comme ordinairement,

$$(5) \qquad A_1^2-aB_1^2=(-1)^k.$$

Cela posé, il est évident que les deux différences

$$u_nA_1-av_nB_1, \quad v_nA_1-u_nB_1$$

ont toujours le même signe, pourvu que $n > 1$; mais pour $n = 1$ cela ne peut pas avoir lieu.

En effet, supposons que les différences

(6) $u_1 A_1 - a v_1 B_1 = (-1)^{\mu} \alpha$, $v_1 A_1 - u_1 B_1 = (-1)^{\mu} \beta$

aient toutes deux le même signe, puis remarquons que (α, β) est une solution de l'équation (1), nous aurons, en vertu de (6),

$$(-1)^{k+\mu} u_1 = \alpha A_1 + a \beta B_1, \quad (-1)^{k+\mu} v_1 = \alpha B_1 + \beta A_1,$$

ce qui donnera nécessairement $\mu = k$, et (α, β) est donc une solution de la suite (2) qui précède le premier élément (u_1, v_1) de cette suite, ce qui est impossible.

Les deux différences

$$u_1 A_1 - a v_1 B_1, \quad u_1 B_1 - v_1 A_1$$

ont donc le même signe, et il existe par conséquent un exposant δ tel que les nombres s_1 et t_1 définis par les expressions

(7) $(-1)^{\delta} s_1 = u_1 A_1 - a v_1 B_1$, $(-1)^{\delta} t_1 = u_1 B_1 - v_1 A_1$

sont tous deux positifs, et je dis que cet exposant δ est précisément celui qui figure dans l'équation

(8) $$u_1^2 - a v_1^2 = (-1)^{\delta_1} \omega.$$

En effet, résolvons par rapport à A_1 et B_1 les deux équations (7), il résulte, en vertu de (8),

(9) $$\omega A_1 = s_1 u_1 + a t_1 v_1, \quad \omega B_1 = s_1 v_1 + t_1 u_1,$$

tandis que les formules (7) et (8) donnent

(10) $$s_1^2 - a t_1^2 = (-1)^{k+\delta_1} \omega,$$

de sorte que (s_1, t_1) est aussi une solution de l'équation (1).

Quant à cette solution (s_1, t_1), deux cas seulement sont possibles, savoir:

1° Les deux solutions (u_1, v_1) et (s_1, t_1) sont identiques. Dans ce cas, nous désignons comme fermée la suite (2).

2° Les deux solutions (u_1, v_1) et (s_1, t_1) sont différentes. Dans ce cas, (s_1, t_1) est le premier élément d'une autre suite

$$(11) \qquad (s_1, t_1),\ (s_2, t_2),\ \ldots,\ (s_n, t_n),\ \ldots$$

de solutions de l'équation (1), et nous aurons, en vertu de (7),

$$(12)\quad (-1)^{k+\delta_1} u_1 = s_1 A_1 - a t_1 B_1, \quad (-1)^{k+\delta_1} v_1 = s_1 B_1 - t_1 A_1.$$

Dans ce qui suit, nous désignons comme réciproques les deux solutions (s_1, t_1) et (u_1, v_1) et comme coordonnées les deux suites (2) et (11), dont les premiers éléments sont les solutions réciproques susdites.

Considérons maintenant une suite quelconque de solutions de l'équation indéterminée (1), ses premiers éléments sont généralement très irrégulièrement distribués parmi les solutions de l'équation correspondante de FERMAT; mais, à compter d'un certain indice, cette irrégularité disparaîtra, comme le montrent clairement les deux lemmes suivants:

II. Soit (u, v) une solution quelconque de l'équation (1) et soit $2A_{n-1} > \omega$, les deux inégalités

$$(13) \qquad A_n > u > A_{n-1}$$

entraînent nécessairement ces deux autres

$$(14) \qquad B_n > a > B_{n-1}.$$

On aura en effet

$$u^2 - A_{n-1}^2 = a(v^2 - B_{n-1}^2) + (-1)^{\delta}\omega - (-1)^{nk-k},$$

et l'inégalité évidente $u \geqq A_{n-1} + 1$ donnera

$$u^2 - A_{n-1}^2 \geqq 2A_{n-1} + 1 > \omega + 1,$$

de sorte que l'on aura nécessairement $v > B_{n-1}$, et l'on démontrera, par le même procédé, que l'inégalité $A_n > u$ entraîne $B_n > v$.

Supposons maintenant satisfaites les inégalités (13) et (14), supplées peut-être par une des égalités

$$u = A_{n-1}, \quad v = B_{n-1},$$

nous disons pour abréger que la solution (u, v) est située dans l'intervalle I_n, ou appartient à cet intervalle, ou que l'intervalle I_n contient la solution (u, v).

Cela posé, il est facile de démontrer le second des lemmes susdits:

III. Il existe, pour une suite quelconque des solutions de l'équation (1), un indice n, tel que l'intervalle I_n contient précisément un élément (u_m, v_m) de la suite, et l'élément (u_{m+p}, v_{m+p}) appartient à l'intervalle I_{n+p}, quel que soit l'indice p.

En effet, les inégalités simultanées

$$A_n > u_m \geqq A_{n-1}, \quad B_n > v_n \geqq B_{n-1},$$

où les signes d'égalité ne sont pas tous deux applicables, donnera, en vertu des formules récursives générales (3),

$$A_{n+p} > u_{m+p} > A_{n+p-1}, \quad B_{n+p} > v_{m+p} > B_{n+p-1};$$

c'est-à-dire que l'élément (u_{m+p}, v_{m+p}) est situé dans l'intervalle I_{m+p}.

Dans ce qui suit, nous désignons comme irrégulière une solution (u, v) de l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^\delta \omega,$$

pourvu qu'elle n'appartienne à aucun des intervalles I_n.

De plus, soient (u, v) et (u_1, v_1) deux solutions de l'équation susdite, nous écrivons

$$(u, v) > (u_1, v_1),$$

pourvu que ou $u > u_1$ ou $u = u_1$, mais $v > v_1$.

III. Des suites fermées et du paramètre 2.

Revenons maintenant aux formules (7) de l'article précédent, puis supposons identiques les deux solutions (s_1, t_1) et (u_1, v_1) de l'équation de LAGRANGE

(1) $$u^2 - av^2 = (-1)^\varepsilon \omega,$$

nous aurons, en remplaçant l'exposant δ_1 par δ,

(2) $$av_1 B_1 = u_1(A_1 - (-1)^\delta), \quad u_1 B_1 = v_1(A_1 + (-1)^\delta).$$

Multiplions ensuite les deux équations (2), il résulte

(3) $$A_1^2 - aB_1^2 = 1,$$

de sorte que la base a est nécessairement de seconde espèce.

Quant aux équations (2), remarquons que u_1 est premier et avec a et avec v_1, il est évident que B_1 est divisible par le produit $u_1 v_1$. Posons donc

(4) $$B_1 = k u_1 v_1,$$

où k est un positif entier, il résulte, en vertu de (2),

(5) $$akv_1^2 = A_1 - (-1)^\delta, \quad ku_1^2 = A_1 + (-1)^\delta,$$

ce qui donnera

(6) $$akv_1^2 = ku_1^2 - (-1)^\delta 2,$$

équation qui est impossible, à moins que

$$k = 1, \quad k = 2.$$

Or, la dernière de ces valeurs est inadmissible, parce que (u, v) n'est pas une solution de l'équation de FERMAT ayant la base a; c'est-à-dire que l'équation (6) se présente sous la forme

(7) $$u_1^2 - av_1^2 = (-1)^\delta 2.$$

De plus, on aura, en vertu de la proposition VI de l'article I,

(8) $$a = 4\nu + 3, \quad \delta = \nu - 1.$$

Introduisons maintenant, dans les formules (4) et (5), la seule valeur possible $k = 1$, il résulte

$$A_1 = u_1^2 - (-1)^\delta, \quad B_1 = u_1 v_1,$$

formules qui déterminent parfaitement les nombres u_1 et v_1, et nous aurons évidemment

$$A_1 > u_1, \quad B_1 \geqq v_1,$$

de sorte que la solution générale (u_n, v_n) de la suite fermée en question appartient, quel que soit l'indice n, à l'intervalle I_n.

Cela posé, prenons pour point de départ l'équation de LAGRANGE (7), savoir

$$u^2 - av^2 = (-1)^\delta 2, \tag{9}$$

supposée résoluble, puis désignons par (s, t) et (u, v) deux solutions quelconques de cette équation, savoir

$$s^2 - at^2 = (-1)^\delta 2, \quad u^2 - av^2 = (-1)^\delta 2, \tag{10}$$

je dis que les nombres x_1 et y_1, x_2 et y_2 définis par les expressions

$$2x_1 = su + atv, \quad 2y_1 = sv + tu \tag{11}$$

$$2x_2 = |su - atv|, \quad 2y_2 = |sv - tu| \tag{12}$$

satisfont à l'équation de FERMAT

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

En effet, multiplions les deux équations (10), il résulte

$$(su + atv)^2 - a(sv + tu)^2 = 4,$$

ce qui conduira immédiatement au résultat susdit, parce que les nombres s et t, u et v sont tous impairs.

Soit particulièrement $s = u$, $t = v$, on aura

$$x_1 = u^2 - (-1)^\delta, \quad y_1 = uv, \tag{14}$$

résultats qui conduiront à la proposition essentielle:

I. Soit (u_n, v_n) l'élément général d'une suite fermée appartenant à l'équation de LAGRANGE (9), on aura, quel que soit l'indice n,

$$A_{2n-1} = u_n^2 - (-1)^\delta, \quad B_{2n-1} = u_n v_n. \tag{15}$$

Remarquons que la solution (u_n, v_n) appartient à l'intervalle I_n, nous aurons

$$A_{n-1}^2 + aB_{n-1}^2 < u_n^2 + av_n^2 < A_n^2 + aB_n^2,$$

ou, ce qui est la même chose,

$$\frac{A_{2n-1}}{2} < u_n^2 - (-1)^\vartheta < \frac{A_{2n}}{2}. \tag{16}$$

Or, la formule récursive de LAGRANGE

$$A_{m+1} = A_1 A_m + a B_1 B_m$$

donne, en vertu de la condition évidente $A_1 \geqq 2$,

$$A_{m+1} > 2 A_m,$$

de sorte que les inégalités (16) se présentent sous cette autre forme

$$A_{2n-3} < u_n^2 - (-1)^\vartheta \leqq A_{2n-1},$$

et les formules (15) sont évidentes, car B_{2n-2} est pair.

Cela posé, il est évident qu'aucun des intervalles I_n ne peut contenir plus d'une seule solution de l'équation (9), ce qui donnera cette autre proposition:

II. Supposons résoluble l'équation de LAGRANGE (9), l'ensemble de ses solutions forme précisément une suite fermée.

Ce résultat est bien connu.

En effet, prenons pour point de départ la fraction continue

$$\sqrt{a} = [\alpha, (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{2\mu-1}, 2\alpha)], \tag{17}$$

puis désignons par

$$\frac{y_0}{z_0}, \frac{y_1}{z_1}, \frac{y_2}{z_2}, \ldots.$$

les réduites de cette fraction continue, nous aurons généralement

$$u_n = y_{2n\mu-\mu-1}, \quad v_n = z_{2n\mu-\mu-1}. \tag{18}$$

Posons ensuite

$$y_r^2 - a z_r^2 = (-1)^{r-1} \omega_r, \tag{19}$$

nous aurons donc ici

$$\omega_{\mu-1} = 2. \tag{20}$$

Soit, au contraire, pour la fraction continue (17),

$$\omega_{\mu-1} > 2, \tag{21}$$

la base a est divisible par $\omega_{\mu-1}$ ou par $\frac{\omega_{\mu-1}}{2}$, selon que $\omega_{\mu-1}$ est impair ou pair, de sorte que l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^\mu \omega_{\mu-1}$$

n'est pas résoluble.

Remarquons, en passant, que les formules (15) ont été étudiées par PAUL TANNERY [1] qui suppose qu'ARCHIMÈDE les ait appliquées pour calculer les solutions de l'équation

$$x^2 - 3y^2 = 1$$

à l'aide de celles de l'équation correspondante

$$u^2 - 3v^2 = -2.$$

IV. Des suites coordonnées.

Revenons maintenant à l'équation générale

$$u^2 - av^2 = (-1)^\vartheta \omega, \quad \omega > 2, \tag{1}$$

puis désignons par

$$\begin{cases} (s_1, t_1), (s_2, t_2), \ldots, (s_n, t_n), \ldots \\ (u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n), \ldots \end{cases} \tag{2}$$

deux suites coordonnées, formées des solutions de l'équation (1), nous avons tout d'abord à démontrer la proposition:

I. Les éléments généraux des deux suites coordonnées (2) sont liés par les formules

$$s_n u_p + a t_n v_p = \omega A_{n+p-1}, \quad s_n v_p + t_n u_p = \omega B_{n+p-1}. \tag{3}$$

En effet, appliquons les formules récursives générales

$$u_{n+p} = u_p A_n + a v_p B_n, \quad v_{n+p} = u_p B_n + v_p A_n \tag{4}$$

et les formules analogues contenant les s_n et t_n, les formules (3) sont les conséquences immédiates des formules (9) de l'article II.

[1] Mémoires scientifiques, publiés par J.-L. HEIBERG et H.-G. ZEUTHEN. Voir notamment t. I, pp. 80—105, 238—239, 252—253; t. II, p.160—161.

Posons maintenant

$$(5) \qquad s_n^2 - a t_n^2 = (-1)^{\delta_n}\omega\,, \quad u_p^2 - a v_p^2 = (-1)^{\varepsilon_p}\omega\,,$$

et résolvons par rapport à A_n et B_n les deux équations (4), puis remplaçons n par $n-p$, il résulte

$$(6) \quad \begin{cases} \omega A_{n-p} = (-1)^{\varepsilon_p}(u_n u_p - a v_n v_p)\,, \\ \omega B_{n-p} = (-1)^{\varepsilon_p}(v_n u_p - v_p u_n)\,, \end{cases}$$

où il faut supposer naturellement $n > p$.

Quant aux applications des deux formules (3) et (6), nous désignons comme multiplication positive l'opération indiquée par l'identité algébrique

$$(7) \qquad (p^2 - aq^2)(\alpha^2 - a\beta^2) = (p\alpha + aq\beta)^2 - a(p\beta + q\alpha)^2,$$

tandis que la multiplication négative se définit par l'identité analogue

$$(8) \qquad (p^2 - aq^2)(\alpha^2 - a\beta^2) = (p\alpha - aq\beta)^2 - a(p\beta - q\alpha)^2.$$

Ces définitions adoptées, il est facile de démontrer la proposition :

II. Les éléments de deux suites coordonnées conduiront, par la multiplication positive, à l'équation de FERMAT.

On aura, en effet, en multipliant les deux formules (5), puis appliquant (3),

$$(9) \qquad \left(\frac{s_n u_p + a t_n v_p}{\omega}\right)^2 - a\left(\frac{s_n v_p + t_n u_p}{\omega}\right)^2 = (-1)^{\delta_n + \varepsilon_p}.$$

La multiplication négative donnera de même, en vertu de (6),

$$(10) \qquad \left(\frac{u_n u_p - a v_n v_p}{\omega}\right)^2 - a\left(\frac{u_n v_p - u_p v_n}{\omega}\right)^2 = (-1)^{\varepsilon_n + \varepsilon_p},$$

d'où il résulte la proposition analogue à la précédente :

III. Les éléments de la même suite conduiront, par la multiplication négative, à l'équation de FERMAT.

Quant aux deux autres équations, analogues à (9) et (10),

$$(11)\quad \begin{cases} (s_n u_p - a t_n v_p)^2 - a (s_n u_p - t_n u_p)^2 = (-1)^{\delta_n+\varepsilon_p}\omega^2 \\ (u_n u_p + a v_n v_p)^2 - a (u_n v_p + v_n u_p) = (-1)^{\varepsilon_n+\varepsilon_p}\omega^2, \end{cases}$$

posons pour abréger

$$\omega_1 = \omega\,, \quad \omega_1 = \frac{\omega}{2}\,,$$

selon que ω est pair ou impair, nous démontrerons, dans l'article VIII, que les équations (11) représentent des solutions de l'équation

$$(12)\qquad u^2 - a v^2 = (-1)^{\varrho}\omega_1^2,$$

Cela posé, nous avons à démontrer les théorèmes inverses de II et III, savoir:

IV. Supposons que les deux solutions (s_μ, t_μ) et (u_ν, v_ν) de l'équation (1) conduisent, par la multiplication positive, à l'équation de FERMAT, ces deux solutions appartiennent à des suites coordonnées.

Soit

$$(13)\qquad s_\mu u_\nu + a t_\mu v_\nu = \omega A_n\,, \quad s_\mu v_\nu + t_\mu u_\nu = \omega B_n\,,$$

nous ne savons dès à présent rien sur la grandeur relative des trois indices μ, ν, n, mais les formules récursives

$$\begin{aligned} s_\mu &= s_1 A_{\mu-1} + a t_1 B_{\mu-1}\,, \quad t_\mu = s_1 B_{\mu-1} + t_1 A_{\mu-1} \\ u_\nu &= u_1 A_{\nu-1} + a v_1 B_{\nu-1}\,, \quad v_\nu = u_1 B_{\nu-1} + v_1 A_{\nu-1} \\ A_{p+r} &= A_p A_r + a B_p B_r\,, \qquad B_{p+r} = A_p B_r + B_p A_r \end{aligned}$$

donnent, en vertu de (13),

$$(14)\quad \begin{cases} (s_1 u_1 + a t_1 v_1) A_\sigma + (s_1 v_1 + t_1 u_1) B_\sigma = \omega A_n \\ (s_1 u_1 + a t_1 v_1) A_\sigma + (s_1 v_1 + t_1 u_1) A_\sigma = \omega B_n \end{cases}$$

où nous avons posé pour abréger

$$\sigma = \mu + \nu - 2.$$

Cela posé, nous aurons évidemment $\sigma > n$, de sorte que

les formules récursives des A_n et des B_n donnent, en vertu de (14),

(15) $\quad s_1 u_1 + a t_1 v_1 = \omega A_{n-\sigma}, \quad s_1 v_1 + t_1 u_1 = \omega B_{n-\sigma}.$

Soit maintenant, dans ces deux formules, $n-\sigma = 1$, les deux solutions (s_1, t_1) et (u_1, v_1) sont réciproques.

Soit, au contraire, $n-\sigma > 1$, et soit (α_p, β_p) l'élément général de la suite coordonnée à celle qui contient la solution (s_μ, t_μ), on aura, en vertu de (3),

$$s_1 \alpha_{n-\sigma} + a t_1 \beta_{n-\sigma} = \omega A_{n-\sigma},$$

$$s_1 \beta_{n-\sigma} + t_1 \alpha_{n-\sigma} = \omega B_{n-\sigma};$$

d'où il résulte, en vertu de (15),

$$u_1 = \alpha_{n-\sigma}, \quad v_1 = \beta_{n-\sigma};$$

ce qui est impossible, parce que (u_1, v_1) est le premier élément de la suite à laquelle cette solution appartient.

V. Supposons que les deux solutions (s_μ, t_μ) et (u_ν, v_ν) de l'équation (1) conduisent, par la multiplication négative, à l'équation de FERMAT, ces deux solutions appartiennent à la même suite.

Soient

(16) $\quad s_\mu u_\nu - a t_\mu v_\nu = (-1)^\sigma \omega A_n, \quad s_\mu v_\nu - t_\mu u_\nu = (-1)^\tau \omega B_n,$

nous ne connaissons dès à présent ni la grandeur relative des indices μ, ν, n ni la parité des exposants σ et τ, mais posons pour abréger

$$\sigma + \tau - 1 = \varrho,$$

il résulte, en vertu de (16),

$$B_n(s_\mu u_\nu - a t_\mu v_\nu) + (-1)^\varrho A_n(s_\mu v_\nu - t_\mu u_\nu) = 0,$$

ou, ce qui est la même chose,

(17) $\quad s_\mu(u_\nu B_n + (-1)^\varrho v_\nu A_n) = t_\mu(a v_\nu B_n + (-1)^\varrho u_n A_n).$

Or, s_μ et t_μ étant premiers entre eux, il résulte, en vertu de (17),

$$(18)\quad \begin{cases} a v_\nu B_n + (-1)^\varrho u_\nu A_n = M s_{\mu} \\ u_\nu B_n + (-1)^\varrho v_\nu A_n = M t_{\mu}, \end{cases}$$

où M est un nombre entier, positif ou négatif.

Cela posé, appliquons l'équation de FERMAT

$$A_n^2 - a B_n^2 = (-1)^{nk},$$

puis cherchons, des équations (18), les valeurs de u_ν et de v_ν, il résulte

$$(19)\quad \begin{cases} u_\nu = (-1)^{nk+\varrho}(s_{\mu} A_n - (-1)^\varrho a t_{\mu} B_n) M \\ v_\nu = (-1)^{nk+\varrho}(t_{\mu} A_n - (-1)^\varrho s_{\mu} B_n) M, \end{cases}$$

ce qui donnera

$$M = \pm 1,$$

car u_ν et v_ν sont premiers entre eux.

Soit maintenant ϱ un nombre pair, il faut, en vertu de (18), supposer $M = 1$, ce qui donnera

$$(20)\qquad s_{\mu} = u_{\nu+n}, \quad t_{\mu} = v_{\nu+n}.$$

Soit, au contraire, ϱ un nombre impair, on aura, en vertu de (19),

$$M = (-1)^{nk+1},$$

ce qui donnera

$$(21)\qquad u_\nu = s_{\mu+n}, \quad v_\nu = t_{\mu+n}.$$

V. Des bases de première espèce.

Il est bien intéressant, ce me semble, que la résolubilité simultanée de certaines équations de LAGRANGE, ayant la même base, donne des éclaircissements essentiels sur la nature de cette base.

A cet effet, nous avons tout d'abord à démontrer le théorème:

I. Supposons résolubles les deux équations de LAGRANGE

(1) $$u^2 - av^2 = p^\varrho, \quad u_1^2 - av_1^2 = -p^\varrho,$$

où p est un nombre premier quelconque, a est toujours une base de première espèce.

Soit p un nombre premier impair, les deux nombres

(2) $$uu_1 + avv_1, \quad uu_1 - avv_1$$

sont premiers entre eux, et il est évident que ces deux autres nombres

(3) $$uv_1 + u_1 v, \quad uv_1 - u_1 v$$

auront la même propriété.

De plus, il résulte, en vertu des équations (1),

(4) $u^2 u_1^2 \equiv a^2 v^2 v_1^2 \pmod{p^\varrho}$, $u^2 v_1^2 \equiv u_1^2 v^2 \pmod{p^\varrho}$;

c'est-à-dire qu'il existe un exposant δ, tel que

(5) $uu_1 + (-1)^\delta avv_1 = p^\varrho \alpha, \quad uv_1 + (-1)^\delta u_1 v = p^\varrho \beta,$

donc on aura, en multipliant les deux équations (1),

(6) $$\alpha^2 - a\beta^2 = -1.$$

Soit ensuite $p = 2$, nous avons à étudier séparément les trois cas suivants:

1° $\varrho = 1$; dans ce cas, les équations (1) ne sont jamais simultanément résolubles.

2° $\varrho = 2$, $a = 8\mu + 5$. Remarquons que les nombres u et v, u_1 et v_1 sont tous impairs, il existe un exposant δ, tel que les équations (5) sont valables, donc on aura ici

(7) $$\left(\frac{uu_1 + (-1)^\delta avv_1}{4}\right)^2 - a\left(\frac{uv_1 + (-1)^\delta u_1 v}{4}\right)^2 = -1,$$

(8) $$\left(\frac{uu_1 - (-1)^\delta avv_1}{2}\right)^2 - a\left(\frac{uv_1 - (-1)^\delta u_1 v}{2}\right)^2 = -4.$$

3° $\varrho \geqq 3$, $a = 8\mu + 1$. Dans ce cas, il existe un exposant δ, tel que

(9) $uu_1 - (-1)^\delta avv_1 = 4\mu + 2, \quad uv_1 - (-1)^\delta u_1 v = 4\nu + 2,$

(10) $uu_1 + (-1)^\delta avv_1 = 2^{\varrho-1} k, \quad uv_1 + (-1)^\delta u_1 v = 2^{\varrho-1} l,$

et je dis que les nombres k et l, ainsi définis, sont tous deux pairs. En effet, on aura, en multipliant les deux équations (1),

$$k^2 - al^2 = -4,$$

ce qui est impossible pour des valeurs impaires de k et l, parce que a est un nombre de la forme $8\mu+1$.

Le paramètre 4 joue un rôle très singulier dans la théorie des équations de Lagrange, ce qui est mis en pleine lumière par la proposition curieuse:

II. Supposons résoluble l'équation de Lagrange

$$u^2 - av^2 = -4, \tag{11}$$

la base a est nécessairement de première espèce.

En effet, il résulte, en vertu de (11),

$$\left(\frac{u^2+av^2}{2}\right)^2 - a(uv)^2 = 4, \tag{12}$$

et la proposition II est une conséquence immédiate de I.

Enfin nous avons à démontrer une troisième proposition de ce genre, savoir:

III. Supposons résolubles les deux équations de Lagrange

$$u^2 - av^2 = (-1)^\delta 4p^\varrho, \quad u_1^2 - av_1^2 = (-1)^{\delta+1} p^\varrho \tag{13}$$

où p est un nombre premier impair, a est toujour une base de première espèce.

Cette proposition est une conséquence immédiate de la précédente, parce que les congruences (5) conduiront à l'équation (11).

CHAPITRE II

Genre d'une équation de Lagrange.

VI. Des multiplications positives et négatives.

Dans la théorie des équations de LAGRANGE, les multiplications positives et négatives jouent un rôle fondamental; c'est pourquoi nous introduisons pour abréger les deux symboles

(1) $$(+)\ (u, v)\ (\alpha, \beta) = (U, V)$$

(2) $$(-)\ (u, v)\ (\alpha, \beta) = (U', V')$$

au lieu des équations

(1 bis) $$U = u\alpha + \alpha v\beta, \quad V = u\beta + v\alpha$$

respectivement

(2 bis) $$U' = u\alpha - \alpha v\beta, \quad V' = u\beta - v\alpha,$$

de sorte que, dans la multiplication négative, les facteurs symboliques (u, v) et (α, β) ne sont pas permutables, parce que l'on aura, dans le produit $(-)\ (\alpha, \beta)\ (u, v)$,

$$V' = v\alpha - u\beta.$$

Or, dans nos recherches suivantes, cette propriété singulière de la multiplication négative ne joue aucun rôle pour les applications, parce qu'il s'agit toujours du carré de V'. Quant aux deux formules symboliques (1) et (2), nous avons tout d'abord à développer une suite d'identités générales, valables quelles que soient les valeurs des nombres qui y figurent.

Soit, en premier lieu,

(3) $$(u_1, v_1),\ (u_2, v_2),\ \ldots,\ (u_n, v_n),\ \ldots$$

une suite infinie, dont les éléments se forment, à l'aide du premier, par les formules récursives

(4) $$u_n = u_1 A_{n-1} + a v_1 B_{n-1}\,, \quad v_n = u_1 B_{n-1} + v_1 A_{n-1}\,,$$

ou A_μ et B_μ désignent comme ordinairement les solutions générales de l'équation de FERMAT ayant la base a, savoir

(5) $$A_\mu^2 - a B_\mu^2 = (-1)^{k\mu},$$

et soit

(6) $$(\pm)\ (u_n, v_n)\ (\alpha, \beta) = (U_n, V_n)\,,$$

je dis que nous aurons, quelle que soit la nature de la multiplication en question,

(7) $$U_n = A_{n-1} U_1 \pm a B_{n-1} V_1\,, \quad V_n = A_{n-1} V_1 \pm B_{n-1} U_1.$$

En effet, posons

$$U_n = u_n\alpha + (-1)^\delta a v_n \beta\,, \quad V_n = u_n\beta + (-1)^\delta v_n \alpha\,,$$

les formules récursives (4) donnent

(8) $$U_n = A_{n-1}(u_1\alpha + (-1)^\delta a v_1\beta) + (-1)^\delta a B_{n-1}(u_1\beta + (-1)^\delta a v_1\alpha)$$

(9) $$V_n = A_{n-1}(u_1\beta + (-1)^\delta v_1\alpha) + (-1)^\delta B_{n-1}(u_1\alpha + (-1)^\delta v_1\beta)\,,$$

ce qui est précisément la formule symbolique (6).

Cela posé, désignons par S la suite (3), par T la suite nouvelle

(10) $$(\alpha_1, \beta_1),\ (\alpha_2, \beta_2),\ \ldots,\ (\alpha_n, \beta_n),\ \ldots$$

dont les éléments sont à former, à l'aide du premier, par les formules récursives, analogues à (4),

(11) $$\alpha_n = A_{n-1}\alpha_1 + a B_{n-1}\beta_1\,, \quad \beta_n = A_{n-1}\beta_1 + B_{n-1}\alpha_1\,,$$

il résulte, en vertu des formules (8) et (9), que les produits symboliques

(12) $$(+)\ (u_n, v_n)\ (\alpha_p, \beta_p)\,, \quad (-)\ (u_n, v_n)\ (\alpha_p, \beta_p)$$

sont des éléments de deux suites nouvelles M et N, ce que nous exprimons par les équations symboliques

(13) $$(+)\,ST = M, \quad (-)\,ST = N.$$

Soient ensuite (u'_n, v'_n) et (α'_n, β'_n) les éléments généraux des deux suites S' et T' coordonnées respectivement à S et à T, ce que nous exprimons par les symboles

(14) $$S' \infty S, \quad T' \infty T,$$

nous aurons, en vertu de la formule (9) de l'article II,

$$u' = (-1)^{\delta}(uA_1 - av B_1), \quad v' = (-1)^{\delta}(uB_1 - vA_1)$$

$$\alpha' = (-1)^{\varepsilon}(\alpha A_1 - a\beta B_1), \quad \beta' = (-1)^{\varepsilon}(\alpha B_1 - \beta A_1),$$

où (u', v') et (u, v), (α', β') et (α, β) sont les premiers éléments des suites S' et S, T' et T, et où nous avons posé

$$u^2 - av^2 = (-1)^{\delta}\omega, \quad \alpha^2 - a\beta^2 = (-1)^{\varepsilon}\omega_1.$$

Cela posé, un élément (U, V) de la suite $(+)\,S'\,T$ se présente sous la forme

$$U = \alpha u' + a\beta v', \quad V = \alpha v' + \beta u',$$

ce qui donnera

(15) $$(-1)^{\delta}U = A_1(\alpha u - a\beta v) + aB_1(u\beta - v\alpha)$$

(16) $$(-1)^{\delta}V = A_1(u\beta - v\alpha) + B_1(u\alpha - av\beta).$$

On aura de même, pour l'élément correspondant (U', V') de la suite $(+)\,ST'$,

$$U' = u\alpha' + av\beta', \quad V' = u\beta' + v\alpha',$$

ou, ce qui est la même chose,

(17) $$(-1)^{\varepsilon}U' = A_1(u\alpha - av\beta) - aB_1(u\beta - v\alpha)$$

(18) $$(-1)^{\varepsilon}V' = B_1(u\alpha - av\beta) - A_1(u\beta - v\alpha).$$

Ces résultats obtenus, il est facile de démontrer l'identité symbolique

(19) $$(-)\,ST' = (-)\,S'T.$$

En effet, posons pour abréger

$$M = u\alpha' - av\beta', \quad N = u\beta' - v\alpha'$$
$$M' = u'\alpha - av'\beta, \quad N' = u'\beta - v'\alpha,$$

il résulte, en vertu des formules fondamentales concernant les suites coordonnées S et S', T et T',

$$(-1)^{\delta}M = (-1)^{\varepsilon}M' = A_1(u\alpha + av\beta) - aB_1(u\beta + v\alpha)$$
$$(-1)^{\delta}N = (-1)^{\varepsilon}N' = B_1(u\alpha + av\beta) - A_1(u\beta + v\alpha),$$

ce qui n'est autre chose que l'identité (19).

Quant aux multiplications positives et négatives, nous avons encore à démontrer une proposition essentielle concernant les produits symboliques

$$(\pm)\,(u, v)\,(\alpha, \beta),$$

où (u, β) et (α, β) sont des solutions quelconques des équations de LAGRANGE

$$(20) \qquad u^2 - av^2 = (-1)^{\delta}\omega, \quad \alpha^2 - a\beta^2 = (-1)^{\varepsilon}\omega_1,$$

où les paramètres ω et ω_1 sont des positifs entiers quelconques, savoir:

I. Un facteur commun des deux nombres

$$(21) \qquad u\alpha + (-1)^{\delta}av\beta = K, \quad u\beta + (-1)^{\delta}v\alpha = L$$

est aussi diviseur commun des deux paramètres ω et ω_1.

En effet, cherchons, des équations (21), les valeurs de α et β, nous aurons, en vertu de (20),

$$(-1)^{\delta}\omega\alpha = uK - (-1)^{\delta}av L, \quad (-1)^{\delta}\omega\beta = uL - (-1)^{\delta}vK.$$

Soit maintenant f un diviseur commun de K et L, f est aussi diviseur commun de $\omega\alpha$ et de $\omega\beta$. Désignons ensuite par f_1 le plus grand commun diviseur de f et de ω, puis posons

$$f = f_1 f_2,$$

f_2 est premier avec ω, donc f_2 est diviseur commun de α et de β, ce qui est impossible, à moins que $f_2 = 1$, d'où on aura $f_1 = f$. Et l'on démontrera, par le même procédé, que f est aussi diviseur de ω_1.

VII. Des paramètres premiers entre eux.

Comme première application des identités générales que nous venons de développer, dans l'article précédent, nous avons à étudier la multiplication des deux équations de LAGRANGE

$$(1) \qquad u^2 - av^2 = (-1)^{\vartheta}\omega\,, \quad u^2 - av^2 = (-1)^{\varepsilon}\omega_1\,,$$

dont les paramètres ω et ω_1 sont premiers entre eux.

A cet effet, remarquons tout d'abord que la proposition I de l'article précédent donnera immédiatement le théorème fondamental:

I. Une multiplication quelconque des deux équations (1) donnera toujours une solution de cette autre équation

$$(2) \qquad u^2 - uv^2 = (-1)^{\vartheta+\varepsilon}\omega\,\omega_1.$$

Supposons maintenant à la fois

$$(3) \qquad \omega > 2\,, \quad \omega_1 > 2\,,$$

puis désignons par (u_n, v_n) et (u_n', v_n') des éléments quelconques de deux suites coordonnées S et S' de la première des équations (1), par (α_n, β_n) et (α_n', β_n') des éléments quelconques de deux suites coordonées T et T' de la seconde des équations susdites, les développements de l'article précédent donnent immédiatement les deux théorèmes généraux:

II. La multiplication des deux équations (1) donnera, quelles que soient les suites coordonnées S et S', T et T':

$$(4) \qquad (+)\,ST' \sim (+)\,S'T$$

$$(5) \qquad (-)\,ST' = (-)\,S'T \sim (+)\,ST.$$

Ces résultats obtenus, il est possible de discuter complètement la multiplication des suites S et S' par les suites T et T', savoir les huit suites

$$(+)\,ST,\ (+)\,ST',\ (+)\,S'T,\ (+)\,S'T'$$
$$(-)\,ST,\ (-)\,ST',\ (-)\,S'T,\ (-)\,S'T'.$$

A cet effet, remarquons tout d'abord que la proposition II donnera immédiatement

$$(6)\qquad (-)\,ST' = (-)\,S'T,\quad (-)\,S'T' = (-)\,ST$$

$$(7)\qquad (+)\,ST \infty (+)\,S'T',\quad (+)\,ST' \infty (+)\,S'T,$$

nous avons à étudier séparément les deux hypothèses suivantes:

1° Les deux nombres

$$(8)\qquad u\alpha - av\beta\,.\quad u\beta - v\alpha$$

ont le même signe.

Dans ce cas nous aurons

$$(+)\,ST' = (-)\,ST = (-)\,S'T' \infty (+)\,ST$$
$$(-)\,ST' = (-)\,S'T = (+)\,S'T' \infty (+)\,ST'.$$

Posons donc

$$(9)\qquad \sigma = (+)\,ST,\quad \tau = (+)\,ST',$$

il résulte, pour les suites coordonnées, les trois expressions

$$(10)\qquad \sigma' = (+)\,ST' = (-)\,ST = (-)\,S'T'$$

$$(11)\qquad \tau' = (+)\,S'T' = (-)\,ST' = (-)\,S'T.$$

2° Les deux nombres (8) ont des signes différents.

Dans ce cas, nous aurons

$$(12)\qquad (+)\,S'T = (-)\,ST = (-)\,S'T',$$

et ces trois suites identiques sont coordonnées ou à $(+)\,S'T'$ ou à $(+)\,ST$.

Supposons tout d'abord

$$(+)\,S'T \infty (+)\,S'T',$$

nous aurons

$$(-)\,ST' = (-)\,S'T = (+)\,ST \infty (+)\,S'T',$$

de sorte qu'il résulte, pour les suites coordonnées de l'équation (2),

$$\sigma = (+)\, S'T', \quad \tau = (+)\, S'T \tag{13}$$

$$\sigma' = (+)\, ST = (-)\, ST' = (-)\, S'T \tag{14}$$

$$\tau' = (+)\, S'T = (-)\, ST = (-)\, S'T'. \tag{15}$$

Soit, au contraire, les trois suites (12) coordonnées à $(+)\, ST$, on aura

$$(+)\, S'T' = (-)\, S'T = (-)\, ST' \infty (+)\, ST,$$

ce qui donnera, pour les suites coordonnées de l'équation (2),

$$\sigma = (+)\, ST, \quad \tau = (+)\, S'T \tag{16}$$

$$\sigma' = (+)\, S'T' = (-)\, S'T = (-)\, ST' \tag{17}$$

$$\tau' = (+)\, S'T = (-)\, ST = (-)\, S'T'. \tag{18}$$

Cela posé, nous avons démontré le second des théorèmes généraux susdits:

III. La multiplication de deux couples de suites coordonnées S et S', T et T' de chacune des équations (1) conduira toujours à deux couples de suites coordonnées σ et σ', τ et τ' de l'équation (2).

On voit que la multiplication que nous venons d'étudier a la propriété curieuse que deux des suites ainsi obtenues ne se présentent qu'une seule fois, tandis que les deux suites coordonnées se présentent trois fois. Or, on voit que les quatre multiplications positives donnent précisément les deux couples de suites coordonnées de l'equation (2).

Quant à la multiplication des deux équations (1), nous avons encore à démontrer la proposition:

IV. Aucune des quatre égalités

$$(\pm)\, ST = (\pm)\, SU \tag{19}$$

n'est possible, à moins que les deux suites T et U ne soient ou identiques ou coordonnées.

On peut, en vertu de l'égalité (5)

$$(-)\, ST = (+)\, ST',$$

se borner à étudier une seule des quatre équations (19), par exemple

(20) $$(+)\,ST = (+)\,SU.$$

Soient maintenant (α, β) un élément quelconque de S, (u, v) et (u_1, v_1) des éléments quelconques de T et U, on aura, en vertu de (20),

$$(u-u_1)\,\alpha + a\,(v-v_1)\,\beta = 0$$
$$(u-u_1)\,\beta + (v-v_1)\,\alpha = 0\,,$$

ce qui donnera nécessairement $u = u_1$, $v = v_1$, parce que les hypothèses $\alpha = \beta = 0$ sont inadmissibles.

Pour mettre en pleine lumière le caractère singulier de la multiplication de deux équations de LAGRANGE, il nous semble utile de considérer des exemples convenables.

Exemple I. $a = 7$, $\omega = 3$, $\omega_1 = 19$.

Les premiers éléments des deux suites coordonnées S et S' de l'équation

$$u^2 - 7v^2 = -3$$

sont (2, 1) et (5, 2), savoir

$$2^2 - 7\cdot 1^2 = -3\,, \quad 5^2 - 7\cdot 2^2 = -3\,,$$

tandis que les premiers éléments des suites coordonnées T et T' de l'équation

$$u^2 - 7v^2 = -19$$

sont (3, 2) et (18, 7), savoir

$$3^2 - 7\cdot 2^2 = -19\,, \quad 18^2 - 7\cdot 7^2 = -19.$$

Les deux couples de suites coordonnées σ et σ', τ et τ' de l'équation

$$u^2 - 7v^2 = 57$$

sont (20, 7) et (13, 4) respectivement (43, 16) et (8, 1), savoir, pour σ et σ',

$$20^2 - 7\cdot 7^2 = 57\,, \quad 13^2 - 7\cdot 4^2 = 57$$

et pour τ et τ'

$$43^2 - 7\cdot 16^2 = 57\,, \quad 8^2 - 7\cdot 1^2 = 57.$$

Dans ce cas, nous aurons

$$\sigma = (+)\,ST\,, \quad \tau = (+)\,S'T$$
$$\sigma' = (+)\,S'T' = (-)\,S'T = (-)\,ST'$$
$$\tau' = (+)\,ST' = (-)\,ST = (-)\,S'T'.$$

Exemple II. $a = 5\,, \quad \omega = 4\,, \quad \omega_1 = 11.$

On aura ici, pour S et S', les premiers éléments (1, 1) et (3, 1), savoir

$$1^2 - 5\cdot 1^2 = -4\,, \quad 3^2 - 5\cdot 1^2 = 4\,,$$

tandis que les suites T et T' ont les premiers éléments (3, 2) et (4, 1), savoir

$$3^2 - 5\cdot 2^2 = -11\,, \quad 4^2 - 5\cdot 1^2 = 11.$$

Quant aux deux couples de suites coordonnées σ et σ', τ et τ' de l'équation indéterminée

$$u^2 - 5v^2 = \pm 44\,,$$

on aura, pour les premiers éléments de σ et σ', (13, 5) et (1, 3), savoir

$$13^2 - 5\cdot 5^2 = 44\,, \quad 1^2 - 5\cdot 3^2 = -44\,,$$

tandis que les suites τ et τ' ont les premiers éléments (9, 5) et (7, 1), savoir

$$9^2 - 5\cdot 5^2 = -44\,, \quad 7^2 - 5\cdot 1^2 = 44.$$

Dans ce cas, on aura

$$\sigma = (+)\,ST\,, \quad \tau = (+)\,ST'$$
$$\sigma' = (+)\,S'T' = (-)\,S'T = (-)\,ST'$$
$$\tau' = (+)\,S'T = (-)\,ST = (-)\,S'T'.$$

Quant au cas particulier $\omega = 2$, posons par exemple

$$S' = S\,,$$

les formules (4) et (5) donnent les résultats

$$(+)\,ST' \sim (+)\,ST$$
$$(-)\,ST' \sim (+)\,ST\,,$$

de sorte que nous aurons

$$\sigma = (+)\,ST, \quad \sigma' = (-)\,ST = (-)\,ST' = (+)\,ST'.$$

Multiplions par exemple les deux équations

$$u^2 - 7v^2 = 2\,, \quad u^2 - 7v^2 = -3\,,$$

la suite S a le premier élément (3, 1), savoir

$$3^2 - 7\cdot 1^2 = 2\,,$$

tandis que les suites coordonnées T et T' ont les premiers éléments (2, 1) et (5, 2). Quant à l'équation

$$u^2 - 7v^2 = -6\,,$$

les premiers éléments de ses deux suites coordonnées σ et σ' sont (13, 5) et (1, 1), savoir

$$13^2 - 7\cdot 5^2 = -6\,, \quad 1^2 - 7\cdot 1^2 = -6.$$

Et nous aurons ici

$$\sigma = (+)\,ST, \quad \sigma' = (-)\,ST = (-)\,ST' = (+)\,ST'.$$

VIII. Du genre d'une équation de Lagrange.

Les résultats, obtenus dans l'article précédent, permettent de démontrer quelques théorèmes fondamentaux concernant le genre d'une équation de LAGRANGE, savoir le nombre total de suites formées de ses solutions.

Cette définition du genre adoptée, les résultats obtenus dans l'article III donnent immédiatement la proposition:

I. Les équations au paramètre 2 sont du genre 1, et inversement.

Soit ensuite $\omega > 2$ la puissance d'un nombre premier ou le double d'une telle puissance, il existe, en vertu des développements de l'article V, un exposant σ, tel que

$$\left(\frac{uu_1 + (-1)^\sigma uvv_1}{\omega}\right)^2 - a\left(\frac{uv_1 + (-1)^\sigma u_1 v}{\omega}\right)^2 = (-1)^{\delta+\varepsilon},$$

où (u, v) et (u_1, v_1) appartiennent à chacune des deux suites

coordonnées appartenant à l'équation de LAGRANGE en question.

Appliquons ensuite les propositions IV et V de l'article IV, nous aurons cette autre proposition :

II. Une équation de LAGRANGE, dont le paramètre $\omega > 2$ est la puissance d'un nombre premier ou le double d'une telle puissance, est toujours du genre 2.

Quant à ce dernier théorème, remarquons expressément que le théorème inverse n'est pas vrai, car l'équation

$$u^2 - 37v^2 = \pm 12$$

est du genre 2.

Posons maintenant

$$\omega = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \tag{1}$$

où $p_1, p_2, \dots, p_r$ sont des nombres premiers inégaux, puis supposons résolubles les r équations

$$u^2 - av^2 = (-1)^{\delta_s} p_s^{\alpha_s}, \quad s = 1, 2, 3, \dots, r, \tag{A_r}$$

nous disons que l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^{\delta} \omega, \quad \delta = \delta_1 + \delta_2 + \dots + \delta_r \tag{2}$$

est parfaitement décomposable. Et, cette définition adoptée, il est facile de démontrer la proposition :

III. Le genre d'une équation parfaitement décomposable, dont le paramètre contient r facteurs premiers, est au moins égal à 2^{r-1} ou à 2^r, selon que ω est de la forme $4k+2$ ou non.

En effet, supposons tout d'abord que ω ne soit pas de la forme $4k+2$, puis multiplions les deux équations (A_1) et (A_2), nous aurons une équation dont le genre est au moins égal à 4, et ainsi de suite.

Soit maintenant

$$\omega = 4k + 2 = 2\omega_1,$$

l'équation de LAGRANGE au paramètre ω_1 est au moins du genre 2^{r-1}, donc l'équation proposée aura la même propriété.

Démontrons maintenant la proposition inverse de la précédente, savoir:

IV. Le genre d'une équation de LAGRANGE, dont le paramètre ω contient r facteurs premiers, est au plus égal à 2^{r-1} respectivement à 2^r, selon que ω est de la forme $4k+2$ ou non.

En effet, désignons par (s, t) et (u, v) deux solutions quelconques de l'équation en question, savoir

$$s^2 - at^2 = (-1)^\delta \omega, \quad u^2 - av^2 = (-1)^\varepsilon \omega, \tag{3}$$

nous aurons, en éliminant a,

$$(sv + tu)(sv - tu) \equiv 0 \pmod{\omega}, \tag{4}$$

et il est facile de démontrer que le nombre 2 est le seul facteur commun des deux nombres

$$M = sv + tu, \quad N = sv - tu \tag{5}$$

qui divise aussi ω.

En premier lieu, il est évident qu'un facteur commun de M et N est aussi facteur commun des deux nombres

$$M + N = 2sv, \quad M - N = 2tu;$$

de plus, ω est premier avec chacun des nombres s, t, u, v.

Soit ensuite ω un nombre impair, il existe donc une décomposition de la forme

$$\omega = \omega_1 \omega_2, \tag{6}$$

où ω_1 et ω_2 sont premiers entre eux, de sorte que

$$sv + tu \equiv 0 \pmod{\omega_1}, \quad sv - tu \equiv 0 \pmod{\omega_2}, \tag{7}$$

et la décomposition (6) admet précisément

$$\binom{r}{0} + \binom{r}{1} + \ldots + \binom{r}{s} + \ldots + \binom{r}{r} = 2^r$$

solutions différentes.

Combinons maintenant la solution fixe (s, t) avec toutes les solutions possibles de l'équation de LAGRANGE en question, il est évident que le nombre total de ces solutions ne peut jamais dépasser 2^r.

Soit, au contraire, ω un nombre pair, nous posons

$$\omega = 2\omega_1\omega_2, \tag{8}$$

où ω_1 et ω_2 sont premiers entre eux, et il est évident que le nombre total des décompositions (7) est 2^{r-1} respectivement 2^r, selon que ω est de la forme $4k+2$ ou non.

Cette démonstration de la proposition IV est due à M. G. RASCH.

Or, les propositions III et IV étant établies, nous aurons immédiatement cette autre:

V. Le genre d'une équation parfaitement décomposable, dont le paramètre ω contient r facteurs premiers, est precisément égal à 2^{r-1} ou à 2^r, selon que ω est de la forme $4k+2$ ou non.

La détermination exacte du genre d'une équation quelconque est évidemment un problème très difficile, c'est pourquoi nous nous bornerons ici aux résultats généraux que nous venons d'établir.

IX. Des paramètres avec facteurs communs.

Considérons maintenant les deux équations de LAGRANGE

$$u^2 - av^2 = (-1)^{\varrho}\omega, \quad u_1^2 - av_1^2 = (-1)^{\sigma}\omega_1, \tag{1}$$

dont les paramètres ω et ω_1, ne sont pas premiers entre eux.

Soit δ un exposant quelconque, il existe, en vertu du théorème I de l'article VI, un nombre f, diviseur commun de ω et de ω_1, tel que l'équation

$$\left(\frac{uu_1 + (-1)^{\delta} a v v_1}{f}\right)^2 - a\left(\frac{uv_1 + (-1)^{\delta} u_1 v}{f}\right)^2 = \frac{(-1)^{\varrho+\sigma}\omega\omega_1}{f^2} \tag{2}$$

est résoluble.

Or, le problème général concernant la multiplication des deux équations (1) me semble assez compliqué, et je n'ai pas réussi à obtenir des résultats d'une portée plus étendue. C'est pourquoi nous nous bornerons à étudier ici le cas spécial $\omega = \omega_1$, de sorte qu'il s'agit d'une seule équation de LAGRANGE.

A cet effet, supposons que l'équation en question

$$u^2 - av^2 = (-1)^\varrho \omega \tag{3}$$

soit au moins du rang 4, puis désignons par (u, v) et (u_1, v_1) deux solutions de cette équation qui n'appartiennent ni à la même suite ni à deux suites coordonnées, il résulte, en vertu de (3) et de l'équation correspondante

$$u_1^2 - av_1^2 = (-1)^\sigma \omega , \tag{4}$$

les deux congruences

$$\begin{cases} (uu_1)^2 - (avv_1)^2 \equiv 0 \pmod{\omega} \\ (uv_1)^2 - (u_1 v)^2 \equiv 0 \pmod{\omega} , \end{cases} \tag{5}$$

ce qui nous conduira à étudier séparément les cas suivants:

1° Soit ω un nombre impair, il est possible de décomposer ω en deux facteurs ω_1 et ω_2, premiers entre eux, savoir

$$\omega = \omega_1 \omega_2 , \tag{6}$$

de sorte que nous aurons, en vertu de (5),

$$uu_1 + avv_1 \equiv 0 \pmod{\omega_1}$$
$$uu_1 - avv_1 \equiv 0 \pmod{\omega_2} ,$$

ce qui donnera, en vertu des congruences (5),

$$uv_1 + u_1 v \equiv 0 \pmod{\omega_1}$$
$$uv_1 - u_1 v \equiv 0 \pmod{\omega_2} ,$$

donc nous aurons les deux équations résolubles

$$\left(\frac{uu_1 + avv_1}{\omega_1}\right)^2 - a\left(\frac{uv_1 + u_1 v}{\omega_1}\right)^2 = (-1)^{\varrho+\sigma}\omega_2^2 \tag{7}$$

$$\left(\frac{uu_1 - avv_1}{\omega_2}\right)^2 - a\left(\frac{uv_1 - u_1 v}{\omega_2}\right)^2 = (-1)^{\varrho+\sigma}\omega_1^2 , \tag{8}$$

et il est évident que ni ω_1 ni ω_2 ne peut être égal à l'unité parce que les deux solutions (u, v) et (u_1, v_1) n'appartiennent pas au même couple de suites coordonnées.

2° Supposons $\omega = 4k+2$, nous aurons, au lieu de (6),

$$\omega = 2\omega_1\,\omega_2\,, \tag{9}$$

où ω_1 et ω_2 sont des nombres impairs, premiers entre eux, ce qui donnera

$$uu_1 + avv_1 \equiv 0 \pmod{2\omega_1}$$
$$uu_1 - avv_1 \equiv 0 \pmod{2\omega_2}\,,$$

donc nous aurons, comme dans le cas précédent, les deux équations résolubles

$$\left(\frac{uu_1 + avv_1}{2\omega_1}\right)^2 - a\left(\frac{uv_1 + u_1 v}{2\omega_1}\right)^2 = (-1)^{\varrho+\sigma}\omega_2^2 \tag{10}$$

$$\left(\frac{uu_1 - avv_1}{2\omega_2}\right)^2 - a\left(\frac{uv_1 - u_1 v}{2\omega_2}\right)^2 = (-1)^{\varrho+\sigma}\omega_1^2\,. \tag{11}$$

3° Soit $\omega = 8k+4$, on aura, au lieu de (6),

$$\omega = 4\omega_1\,\omega_2\,, \tag{12}$$

où ω_1 et ω_2 sont toujours impairs et premiers entre eux, de sorte qu'il existe un exposant ε, tel que

$$uu_1 + (-1)^{\varepsilon} avv_1 \equiv 0 \pmod{4\omega_1}$$
$$uu_1 - (-1)^{\varepsilon} avv_1 \equiv 0 \pmod{2\omega_2}\,,$$

car la différence, ou la somme, des premiers membres de ces deux congruences sont des nombres de la forme $4k+2$.

Cela posé, nous aurons, dans ce cas, les deux équations résolubles

$$\left(\frac{uu_1 + (-1)^{\varepsilon} avv_1}{4\omega_1}\right)^2 - a\left(\frac{uv_1 + (-1)^{\varepsilon} u_1 v}{4\omega_1}\right)^2 = (-1)^{\varrho+\sigma}\omega_2^2 \tag{13}$$

$$\left(\frac{uu_1 - (-1)^{\varepsilon} avv_1}{2\omega_2}\right)^2 - a\left(\frac{uv_1 - (-1)^{\varepsilon} u_1 v}{2\omega_2}\right)^2 = (-1)^{\varrho+\sigma}\omega_1^2\,. \tag{14}$$

4° Soit a multiple de 8, on aura, au lieu de (6),

$$\omega = 2^n\omega_1\,\omega_2\,, \quad n \geqq 3\,, \tag{15}$$

où ω_1 et ω_2 sont impairs et premiers entre eux, et les congruences (5) donnent ici, comme dans le cas précédent,

$$uu_1+(-1)^{\varepsilon}avv_1 \equiv 0 \pmod{2\omega_1}$$
$$uu_1-(-1)^{\varepsilon}avv_1 \equiv 0 \pmod{2^{n-1}\omega_2},$$

de sorte qu'il résulte finalement les deux équations résolubles

$$(16)\quad \left\{ \left(\frac{uu_1+(-1)^{\varepsilon}avv_1}{2\omega_1}\right)^2 - a\left(\frac{uv_1+(-1)^{\varepsilon}u_1v}{2\omega_1}\right)^2 = (-1)^{\varrho+\sigma}2^{2n-2}\omega_2^2 \right.$$

$$(17)\quad \left\{ \left(\frac{uu_1-(-1)^{\varepsilon}avv_1}{2^{n-1}\omega_2}\right)^2 - a\left(\frac{uv_1-(-1)^{\varepsilon}u_1v}{2^{n-1}\omega_2}\right)^2 = (-1)^{\varrho+\sigma}\omega_1^2 . \right.$$

Du reste, les multiplications que nous venons d'étudier ici possèdent les mêmes propriétés curieuses que celles établies dans l'article VII, où les paramètres sont premiers entre eux, nous le verrons dans l'article qui suit.

X. Des équations du genre 4.

Soient p et q deux nombres premiers inégaux, et soient les exposants ϱ et σ choisis tels que le produit $p^{\varrho}q^{\sigma}$ n'est pas de la forme $4k+2$, les résultats généraux, obtenus dans l'article VIII, donnent immédiatement la proposition:

I. Supposons décomposable l'équation de LAGRANGE

$$(1)\qquad u^2-av^2 = (-1)^m p^{\varrho}q^{\sigma},$$

cette équation est précisément du rang 4.

Or, cette condition suffisante n'est pas nécessaire, pour que l'équation (1) soit du genre 4. Quant à la démonstration de ce postulat, nous avons tout d'abord à démontrer cette autre proposition:

II. Supposons que l'équation (1) soit du genre 4, ces deux autres équations

$$(2) \qquad u^2 - av^2 = (-1)^{\lambda} p^{2\varrho}, \quad u^2 - av^2 = (-1)^{\mu} q^{2\sigma}$$

sont aussi résolubles, pourvu que les nombres premiers p et q soient tous deux impairs.

En effet, désignons par (s, t) et (u, v) deux solutions de l'équation (1) qui n'appartiennent pas au même couple de suites coordonnées, nous savons, conformément aux résultats obtenus dans l'article IV, que la multiplication des deux équations

$$s^2 - at^2 = (-1)^{\alpha} p^{\varrho} q^{\sigma}, \quad u^2 - av^2 = (-1)^{\beta} p^{\varrho} q^{\sigma}$$

ne conduira jamais à l'équation de FERMAT.

Cela posé, il existe, en vertu du théorème I de l'article IV, un éxposant δ, tel que

$$su + (-1)^{\delta} atv \equiv 0 \pmod{p^{\varrho}}$$

$$su - (-1)^{\delta} atv \equiv 0 \pmod{q^{\sigma}},$$

ce qui conduira immédiatement au but.

Quant à l'inversion de la proposition II, nous préférons de démontrer le théorème plus général:

III. Supposons résolubles les deux équations de LAGRANGE

$$(3) \qquad u^2 - av^2 = (-1)^{\lambda} p^{2\varrho} \omega, \quad u^2 - av^2 = (-1)^{\mu} p^{\varrho} \omega,$$

où $\omega > 2$ et où p est un nombre premier impair qui ne divise pas ω, la dernière de ces équations est au moins du rang 4.

En effet, désignons par (s, t) et (s_1, t_1) deux solutions appartenant à des suites coordonnées de la seconde des équations (3), par (u, v) et (u_1, v_1) des solutions appartenant aux deux suites coordonnées de la première des équations susdites, il existe un exposant δ, tel que

$$|su+(-1)^{\delta}atv| = p^{\varrho}k\,, \qquad |sv+(-1)^{\delta}tu| = p^{\varrho}l$$
$$|su_1-(-1)^{\delta}atv_1| = p^{\varrho}k_1\,, \quad |sv_1-(-1)^{\delta}tu_1| = p^{\varrho}l_1\,,$$

et il s'agit donc de démontrer que les solutions (k, l) et (k_1, l_1) de la dernière des équations (3) n'appartiennent pas au même couple de suites coordonnées que (s, t).

Or, remarquons que la solution (s_1, t_1) donnera des formules analogues aux précédentes, nous pouvons nous borner à l'étude des nombres provenus des multiplications positives.

Supposons donc, en premier lieu, que la solution (α, β), définie par les formules,

$$(4) \qquad su+atv = p^{\varrho}\alpha\,, \quad sv+tu = p^{\varrho}\beta$$

appartienne à la même suite que (s, t), il est possible de choisir la solution (u, v), telle que

$$su+atv = p^{\varrho}(sA_{\gamma}+atB_{\gamma})$$
$$sv+tu = p^{\varrho}(sB_{\gamma}+tA_{\gamma})$$

où γ est un indice quelconque, et ces deux équations, homogènes en s et t, ne sont pas possibles, à moins que leur déterminant ne disparisse, ce qui donnera

$$(u-p^{\varrho}A_{\gamma})^2 = a(v-p^{\varrho}B_{\gamma})^2\,,$$

équation qui est impossible, parce que la base a n'est pas un carré exact, et les deux équations simultanées

$$u = p^{\varrho}A_{\gamma}\,, \quad v = p^{\varrho}B_{\gamma}$$

sont exclues.

En second lieu, supposons que la solution (α, β) définie par les formules (4), appartienne à la suite coordonnée à celle qui contient (s, t), il résulte des expressions de la forme

$$su+atv = p^{\varrho}s_1\,, \quad tu+sv = p^{\varrho}t_1\,,$$

ce qui donnera

$$(5)\quad \begin{cases} u(s^2+at^2)+av(2st) = p^{2\varrho}A_\gamma \\ v(s^2+at^2)+u(2st) = p^{2\varrho}B_\gamma , \end{cases}$$

où γ est un indice convenablement choisi.

Or, les deux nombres

$$(6)\qquad U = s^2+at^2, \quad V = 2st$$

satisfont à l'équation résoluble

$$(7)\qquad U^2 - aV^2 = p^{2\varrho}\omega^2 ,$$

et il résulte, en vertu des équations (5),

$$(-1)^\alpha U = \omega(uA_\gamma - avB_\gamma)$$
$$(-1)^\alpha V = \omega(uB_\gamma - vA_\gamma) ,$$

ce qui est impossible, parce que U et V sont tous deux premiers avec ω.

Cela posé, il est évident que l'inversion de la proposition II se présente sous la forme:

IV. Supposons résoluble l'équation (1), les équations (2) sont en même temps résolubles ou non, et, en cas de résolubilité, l'équation (1) est du genre 4.

Les équations non décomposables du genre 4 et de la forme (1) sont très nombreuses, et leur multiplication présente les mêmes propriétés curieuses que les équations générales étudiées dans l'article VII, nous le verrons dans les exemples suivants.

Exemple I. $\qquad a = 34, \quad \omega = 15.$

L'équation non décomposable

$$u^2 - 34v^2 = (-1)^\vartheta 15$$

est du rang 4, en admettant deux couples de suites coordonnées s et s', déterminées par les solutions

$$(8)\qquad 7^2 - 34\cdot 1^2 = 41^2 - 34\cdot 7^2 = 15 ,$$

t et t' déterminées par les solutions

(9) $$11^2-34\cdot 2^2 = 23^2-34\cdot 4^2 = -15,$$

tandis que l'équation

$$u^2-34v^2 = -9$$

admet les deux suites coordonnées σ et σ' déterminées par les solutions

(10) $$29^2-34\cdot 5^2 = 5^2-34\cdot 1^2 = -9,$$

et les deux suites coordonnées τ et τ' de l'équation

$$u^2-34v^2 = -25$$

sont déterminées par les solutions

(11) $$99^2-34\cdot 17^2 = 3^2-34\cdot 1^2 = -25.$$

Ces définitions adoptées, on aura, en multipliant les équations (8) et (9),

$$(+)\,st = \sigma, \quad (+)\,st' = \tau$$
$$(+)\,s't' = (-)\,st' = (-)\,s't = \sigma'$$
$$(+)\,s't = (-)\,st = (-)\,s't' = \tau',$$

tandis que la multiplication de (8) et (10) donnera

$$(+)\,s'\sigma' = (-)\,s\sigma' = (-)\,s'\sigma = t, \quad (+)\,s\sigma = t',$$

et l'on trouvera des résultats analogues, en multipliant les autres équations en question.

Exemple II. $a = 10, \quad \omega = 39.$

Les suites coordonnées s et s' de l'équation

$$u^2-10v^2 = \pm 39$$

sont déterminées par les solutions

(12) $$1^2-10\cdot 2^2 = -39, \quad 17^2-10\cdot 5^2 = 39,$$

les suites coordonnées t et t' par les équations

(13) $$7^2-10\cdot 1^2 = 39, \quad 11^2-10\cdot 4^2 = -39.$$

tandis que les suites coordonnées σ et σ' de l'équation

$$u^2-10v^2 = \pm 9$$

proviennent des solutions

(14) $$1^2-10\cdot 1^2=-9,\quad 7^2-10\cdot 2^2=9$$

et les suites coordonnées τ et τ' de

$$u^2-10v^2=\pm 169$$

ont leurs premiers éléments déterminés par les solutions

(15) $$9^2-10\cdot 5^2=-169,\quad 23^2-10\cdot 6^2=169.$$

on trouve ici, en multipliant les équations (12) et (13),

$$\sigma'=(+)st',\quad \sigma=(+)s't=(+)st'=(-)st$$
$$\tau=(+)st,\quad \tau'=(+)s't=(-)s't'=(-)st',$$

tandis que la multiplication de (12) et (14) donnera

$$t=(+)s\sigma,\quad t'=(+)s'\sigma'=(-)s\sigma'=(-)s'\sigma,$$

et l'on obtiendra des résultats analogues, en multipliant les autres équations en question.

Quant aux bases paires de la forme (1), nous avons à démontrer les deux propositions suivantes:

V. L'équation de Lagrange

(16) $$u^2-av^2=(-1)^{\varkappa}4p^{\varrho},$$

où p est un nombre premier impair, ne peut jamais être du rang 4, à moins qu'elle ne soit décomposable.

Soient, en effet, (s, t) et (u, v) deux solutions de l'équation (16) appartenant à deux couples différents de suites coordonnées, on aura

(17) $$(su\pm atv)^2-a(sv\pm tu)^2=(-1)^{\lambda}16p^{2\varrho}.$$

Or, il existe un exposant ε, tel que

(18) $$su+(-1)^{\varepsilon}atv=4k+2,\quad st+(-1)^{\varepsilon}uv=4k_1+2,$$

et ces valeurs sont nécessairement multiples de p^{ϱ}, parce que l'équation (17) ne peut jamais être une équation de Fermat, ce qui donnera

$$(19)\quad \left(\frac{su+(-1)^{\varepsilon}atv}{2p^{\varrho}}\right)^2 - a\left(\frac{st+(-1)^{\varepsilon}uv}{2p^{\varrho}}\right) = (-1)^{\lambda}4\,;$$

c'est-à-dire que l'équation (16) est décomposable.

VI. L'équation non décomposable

$$(20)\qquad u^2 - av^2 = (-1)^k 2^{\sigma} p^{\varrho}\,,\quad \sigma \geqq 3\,,$$

où p est un nombre premier impair, ne peut jamais être du genre 4, à moins que les deux équations

$$(21)\quad u^2 - av^2 = (-1)^{\lambda} 2^{2\sigma-2}\,,\quad u^2 - av^2 = (-1)^{\lambda} p^{2\varrho}$$

ne soient résolubles.

On aura ici, avec les mêmes significations que dans le cas précédent,

$$(22)\quad \begin{cases} su+(-1)^{\varepsilon}atv = 4k+2\,, & sv+(-1)^{\varepsilon}tu = 4k_1+2 \\ su-(-1)^{\varepsilon}atv = 2^{\sigma-1}\alpha\,, & sv-(-1)^{\varepsilon}tu = 2^{\sigma-1}\beta\,, \end{cases}$$

et il est évident que α et β sont premiers avec p, car soient α et β multiples de p ou, ce qui est la même chose, de p^{ϱ}, on trouvera une équation de la forme (19), ce qui est inadmissible, parce que a est de la forme $8l+1$.

Cela posé, on aura nécessairement

$$su+(-1)^{\varepsilon}atv = 2p^{\varrho}\alpha_1\,,\quad sv+(-1)^{\varepsilon}tu = 2p^{\varrho}\beta_1\,,$$

où α_1 et β_1 sont impairs, ce qui donnera précisément la première des équations (21).

Quant aux valeurs α et β, définies par les dernières formules (22), on aura

$$\alpha^2 - a\beta^2 = (-1)^{\lambda} 4p^{2\varrho}\,,$$

ce qui est impossible, à moins que α et β ne soient des nombres pairs, et l'on trouvera la seconde des équations (21).

CHAPITRE III

De l'opération itérative.

XI. Opération itérative du second ordre.

Soient (s_μ, t_μ) et (σ_ν, τ_ν) des éléments quelconques de deux suites coordonnées appartenant à l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^\delta \omega ,$$

savoir

$$(1) \qquad s_\mu^2 - a t_\mu^2 = (-1)^{\delta_\mu} \omega , \quad \sigma_\nu^2 - a \tau_\nu^2 = (-1)^{\varepsilon_\nu} \omega ,$$

nous avons à étudier plus profondément les multiplications positives et négatives

$$(2) \quad \begin{cases} (s_\mu s_\nu + a t_\mu t_\nu)^2 - a(t_\mu s_\nu + s_\mu t_\nu)^2 = (-1)^{\delta_\mu + \delta_\nu} \omega^2 \\ (\sigma_\mu \sigma_\nu + a \tau_\mu \tau_\nu)^2 - a(\sigma_\mu \tau_\nu + \sigma_\nu \tau_\mu)^2 = (-1)^{\varepsilon_\mu + \varepsilon_\nu} \omega^2 \\ (s_\mu \sigma_\nu - a t_\mu \tau_\nu)^2 - a(s_\mu \tau_\nu - \sigma_\nu t_\mu)^2 = (-1)^{\delta_\mu + \varepsilon_\nu} \omega^2 , \end{cases}$$

ou, écrites sous forme commune

$$(3) \qquad u^2 - av^2 = (-1)^\varphi \omega^2 .$$

Nous ne savons dès à présent rien sur la résolubilité de cette équation, mais il est facile de démontrer la proposition:

I. Soit f le plus grand commun diviseur des deux nombres

$$(4) \qquad s_1^{(2)} = s_1^2 + a t_1^2 , \quad t_1^{(2)} = 2 s_1 t_1$$

et soit

$$(5) \qquad \omega = f \omega_1 ,$$

l'équation indéterminée

$$u_1^2 - a v_1^2 = (-1)^{\varphi} \varphi_1 \tag{6}$$

est toujours résoluble.

En effet, posons $s_1^{(2)} = f u_1$, $t_1^{(2)} = f v_1$,

u_1 et v_1 sont premiers entre eux, et il résulte, en vertu de (3), que ω est divisible par f, ce qui donnera l'équation résoluble (6).

Posons ensuite

$$\sigma_1^{(2)} = \sigma_1^2 + a\tau_1^2, \quad \tau_1^{(2)} = 2\sigma_1\tau_1, \tag{7}$$

puis appliquons les formules fondamentales

$$s_1\sigma_1 + a t_1\tau_1 = \omega A_1, \quad s_1\tau_1 + \sigma_1 t_1 = \omega B_1,$$

nous aurons, en vertu de (1),

$$(-1)^{\vartheta_1}\sigma_1 = s_1A_1 - a t_1B_1, \quad (-1)^{\vartheta_1}\tau_1 = s_1B_1 - t_1A_1$$
$$(-1)^{\varepsilon_1}s_1 = \sigma_1A_1 - a\tau_1B_1, \quad (-1)^{\varepsilon_1}t_1 = \sigma_1B_1 - \tau_1A_1,$$

ce qui donnera, après une réduction simple,

$$\begin{cases} \sigma_1^{(2)} = A_2 s_1^{(2)} - aB_2 t_1^{(2)}, & \tau_1^{(2)} = B_2 s_1^{(2)} - A_2 t_1^{(2)} \\ s_1^{(2)} = A_2\sigma_1^{(2)} - aB_2\tau_1^{(2)}, & t_1^{(2)} = B_2\sigma_1^{(2)} - A_2\tau_1^{(2)}, \end{cases} \tag{8}$$

de sorte que nous aurons

$$s_1^{(2)}\sigma_1^{(2)} + a t_1^{(2)}\tau_1^{(2)} = \omega^2 A_2, \quad s_1^{(2)}\tau_1^{(2)} + t_1^{(2)}\sigma_1^{(2)} = \omega^2 B_2. \tag{9}$$

Cela posé, les formules (8) montrent clairement que f est aussi plus grand commun diviseur de $\sigma_1^{(2)}$ et de $\tau_1^{(2)}$, tandis qu'il résulte, en vertu des formules (9), que les deux couples

$$(s_1^{(2)}, t_1^{(2)}), \quad (\sigma_1^{(2)}, \tau_1^{(2)}) \tag{10}$$

forment, après la suppression de leur plus grand commun facteur f, deux solutions de l'équation indéterminée (6), appartenant à des suites coordonnées.

Soient maintenant (p_μ, r_μ) respectivement (π_ν, ϱ_ν) les

éléments généraux des deux suites coordonnées susdites, nous avons tout d'abord à déterminer les indices de chacune des deux solutions provenues du couple (10), et c'est une conséquence immédiate des formules (9) que ces indices sont respectivement 1 et 2.

A cet effet, supposons

$$(s_1, t_1) < (\sigma_1, \tau_1),$$

nous aurons aussi

$$(s_1^{(2)}, t_1^{(2)}) < (\sigma_1^{(2)}, \tau_1^{(2)}),$$

ce qui donnera immédiatement

$$(11)\quad \begin{cases} s_1^{(2)} = fp_1, & t_1^{(2)} = fr_1 \\ \sigma_1^{(2)} = f\pi_2, & \tau_1^{(2)} = f\varrho_2. \end{cases}$$

Cela posé, les formules récursives générales

$$s_\mu = s_1 A_{\mu-1} + a t_1 B_{\mu-1}, \quad t_\mu = s_1 B_{\mu-1} + t_1 A_{\mu-1}$$
$$\sigma_\nu = \sigma_1 A_{\nu-1} + a t_1 B_{\nu-1}, \quad \tau_\nu = s_1 B_{\nu-1} + \tau_1 A_{\nu-1}$$

donnent, après un calcul direct,

$$s_\lambda s_\mu + a t_\lambda t_\mu = s_1^{(2)} A_{\lambda+\mu-2} + a t_1^{(2)} B_{\lambda+\mu-2}$$
$$s_\lambda t_\mu + t_\lambda s_\mu = s_1^{(2)} B_{\lambda+\mu-2} + t_1^{(2)} A_{\lambda+\mu-2},$$

d'où il résulte, en vertu de (11),

$$(12)\quad s_\lambda s_\mu + a t_\lambda t_\mu = fp_{\lambda+\mu-1}, \quad s_\lambda t_\mu + t_\lambda s_\mu = fr_{\lambda+\mu-1},$$

et l'on aura, par un procédé analogue,

$$(13)\quad \sigma_\lambda \sigma_\mu + a \tau_\lambda \tau_\mu = f\pi_{\lambda+\mu}, \quad \sigma_\lambda \tau_\mu + \tau_\lambda \sigma_\mu = f\varrho_{\lambda+\mu}.$$

Quant à la troisième opération, indiquée par les formules (2), nous prenons pour point départ les formules fondamentales

$$(14)\quad s_\lambda \sigma_\nu + a t_\lambda \tau_\nu = \omega A_{\lambda+\nu-1}, \quad s_\lambda \tau_\nu + t_\lambda \sigma_\nu = \omega B_{\lambda+\nu-1},$$

et il résulte, en vertu de (12),

$$\sigma_\nu p_{\lambda+\mu-1} + a \tau_\nu r_{\lambda+\mu-1} = \omega_1 s_{\lambda+\mu+\nu-1}$$
$$\sigma_\nu r_{\lambda+\mu-1} + t_\nu p_{\lambda+\mu-1} = \omega_1 t_{\lambda+\mu+\nu-1}.$$

Cherchons ensuite, de ces deux équations, les nombres $p_{\lambda+\mu-1}$ et $r_{\lambda+\mu-1}$, puis posons

$$\lambda+\mu+\nu = \varkappa+1, \quad \varkappa > \nu,$$

nous aurons

$$(15)\quad \begin{cases} fp_{\varkappa-\nu} = (-1)^{\varepsilon_\nu}(s_\varkappa \sigma_\nu - a t_\varkappa \tau_\nu) \\ fr_{\varkappa-\nu} = (-1)^{\varepsilon_\nu}(t_\varkappa \sigma_\nu - s_\varkappa \tau_\nu). \end{cases}$$

Les formules (14) donnent de même

$$s_\nu \pi_{\lambda+\mu} + a t \varrho_{\lambda+\mu} = \omega_1 \sigma_{\lambda+\mu+\nu-1}$$
$$s_\nu \varrho_{\lambda+\mu} + t_\nu \pi_{\lambda+\mu} = \omega_1 \tau_{\lambda+\mu+\nu-1};$$

posons ensuite, comme dans le cas précédent,

$$\lambda+\mu+\nu = \varkappa+1, \quad \varkappa > \nu,$$

nous aurons ici

$$(16)\quad \begin{cases} f\pi_{\varkappa-\nu+1} = (-1)^{\vartheta_\nu}(s_\nu \sigma_\varkappa - a t_\nu \tau_\varkappa) \\ f\varrho_{\varkappa-\nu+1} = (-1)^{\vartheta_\nu}(s_\nu \tau_\varkappa - t_\nu \sigma_\varkappa). \end{cases}$$

Quant au cas spécial $\varkappa = \nu$, posons, dans (14), $\lambda = \nu$, le même procédé que dans les cas précédents donnera les formules

$$(17)\quad \begin{cases} f\pi_1 = (-1)^{\vartheta_\nu}(s_\nu \sigma_\nu - a t_\nu \tau_\nu) \\ f\varrho_1 = (-1)^{\vartheta_\nu}(s_\nu \tau_\nu - t_\nu \sigma_\nu), \end{cases}$$

valables quel que soit l'indice ν.

Cela posé, nous avons démontré le théorème fondamental:

II. Les opérations indiquées par les formules (2), conduiront, après la suppression du facteur commun f^2, à deux suites coordonnées appartenant à l'équation indéterminée (6).

Quant aux opérations que nous venons d'étudier, nous

avons encore à démontrer quelques propositions qui nous seront utiles dans ce qui suit, savoir:

III. Des équations de la forme

$$s_n s_p + a t_n t_p = k s_r , \quad s_n t_p + t_n s_p = k t_r \tag{18}$$

ne sont possibles, à moins que

$$k = \omega = 1 ; \quad s_n = A_n , \quad t_n = B_n .$$

En effet, on aura, en vertu de (18),

$$\omega^2 = k^2 \omega , \quad k^2 = \omega ;$$

de plus, on verra, en cherchant des équations (18) les nombres s_n et t_n, que k est diviseur commun de s_n et t_n, ce qui est impossible, à moins que $k = 1$, ce qui donnera $\varphi = 1$.

IV. Des équations de la forme

$$s_n s_p + a t_n t_p = k A_r , \quad s_n t_p + t_n s_p = k B_r \tag{19}$$

ne sont possibles, à moins que

$$k = \omega = 2.$$

On aura, dans ce cas,

$$k^2 = \omega^2 , \quad k = \omega ;$$

de plus, soit $n > p$, on aura, en vertu de (18), et, en appliquant les formules récursives,

$$s_n^2 + a t_n^2 = \omega A_{n+r-p} , \quad 2 s_n t_n = \omega B_{n+r-p} ,$$

ce qui donnera immédiatement $\omega = 2$, parce que ω est premier et avec s_n et avec t_n.

V. Des équations de la forme

$$s_n s_p + a t_n t_p = k \sigma_r , \quad s_n t_p + t_n s_p = k \tau_r \tag{20}$$

ne sont possibles, à moins que

$$\omega = 4 , \quad k = 2.$$

On aura, comme dans la démonstration de III,

$$\omega = k^2 ;$$

de plus, les formules récursives donnent ici, pour $n > p$,

$$s_n^2 + a t_n^2 = k \sigma_{n+r-p}, \quad s_n t_n = k \tau_{n+r-p}, \tag{21}$$

de sorte qu'il résulte immédiatement $k = 2$.

Quant à l'équation indéterminée

$$u^2 - a v^2 = (-1)^\delta 4, \tag{22}$$

dont il s'agit ici, on aura donc, en vertu des formules générales (12) et (13),

$$\begin{cases} s_\lambda s_\mu + a t_\lambda t_\mu = 2\sigma_{\lambda+\mu-1}, & s_\lambda t_\mu + t_\lambda s_\mu = 2\tau_{\lambda+\mu-1} \\ \sigma_\lambda \sigma_\mu + a\tau_\lambda \tau_\mu = 2 s_{\lambda+\mu}, & \sigma_\lambda \tau_\mu + \tau_\lambda \sigma_\mu = 2 t_{\lambda+\mu}. \end{cases} \tag{23}$$

ce qui donnera, en vertu de (22),

$$\begin{cases} \sigma_{2\lambda-1} = s_\lambda^2 - (-1)^\delta 2, & \tau_{2\lambda-1} = s_\lambda t_\lambda \\ s_{2\lambda} = \sigma_\lambda^2 - (-1)^\epsilon 2, & t_{2\lambda} = \sigma_\lambda \tau_\lambda ; \end{cases} \tag{24}$$

c'est-à-dire que l'on aura toujours

$$\sigma_1^2 - a\tau_1^2 = 4,$$

d'où il résulte la proposition curieuse, due à CAYLEY:[1]

VI. Soit, dans (22), admissible l'exposant $\delta = 1$, ou, ce qui est la même chose, soit a une base de première espèce, la plus petite solution (s_1, t_1) correspond au paramètre -4.

Nous désignons pour abréger comme opérations itératives du second ordre les formules (2) que nous venons d'étudier.

XII. Opérations itératives d'un ordre quelconque.

Soit (s_λ, t_λ) une solution quelconque de l'équation de LAGRANGE

$$u^2 - a v^2 = (-1)^\delta \omega, \tag{1}$$

nous avons, dans l'article précédent, étudié l'opération ité-

[1] Journal de Crelle, t. 53, p. 369—371; 1857.

rative du second ordre. Quant à l'opération itérative de l'ordre n, nous posons

$$(2)\quad s_\mu^{(n)} = s_\mu^{(1)} s_\mu^{(n-1)} + a\, t_\mu^{(1)} t_\mu^{(n-1)}, \quad t_\mu^{(n)} = s_\mu^{(1)} t_\mu^{(n-1)} + t_\mu^{(1)} s_\mu^{(n-1)},$$

ce qui donnera pour l'équation de FERMAT

$$(3)\qquad A_\mu^{(n)} = A_{n\mu}, \quad B_\mu^{(n)} = B_{n\mu},$$

tandis que l'opération itérative du $n^{\text{ième}}$ ordre conduira à une équation de la forme

$$u^2 - av^2 = (-1)^{n\delta}\omega^n.$$

Or, on démontrera, comme dans l'article précédent, la proposition fondamentale:

I. Soit f_n le plus grand commun diviseur de $s_1^{(n)}$ et $t_1^{(n)}$, et soit

$$(4)\qquad \omega^n = f_n^2\, \omega_n,$$

l'équation de LAGRANGE

$$(5)\qquad u^2 - av^2 = (-1)^{n\delta}\omega_n$$

est toujours résoluble.

Posons ensuite

$$(6)\qquad s_1^{(n)} = f_n p_z^{(n)}, \quad t_1^{(n)} = f_n r_z^{(n)},$$

nous aurons généralement

$$(7)\qquad s_\mu^{(n)} = f_n p_{z+\mu n-n}, \quad t_\mu^{(n)} = f_n r_{z+\mu n-n},$$

En effet, soit $n = 2$, on aura $z = 1$ ou $z = 2$, et les formules (7), ainsi obtenues, ne sont autre chose que les formules (12) et (13) de l'article précédent, et la conclusion de n à $n+1$ est évidente.

Soit particulièrement $\omega = 2$, on aura, en vertu de la proposition II de l'article précédent,

$$(8)\quad \begin{cases} s_1^{(2n)} = 2^n A_n, & t_1^{(2n)} = 2^n B_n \\ s_1^{(2n+1)} = 2^n s_{2n+1}, & t_1^{(2n+1)} = 2^n t_{2n+1}. \end{cases}$$

Supposons maintenant $\varphi > 2$, (s_1, t_1) a une solution

réciproque (σ_1, τ_1) et les nombres $\pi_\mu^{(n)}$ et $\varrho_\mu^{(n)}$ définies par les formules

$$(9)\quad \begin{cases} \sigma_\nu^{(n)} = f_n \pi_{\lambda+\mu n-n}^{(n)}, \quad \tau_\nu^{(n)} = f_n \varrho_{\lambda+\mu n-n}^{(n)} \\ \sigma_1^{(n)} = f_n \pi_\lambda^{(n)}, \quad \tau_1^{(n)} = f_n \varrho_\lambda^{(n)} \end{cases}$$

satisfont aussi à l'équation indéterminée (5).

De plus, nous avons à démontrer le théorème fondamental:

II. Les solutions $(p_m^{(n)}, r_m^{(n)})$ et $(\pi_m^{(n)}, \varrho_m^{(n)})$ de l'équation (5) appartiennent à deux suites coordonnées, car

$$(10)\quad s_1^{(n)}\sigma_1^{(n)} + a t_1^{(n)}\tau_1^{(n)} = \omega^n A_n, \quad s_1^{(n)}\tau_1^{(n)} + t_1^{(n)}\sigma_1^{(n)} = \omega^n B_n,$$

ou, ce qui est la même chose,

$$(11)\quad p_\varkappa^{(n)}\pi_\lambda^{(n)} + a r_\varkappa^{(n)}\varrho_\lambda^{(n)} = \omega_n A_n, \quad p_\varkappa^{(n)}\varrho_\lambda^{(n)} + r_\varkappa^{(n)}\pi_\lambda^{(n)} = \omega_n B_n.$$

Dans l'article précédent, nous avons démontré les formules (10) et (11) qui correspondent à $n = 2$. Supposons donc vraies les formules (10), puis multiplions ces deux équations par s_1 et t_1, respectivement par t_1 et s_1, nous aurons, en additionnant les deux formules ainsi obtenues,

$$(12)\quad \begin{cases} \sigma_1^{(n)} s_1^{(n+1)} + a\tau_1^{(n)} t_1^{(n+1)} = \omega^n s_{n+1}, \\ \tau_1^{(n)} s_1^{(n+1)} + \sigma_1^{(n)} t_1^{(n+1)} = \omega^n t_{n+1}. \end{cases}$$

Multiplions ensuite par σ_1 et τ_1, respectivement par τ_1 et σ_1 ces deux formules, nous aurons, en additionnant, les formules obtenues de (10) en remplaçant n par $n+1$.

Quant aux indices $\varkappa$ et λ qui figurent dans les formules (6) et (9), on aura, en vertu de (10) ou (11)

$$(13)\qquad \varkappa + \lambda = n + 1.$$

Or, posons $\varphi = 2$, les formules (8) donnent immédiatement la proposition:

III. Soit (s_1, t_1) la plus petite des solutions ap-

partenant à la suite fermée de l'quation (1), on aura généralement

$$(14)\quad \begin{cases} \varkappa = \lambda = m, \quad n = 2m-1 \\ \varkappa = m, \quad \lambda = m+1, \quad n = 2m. \end{cases}$$

Étudions maintenant le paramètre $\varphi = 4$, les formules (23) de l'article précédent donnent

$$s_\lambda s_1 + a t_\lambda t_1 = 2\sigma_\lambda, \qquad t_\lambda s_1 + s_\lambda t_1 = 2\tau_\lambda$$
$$\sigma_\lambda \sigma_1 + a\tau_\lambda \tau_1 = 2 s_{\lambda+1}, \qquad \tau_\lambda \sigma_1 + \sigma_\lambda \tau_1 = 2 t_{\lambda+1},$$

de sorte qu'il résulte, en vertu des formules (24) de l'article précédent, les résultats généraux

$$(15)\quad \begin{cases} s_1^{(3n+1)} = 2^{3n} s_{n+1}, & t_1^{(3n+1)} = 2^{3n} t_{n+1} \\ s_1^{(3n+2)} = 2^{3n+1}\sigma_{n+1}, & t_1^{(3n+2)} = 2^{3n+1}\tau_{n+1} \\ s_1^{(3n+3)} = 2^{3n+3} A_{n+1}, & t_1^{(3n+3)} = 2^{3n+3} B_{n+1}. \end{cases}$$

La suite coordonnée, formée des solutions $(\sigma_\lambda, \tau_\lambda)$, donnent de même

$$(16)\quad \begin{cases} \sigma_1^{(3n+1)} = 2^{3n}\sigma_{2n+1}, & \tau_1^{(3n+1)} = 2^{3n}\tau_{2n+1} \\ \sigma_1^{(3n+2)} = 2^{3n+1} s_{2n+2}, & \tau_1^{(3n+2)} = 2^{3n+1} t_{2n+2} \\ \sigma_1^{(3n+3)} = 2^{3n+3} A_{2n+2}, & \tau_1^{(3n+3)} = 2^{3n+3} B_{2n+2}; \end{cases}$$

c'est-à-dire que nous aurons pour $\varphi = 4$

$$(17)\qquad f_{3n+1} = 2^{3n}, \quad f_{3n+2} = 2^{3n+1}, \quad f_{3n+3} = 2^{3n+3}$$

tandis que les suites $(p_\lambda^{(3n+1)}, r_\lambda^{(3n+1)})$ et $(\pi_\lambda^{(3n+1)}, \varrho_\lambda^{(3n+1)})$ coïncident avec les suites (s_λ, t_λ) et $(\sigma_\lambda, \tau_\lambda)$, et les suites $(p_\lambda^{(3n+2)}, r_\lambda^{(3n+2)})$, $\pi_\lambda^{(3n+2)}, \varrho_\lambda^{(3n+2)})$ coïncident avec $(\sigma_\lambda, \tau_\lambda)$ et (s_λ, t_λ), et les deux suites $(p_\lambda^{(3n)}, r_\lambda^{(3n)})$ et $(\pi_\lambda^{(3n)}, \varrho_\lambda^{(3n)})$ donnent des solutions de l'équation de FERMAT.

Mentionnons encore que le paramètre $\varphi = 2$ donnera

$$(18)\qquad f_{2n} = f_{2n+1} = 2^n,$$

et que la suite $(p_\lambda^{(2n)}, r_\lambda^{(2n)})$ donne des solutions de l'équa-

tion de FERMAT, tandis que $(p_\lambda^{(2n+1)}, r_\lambda^{(2n+1)})$ n'est autre chose que la suite (s_λ, t_λ) elle-même.

XIII. Détermination générale du facteur f_n.

Il est très intéressant, ce me semble, que le facteur f_n qui joue un rôle fondamental dans l'opération itérative, est facile à déterminer.

A cet effet, nous avons à donner les expressions explicites des nombres $s_\lambda^{(n)}$ et $t_\lambda^{(n)}$, $\sigma_\lambda^{(n)}$ et $\tau_\lambda^{(n)}$, ce qui exige l'application des polynomes $\xi_n(\alpha)$ et $\eta_n(\alpha)$ de CAUCHY, définies par les identités

$$(1) \qquad \xi_n(\cos x) = \cos nx\,, \quad \eta_n(x) = \frac{\sin nx}{\sin x}\,,$$

de sorte que les formules d'addition des fonctions $\cos(nx+x)$ et $\sin(nx+x)$ donnent, pour $\xi_n(\alpha)$ et $\eta_n(\alpha)$, les formules récursives

$$(2) \quad \begin{cases} \xi_{n+1}(\alpha) = \alpha\,\xi_n(\alpha) + (\alpha^2-1)\,\eta_n(\alpha) \\ \eta_{n+1}(\alpha) = \alpha\,\eta_n(\alpha) + \xi_n(\alpha)\,. \end{cases}$$

Posons ensuite

$$(3) \quad \varphi_n(\alpha,\omega) = \omega^{\frac{n}{2}}\,\xi_n\left(\frac{\alpha}{\sqrt{\omega}}\right), \quad \psi_n(\alpha,\omega) = \omega^{\frac{n-1}{2}}\,\eta_n\left(\frac{\alpha}{\sqrt{\omega}}\right),$$

il resulte, en vertu de (2),

$$(4) \quad \begin{cases} \varphi_{n+1}(\alpha,\omega) = \alpha\,\varphi_n(\alpha,\omega) + (\alpha^2-\omega)\,\psi_n(\alpha,\omega) \\ \psi_{n+1}(\alpha,\omega) = \alpha\,\psi_n(\alpha,\omega) + \varphi_n(\alpha,\omega)\,, \end{cases}$$

et les premiers de ces polynomes deviennent

$$\begin{aligned} \varphi_1(\alpha,\omega) &= \alpha\,, & \psi_1(\alpha,\omega) &= 1 \\ \varphi_2(\alpha,\omega) &= 2\alpha^2+\omega\,, & \psi_2(\alpha,\omega) &= 2\alpha \\ \varphi_3(\alpha,\omega) &= 4\alpha^3+3\alpha\omega\,, & \psi_3(\alpha,\omega) &= 4\alpha^2+\omega. \end{aligned}$$

Cela posé, nous avons à démontrer la proposition curieuse:

I. Soit (s_λ, t_λ) une solution quelconque de l'équa-

tion de LAGRANGE

$$u^2 - av^2 = \varrho\,, \tag{5}$$

on aura, quel que soit l'indice n

$$s_\lambda^{(n)} = \varphi_n(s_\lambda, \omega)\,, \quad t_\lambda^{(n)} = t_\lambda \psi_n(s_\lambda, \omega). \tag{6}$$

En effet, remarquons que l'équation (5) se présente sous la forme

$$av^2 = u^2 - \omega\,,$$

ou, ce qui est la même chose,

$$u^2 - (u^2 - \omega)\cdot 1^2 = \omega\,, \tag{7}$$

il est évident que les formules (6) sont vraies pour $n = 1$.

Supposons ensuite valables, pour une certaine valeur de n, la formule

$$(\varphi_n(u, \omega))^2 - (u^2 - \omega)(\psi_n(u, \omega))^2 = \omega\,, \tag{8}$$

nous aurons, en multipliant les équations (7) et (8), puis appliquant les formules récursives (4), les formules obtenues de (8) en y remplaçant n par $n+1$.

Enfin, introduisons, dans (8), la valeur av^2 de $u^2 - \omega$, puis posons

$$u = s_\lambda\,, \quad v = t_\lambda\,,$$

nous aurons les formules générales (6), ce qui donnera immédiatement les expressions explicites de $s_\lambda^{(n)}$ et $t_\lambda^{(n)}$, car

$$\left\{\begin{aligned} \varphi_n(\alpha, \omega) &= 2^{n-1}\alpha^n + \sum_{r=1}^{\leq \frac{n}{2}} \frac{(-1)^r n}{2r} \binom{n-r-1}{r-1} (2\alpha)^{n-2r}\omega^r \\ \psi_n(\alpha, \omega) &= \sum_{r=0}^{\leq \frac{n-1}{2}} (-1)^r \binom{n-r-1}{r-1} (2\alpha)^{n-2r-1}\omega^r. \end{aligned}\right. \tag{9}$$

De plus, on peut obtenir des formules correspondantes pour l'équation indéterminée

$$u^2 - av^2 = -\varrho$$

en remplaçant, dans les formules précédentes, ω par $-\omega$.

Cela posé, il est facile de déterminer la valeur du facteur f_n qui correspond à l'équation indéterminée

$$u^2 - av^2 = (-1)^\delta \omega, \tag{10}$$

car on aura immédiatement les théorèmes suivants:

II. Soit, dans l'équation (10), ω un nombre impair, on aura toujours

$$f_n = 1,$$

de sorte que les équations

$$u^2 - av^2 = (-1)^{n\delta} \omega^n \tag{11}$$

sont résolubles, quel que soit le positif entier n.

En effet, remarquons que les coefficients numériques des polynomes $\varphi_n(\alpha, \omega)$ et $\psi_n(\alpha, \omega)$ sont des nombres entiers, il résulte, en vertu de (9),

$$\varphi_n(\alpha, \omega) = 2^{n-1}\alpha^n + \omega K, \quad \psi_n(\alpha, \omega) = (2\alpha)^{n-1} + \alpha K_1, \tag{12}$$

où K et K_1 sont des nombres entiers; c'est-à-dire que $\varphi_n(\alpha, \omega)$ et $\psi_n(\alpha, \omega)$ sont tous deux premiers avec le nombre impair ω, pourvu que α le soit.

Quant à l'équation (10) qui correspond à une valeur paire de ω, nous écrivons cette équation sous la forme

$$u^2 - av^2 = (-1)^\delta 2^p \omega, \tag{13}$$

où ω est de nouveau un nombre impair, ce qui donnera, en vertu de (10),

$$\varphi_n(\alpha, 2^p\omega) = 2^{n-1}\alpha^n + 2^p\omega K, \quad \psi_n(\alpha, 2^p\omega) = (2\alpha)^{n-1} + 2^p\omega K_1,$$

de sorte que f_n est toujours une puissance du premier 2, car les deux nombres impairs α et ω sont premiers entre eux.

Cela posé, nous avons à étudier séparément les trois cas suivants:

III. Soit, dans (13), $p = 1$, on aura

$$f_{2n} = f_{2n+1} = 2^n,$$

de sorte que les équations

(14) $\qquad u^2 - av^2 = \omega^{2n}, \quad u^2 - av^2 = (-1)^{\delta} 2\omega^{2n+1}$

sont toujours résolubles.

On aura, en effet,

$$\psi_n(\alpha, 2\omega) = \sum_{r=0}^{\leqq \frac{n-1}{2}} (-1)^r \binom{n-r-1}{r} \alpha^{n-2r-1} \omega^r 2^{n-r-1},$$

ce qui donnera immédiatement

$$\psi_n(\alpha, 2\omega) = 2^m(2k+1), \quad n = 2m, \quad n = 2m+1.$$

IV. Soit, dans (13), $p = 2$, on aura de même

$$f_{3n+1} = 2^{3n}, \quad f_{3n+2} = 2^{3n+1}, \quad f_{3n+3} = 2^{3n+3},$$

de sorte que les équations indéterminées

$$(15) \quad \begin{cases} u^2 - av^2 = (-1)^{m\delta} 4\omega^m, & m = 3n \pm 1 \\ u^2 - av^2 = (-1)^{m\delta} \omega^m, & m = 3n \end{cases}$$

sont toujours résolubles.

Dans ce cas, la dernière des formules (9) donnera

$$\psi_n(\alpha, 4\omega) = 2^{n-1} \sum_{r=0}^{= \frac{n-1}{2}} (-1)^r \binom{n-r-1}{r} \alpha^{n-2r-1} \omega^r,$$

et il est évident que le facteur de 2^{n-1} qui figure au second membre de cette équation a la même parité quels que soient les deux nombres impairs α et ω, de sorte que l'hypothèse $\alpha = \omega = 1$ conduira immédiatement au résultat susdit.

V. Soit, dans (13), $p \geqq 3$, on aura

$$f_n = 2^{n-1},$$

de sorte que l'équation indéterminée

$$(16) \qquad u^2 - av^2 = (-1)^{n\delta} 2^{np-2n+2} \omega^n$$

est toujours résoluble, quel que soit n.

On aura, dans ce cas, en vertu de (9),

$$\psi_n(\alpha, 2^p\omega) = 2^{n-1} \left[\alpha^{n-1} + \sum_{r=1}^{\leqq \frac{n-1}{2}} (-1)^r \binom{n-r-1}{r} 2^{pr-2r} \alpha^{n-2r-1} \omega^r \right],$$

et il est évident que le facteur de 2^{n-1} qui figure au second membre de cette équation est un nombre impair.

Remarquons en passant, que la proposition V donne, comme corollaire, cette autre:

VI. Le nombre 8 est la seule valeur paire de ω, pour laquelle toutes les équations

$$u^2 - av^2 = (-1)^{n\delta}\omega^n, \tag{17}$$

soient résolubles, pourvu que l'équation qui correspond à $n = 1$ ait cette propriété.

Remarquons encore que les résultats obtenus concernant le facteur f_n donnent immédiatement la proposition curieuse:

VII. Les deux valeurs

$$\omega = 2, \quad \omega = 4$$

représentent les seuls paramètres pour lesquels l'opération itérative détermine, à l'aide d'un élément primitif, la solution complète et de l'équation proposée

$$u^2 - av^2 = (-1)^{\delta}\omega$$

et de l'équation correspondante de Fermat

$$x^2 - ay^2 = (-1)^{\varepsilon}.$$

En effet, l'hypothèse

$$s_\lambda^{(n)} = f_n A_n$$

donnera

$$f_n^2 = \omega^n, \tag{18}$$

et, f_n étant une puissance de 2, ω aura nécessairement la même propriété, et il est évident que la condition (18) n'est remplie, à moins que

$$\omega = 2, \quad n = 2m$$

$$\omega = 4, \quad n = 3m.$$

Quant aux hypothèses

$$s_\lambda^{(n)} = f_n s_\mu, \quad s_\lambda^{(n)} = f_n \sigma_\nu,$$

on aura de même

$$f_n^2 = \omega^{n-1},$$

ce qui donnera respectivement

$$\omega = 2, \quad n = 2m+1; \quad \omega = 4, \quad n = 3m+1$$

et

$$\omega = 4, \quad n = 3m+2.$$

Quant à la résolution complète de toutes les autres équations de LAGRANGE, il faut connaître ou deux solutions différentes, appartenant à chaque couple de suites coordonnées, ou la plus petite solution de l'équation correspondante de FERMAT et une seule solution appartenant à chacun des couples susdits.

XIV. Des puissances d'un nombre premier.

L'opération itérative nous permet de démontrer immédiatement la proposition curieuse:

I. Supposons résolubles les deux équations de LAGRANGE

(1) $$u^2 - av^2 = (-1)^\delta p^m, \quad u^2 - av^2 = (-1)^\varepsilon p^n,$$

où p est un nombre premier impair, puis désignons par f le plus grand commun diviseur de m et n, cette autre équation

(2) $$u^2 - av^2 = (-1)^\varphi p^f$$

est aussi résoluble.

On voit que le théorème est évident dans le cas spécial, où m est divisible par n. Soit ensuite

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

les équations

$$u^2 - av^2 = (-1)^\delta p^{nq} p^r, \quad u^2 - av^2 = (-1)^{n\varepsilon} p^{nq}$$

sont toutes deux résolubles, de sorte que cette autre équation

$$u^2 - av^2 = (-1)^{\delta + n\varepsilon} p^r$$

aura la même propriété, et, en continuant cette opération, on trouve finalement l'équation (2).

Supposons maintenant que r soit la plus petite valeur de l'exposant m, pour laquelle l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^\delta p^m \tag{3}$$

soit résoluble, nous disons pour abréger que p^r est la puissance primitive du nombre premier impair p qui appartient à la base a, et la proposition I donnera immédiatement cette autre:

II. Supposons résoluble l'équation (3), où p est un nombre premier impair, l'exposant m est divisible par l'exposant primitif de p qui appartient à la base a.

Quant au nombre premier 2, des théorèmes généraux analogues aux précédents ne sont pas valables, mais il est facile de démontrer cette autre proposition:

III. Supposons résolubles les deux équations de LAGRANGE

$$u^2 - av^2 = (-1)^\delta 2^n, \quad u^2 - av^2 = (-1)^\delta 2^{n+1}, \tag{4}$$

toutes les équations

$$u^2 - uv^2 = (-1)^{\delta_1} 2^q, \quad q \geqq 3, \tag{5}$$

sont résolubles aussi.

Remarquons tout d'abord que les deux équations (4) ne sont pas résolubles en même temps, à moins que $n \geqq 3$, la multiplication de ces deux équations donnera immédiatement l'équation résoluble

$$u^2 - av^2 = (-1)^{\delta+\varepsilon} 8, \tag{6}$$

et la résolubilité des équations (5) est une conséquence immédiate de la proposition VI de l'article précédent.

CHAPITRE IV

Rang et ordre des nombres.

XV. Sur le rang de certains nombres premiers.

Désignons comme ordinairement par (A_μ, B_μ) une solution quelconque de l'équation de FERMAT ayant la base a, savoir

$$A_\mu^2 - a B_\mu^2 = (-1)^{\mu\varepsilon}, \tag{1}$$

puis désignons par p un positif entier quelconque, il existe un indice r, le rang de p par rapport à la base a,[1] tel que tous les nombres B_{nr} sont multiples de p, tandis qu'aucun autre des nombres B_μ ne peut posséder cette propriété.

Remarquons, en passant, que les nombres

$$\alpha_n = A_{nr}, \quad \beta_n = \frac{1}{p} B_{nr}$$

représentent toutes les solutions de cette autre équation de FERMAT

$$x^2 - a p^2 y^2 = (-1)^{r\varepsilon},$$

déduite de l'équation (1).

La détermination générale du rang d'un nombre donné est évidemment un problème très difficile, mais il est facile de démontrer les propositions suivantes:

I. Soit la base a résidu quadratique du nombre premier p, le rang de p est toujours diviseur de $p-1$.

[1] Voir mon Mémoire: Recherches sur l'Équation de Fermat, article X.

Posons pour abréger

$$p = 2\mu + 1 ,$$

les formules de LAGRANGE

$$A_{p-1} = \sum_{s=0}^{s=\mu} \binom{p-1}{2s} A_1^{2\mu-2s} B_1^{2s} a^s$$

$$B_{p-1} = \sum_{s=0}^{s=\mu-1} \binom{p-1}{2s+1} A_1^{2\mu-2s-1} B_1^{2s+1} a^s$$

suppléées par les congruences

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}, \quad 0 \leqq k \leqq p-1,$$

donnent immédiatement

$$A_{p-1} \equiv A_1^{p-1} \sum_{s=0}^{s=\mu} \left(\frac{B_1^2 a}{A_1^2}\right)^s \pmod{p}$$

$$B_{p-1} \equiv -A_1^{p-2} B_1 \sum_{s=0}^{s=\mu-1} \left(\frac{B_1^2 a}{A_1^2}\right)^s \pmod{p},$$

d'où, en vertu de (1),

$$A_{p-1} \equiv (-1)^\varepsilon (A_1^{p+1} - a^{\mu+1} B_1^{p+1}) \pmod{p}$$

$$B_{p-1} \equiv (-1)^{\varepsilon+1} A_1 B_1 (A_1^{p-1} - a^\mu B_1^{p-1}) \pmod{p}.$$

Appliquons ensuite le théorème de FERMAT, nous aurons, quel que soit le nombre premier impair p,

$$A_{p-1} \equiv (-1)^\varepsilon (A_1^2 - a^{\mu+1} B_1^2) \pmod{p} \tag{2}$$

$$B_{p-1} \equiv (-1)^{\varepsilon+1} (1 - a^\mu) A_1 B_1 \pmod{p}. \tag{3}$$

Soit maintenant a résidu quadratique de p, on aura donc les congruences

$$A_{p-1} \equiv 1 \pmod{p} \tag{4}$$

$$B_{p-1} \equiv 0 \pmod{p} \tag{5}$$

dont la dernière n'est autre chose que la proposition I.

M. G. RASCH, en appliquant les formules de LAGRANGE

$$2aB_\mu^2 = A_{p-1} - (-1)^{\mu\varepsilon}$$
$$2A_\mu B_\mu = B_{p-1},$$

a déduit de (4) cette autre congruence

$$2aB_\mu^2 \equiv 1 - (-1)^{\mu\varepsilon} \pmod{p},$$

ce qui donnera

(6) $$B_\mu \equiv 0 \pmod{p}$$

(7) $$A_\mu \equiv 0 \pmod{p}$$

selon que $\mu\varepsilon$ est pair ou impair; c'est-à-dire que M. RASCH a démontré la proposition:

II. Soit la base a résidu quadratique du nombre premier p, et soit a une base de seconde espèce ou soit p de la forme $4\nu+1$, le rang de a est diviseur de $\frac{p-1}{2}$.

Quant à la seconde des congruences de M. RASCH, j'en ai déduit la proposition curieuse:

III. Soit la base a de première espèce résidu quadratique du nombre premier $p = 4\nu+3$, le rang de p est précisément égal à $p-1$.

En effet, supposons que le rang r du premier p soit une aliquote de $p-1$, nous aurons

$$\mu = 2\nu + 1 = (2k+1)r;$$

c'est-à-dire que r est nécessairement un nombre impair, ce qui est impossible, parce que les nombres A_m et B_{2n+1} sont premiers entre eux.

A ces trois propositions, nous avons à ajouter une quatrième, savoir:

IV. Soit la base a de première espèce non-résidu du nombre premier $p = 4\nu+3$, le rang de p est toujours multiple de 4.

En effet, l'équation de FERMAT

(8) $$A_{2n+1}^2 + 1 = aB_{2n+1}^2$$

montre clairement que le nombre premier p ne peut diviser aucun des nombres B_{2n+1}, de sorte que le rang de p est un nombre pair.

Soit ensuite le nombre

$$B_{4n+2} = A_{2n+1} B_{2n+1}$$

multiple de p, A_{2n+1} aura nécessairement la même propriété, ce qui donnera, en vertu de (8),

$$a B_{2n+1}^2 \equiv 1 \pmod{p},$$

congruence qui est impossible, parce que a est non-résidu de p.

Soit par exemple $a = 2$, cette base est résidu quadratique des nombres premiers de la forme $8\mu \pm 1$ et non-résidu de $p = 8\mu \pm 3$. Le rang du nombre premier $p = 8\mu - 1$ est donc égal à $8\mu - 2$, tandis que le rang du nombre premier $8\mu + 1$ est diviseur de 4μ, et le rang du nombre premier $p = 8\mu \pm 3$ est multiple de 4.

Le nombre premier 7 est par exemple du rang 6, le nombre premier 17, au contraire, du rang 8, car

$$A_3 = 7, \quad A_4 = 17.$$

XVI. Des diviseurs réguliers.

Supposons que le diviseur d de la base a soit premier avec le nombre B_1, déterminé par l'équation de FERMAT

(1) $$A_1^2 - a B_1^2 = (-1)^{\varepsilon},$$

nous disons que d est diviseur régulier de a.

Les diviseurs réguliers jouent un rôle important, dans la théorie des équations de LAGRANGE, comme le montrent clairement les théorèmes que nous avons à démontrer concernant cette idée.

I. Supposons que le facteur régulier d de la base a contienne les facteurs premiers $p_1\ p_2 \ldots p_r$, le nombre

(2) $$K = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_r^{\lambda_r}$$

est précisément du rang K, par rapport à la base a.

A cet effet, étudions tout d'abord la puissance p^λ du diviseur régulier p, les formules de LAGRANGE

$$A_k = A_1^k + \binom{k}{2} a B_1^2 A_1^{k-2} + \dots$$

$$B_k = \binom{k}{1} B_1 A_1^{k-1} + \binom{k}{3} a B_1^3 A_1^{k-3} + \dots$$

donnent les congruences

(2) $$A_k \equiv A_1^k \pmod{p}$$

(3) $$B_k \equiv k B_1 A_1^{k-1} \pmod{p};$$

c'est-à-dire que B_p est le premier des nombres B_k qui soit divisible par p, de sorte que p est, par rapport à la base a, précisément du rang p.

De plus, on aura, en vertu du théorème de FERMAT,

(4) $$A_p \equiv A_1 \pmod{p}$$

(5) $$\frac{1}{p} B_p \equiv B_1 \pmod{p},$$

de sorte que le nombre premier p est aussi diviseur régulier de la base

(6) $$a_1 = ap^2.$$

Étudions ensuite l'équation de FERMAT

(7) $$x^2 - a_1 y^2 = (-1)^{\epsilon_1},$$

puis désignons par $(A_k^{(1)}, B_k^{(1)})$ une solution quelconque de cette équation, nous aurons

(8) $$A_k^{(1)} = A_{pk}, \quad B_k^{(1)} = \frac{1}{p} B_{pk},$$

ce qui donnera, en vertu des congruences (4) et (5),

(9) $$A_k^{(1)} \equiv A_1 \pmod{p}$$

(10) $$B_k^{(1)} \equiv B_1 \pmod{p}.$$

Cela posé, il est évident que le nombre premier p est,

par rapport à la base a_1, du rang p, de sorte que p^2 est du rang p^2, par rapport à la base a. Et la conclusion de $\lambda-1$ à λ est evidente, de sorte que la puissance p^λ est égale à son rang par rapport à la base a.

Posons généralement

$$a_\lambda = ap^\lambda, \tag{11}$$

puis désignons par $(A_k^{(\lambda)}, B_k^{(\lambda)})$ une solution quelconque de l'équation de Fermat

$$x^2 - a_\lambda y^2 = (-1)^{\varepsilon_\lambda}, \tag{12}$$

nous aurons, quel que soit l'indice λ,

$$A_k^{(\lambda)} \equiv A_k \pmod{p} \tag{13}$$

$$B_k^{(\lambda)} \equiv B_k \pmod{p}, \tag{14}$$

ce qui donnera particulièrement

$$A_1^{(\lambda)} \equiv A_{p^\lambda} \pmod{p} \tag{15}$$

$$B_1^{(\lambda)} \equiv \frac{1}{p^\lambda} B_{p^\lambda} \pmod{p}, \tag{16}$$

congruences qui nous seront très utiles dans ce qui suit.

Revenons maintenant au nombre K, défini par la formule (2), puis remarquons que chacun des facteurs

$$p_s^{\lambda_s}, \quad s = 1, 2, 3, \ldots, r,$$

premiers entre eux, est précisément égal à son rang par rapport à la base a, il est évident que le nombre K est du rang K par rapport à la base a.

De plus, l'égalité

$$\varepsilon_\lambda = \varepsilon p^\lambda$$

donnera immédiatement cette autre proposition:

II. Les deux bases a et aK^2 sont toujours de la même espèce, pourvu que K soit impair. Soit, au contraire, K un nombre pair, aK^2 est toujours une base de seconde espèce.

Supposons particulièrement que la base a et le nombre B_1 soient premiers entre eux, nous disons pour abréger que a est une base régulière, et l'application des théorèmes précédents aux bases régulières est évidente. C'est pourquoi nous nous bornerons à démontrer la proposition suivante:

III. Posons

$$B_1 = f\beta_1, \tag{17}$$

où β_1 est premier avec a, tandis que tous les facteurs premiers de f divisent aussi a, le nombre

$$a' = af^2 \tag{18}$$

est une base régulière.

En effet, remarquons que f divise tous les B_μ, puis posons

$$\alpha_\mu = A_\mu, \quad \beta_\mu = \frac{B_\mu}{f}, \tag{19}$$

nous aurons évidemment

$$a'\beta_\mu^2 = aB_\mu^2,$$

de sorte que toutes les solutions de l'équation de FERMAT

$$x^2 - a'y^2 = (-1)^{\varepsilon'} \tag{20}$$

se présentent sous la forme

$$x = \alpha_\mu, \quad y = \beta_\mu. \tag{21}$$

Dans l'article XVIII, nous avons à donner des applications importantes des bases régulières, applications qui exigent une étude plus approfondie des solutions d'une équation de LAGRANGE.

XVII. De l'ordre des positifs entiers.

Quant à l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^\vartheta \omega, \tag{1}$$

supposée résoluble, il est évident que les solutions de cette équation contiennent les solutions de celle-ci

$$u^2 - ap^2v^2 = (-1)^{\vartheta_1}\omega, \tag{2}$$

pourvu qu'elle soit résoluble, ce qui n'est pas toujours le cas, parce que $(-1)^{\vartheta_1}\omega$ doit être résidu quadratique de p.

Quoi qu'il en soit, supposons résolubles les deux équations (1) et (2), puis désignons par (u_q, v_q) le premier élément d'une suite S, appartenant à l'équation (1), dans lequel v_q est multiple de p, nous disons pour abréger que le nombre p appartient, dans la suite S, à l'indice q, et, cette définition adoqtée, nous avons tout d'abord à démontrer deux lemmes fondamentaux:

I. Supposons que le nombre p, du rang r par rapport à la base a, appartienne, dans une suite S de l'équation (1), à l'indice q, nous aurons toujours $q \leqq r$. De plus, soit S' la suite coordonnée de S, p appartient, dans S', à l'indice $r-q+1$.

En effet, supposons $q > r$, puis posons

$$q = rs + t, \quad 1 \leqq t \leqq r,$$

la formule récursive

$$v_q = u_t B_{rs} + v_t A_{rs}$$

montre que v_t est divisible par p, ce qui est impossible, de sorte que nous aurons nécessairement $q \leqq r$.

Soit ensuite $\omega > 2$, et soit (u'_μ, v'_μ) un élément quelconque de la suite S' coordonnée à S, on aura

$$u_q v'_{r-q+1} + v_q u'_{r-q+1} = \omega B_r,$$

de sorte que v'_{r-q+1} est nécessairement multiple de p, parce que p, étant diviseur de v_q, est premier avec u_q, et il est évident que v'_{r-q+1} est le premier des nombres v'_μ qui puisse être divisible par p.

Dans le cas particulier $\omega = 2$, nous disons que le nombre p est, par rapport à la suite S, de l'ordre q.

Supposons ensuite, pour $\omega > 2$, $q \leqq r-q+1$, nous

disons de même, que p est, dans le couple de suites coordonnées S et S', de l'ordre q.

Cela posé, il est facile de démontrer le second des deux lemmes susdits:

II. Supposons que le positif entier p du rang r appartienne, dans la suite S, à l'indice q, tous les nombres v_{q+rs} sont multiples de p, tandis qu'aucun autre des v_μ ne peut posséder cette propriété.

En premier lieu, il résulte immédiatement de la formule récursive

$$v_{q+rs} = v_q A_{rs} + u_q B_{rs}$$

que v_{q+rs} est multiple de p. Soit ensuite v_m, pour $m > q$, divisible par p, on aura

$$v_m = v_q A_{m-q} + u_q B_{m-q},$$

de sorte que B_{m-q} est multiple de p, ce qui donnera

$$m - q = rs, \quad m = q + rs.$$

Or, ces deux lemmes établis, il est facile de démontrer le théorème général:

III. Supposons que le positif entier p du rang r soit, dans les deux suites coordonnées S et S', de l'ordre q, les éléments

$$(3) \qquad \left(u_{q+rs}, \frac{1}{p} v_{q+rs}\right), \quad \left(u'_{r-q+rs+1}, \frac{1}{p} v'_{r-q+rs+1}\right)$$

forment un couple de suites coordonnées appartenant à l'équation (2).

Quant aux exposants δ et δ_1 qui figurent dans les équations (1) et (2), on aura

$$(4) \qquad \delta_1 = \delta + r\varepsilon,$$

où ε est déterminé par l'équation de FERMAT

$$(5) \qquad A_1^2 - aB_1^2 = (-1)^\varepsilon.$$

Soit par exemple $r = 2$, on aura $q = 1$ ou $q = 2$; c'est-à-dire que le nombre p du rang 2 ne peut appartenir à

un couple de suites coordonnées S et S', à moins que v_1 et v_2' ou v_2 et v_1' ne soient multiples de p.

Généralement on peut dire que les idées du rang et de l'ordre des positifs entiers jouent un rôle fondamental dans la théorie des équations de LAGRANGE, ce qui est mis en pleine lumière par la proposition suivante:

IV. Supposons que les rangs r_1 et r_2 des nombres p_1 et p_2, appartenant tous deux à l'équation (1), soient premiers entre eux, le produit p_1p_2 appartient aussi à cette même équation.

En effet, supposons que les nombres p_1 et p_2 appartiennent, dans une suite des solutions de l'équation (1), aux indices s_1 et s_2, les indices μ et ν des v_k qui sont multiples de p, respectivement de p_2, se présentent sous la forme

$$\mu = s_1 + r_1 \varkappa, \quad \nu = s_2 + r_2 \lambda, \tag{6}$$

donc le produit p_1p_2 ne peut appartenir à la suite susdite, à moins que

$$\mu = \nu, \tag{7}$$

condition qui est à la fois nécessaire et suffisante.

Or, l'équation (7) n'est autre chose que l'équation indéterminée

$$r_1 \varkappa - r_2 \lambda = s_1 - s_2, \tag{8}$$

toujours résoluble, parce que r_1 et r_2 sont premiers entre eux.

Soit par exemple

$$\varkappa = \varrho + r_2 \mu,$$

on aura, en vertu de (8),

$$\mu = \nu = s_1 + r_1 \varrho + k r_1 r_2, \quad 0 < s_1 + r_1 \varrho \leqq r_1 r_2,$$

où k est un positif entier quelconque.

Supposons, au contraire, que les rangs r_1 et r_2 aient le plus grand diviseur commun f, l'équation (8) n'est pas

résoluble, à moins que

$$s_1 - s_2 \equiv 0 \pmod{f}, \tag{9}$$

condition que permet de résoudre, aussi dans ce cas, l'équation (8),

Quant à la suite coordonnée S', p_1 et p_2 appartiennent respectivement aux indices

$$s'_1 = r_1 - s_1 + 1, \quad s'_2 = r_2 - s_2 + 1,$$

ce qui donnera

$$s'_1 - s'_2 \equiv 0 \pmod{f}.$$

Soit par exemple

$$a = 2, \quad p_1 = 2, \quad p_2 = 3,$$

on aura

$$r_1 = 2, \quad r_2 = 4,$$

de sorte que le diviseur 6 n'appartient à un couple de suites coordonnées de l'équation

$$u^2 - 2v^2 = \pm\omega,$$

à moins que les ordres s_1 et s_2 des premiers 2 et 3 ne soient de la même parité.

Revenons maintenant à l'équation de FERMAT

$$A_n^2 - aB_n^2 = (-1)^{n\varepsilon},$$

nous savons que les deux nombres A_k et B_{2n+1} sont toujours premiers entre eux, quels que soient leurs indices k et $2n+1$.

Quant à l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^{\vartheta}\omega, \tag{10}$$

nous trouvons une propriété analogue, savoir:

V. Un nombre du rang impair, par rapport à la basè a, qui appartient à une suite (u_n, v_n) des solutions de l'équation (10) est premier avec tous les nombres u_n.

En effet, supposons que u_μ ne soit pas premier avec

le nombre p du rang impair qui appartient à la suite (u_n, v_n), il existe un indice plus grand que μ, savoir $\mu+\nu$, tel que $v_{\mu+\nu}$ est multiple de p, et nous aurons

$$v_{\mu+\nu} = u_\mu B_\nu + v_\mu A_\nu ,$$

de sorte que p et A_ν ne sont pas premiers entre eux, ce qui est impossible.

XVIII. Propriété remarquable des bases régulières.

Les développements de l'article précédent montrent clairement qu'il existe une grande analogie entre les équations de FERMAT et de LAGRANGE. Néanmoins ces deux classes d'équations indéterminées présentent des propriétés entièrement différentes, ce qui est mis en pleine lumière par les recherches suivantes.

Supposons que le nombre p soit, par rapport à la base a, du rang r, de sorte que

$$B_r = p^\varkappa K , \tag{1}$$

où K n'est pas divisible par p, nous disons pour abréger que le nombre p est, par rapport à la base a, du rang r et de la hauteur $\varkappa$.

Soit maintenant ϱ un positif entier quelconque, il existe, en vertu des développements de l'article XV, des indices s, tels que

$$B_s = p^{\varkappa+\varrho} K_1 , \tag{2}$$

où K_1 n'est pas divisible par p.

Quant à l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^\vartheta \omega , \tag{3}$$

l'étude des diviseurs des nombres v_μ est plus compliquée.

En effet, supposons que le nombre p appartienne, dans une suite S, à l'indice m, de sorte que

$$v_m = p^\lambda M , \tag{4}$$

où M n'est pas divisible par p, nous aurons à démontrer la proposition curieuse:

I. Soit, dans les équations (1) et (4), $\lambda < \varkappa$, tous les v_μ qui sont multiples de p, sont divisibles précisément par p^λ, de sorte qu'il n'existe aucun v_μ qui soit divisible par une autre puissance de p.

Supposons

$$v_m = p^\lambda M, \quad B_{rk} = p^\varkappa L,$$

le nombre M n'est pas divisible par p, et nous aurons, en vertu des formules récursives,

$$v_{m+rk} = p^\lambda (MA_{rk} + u_m p^{\varkappa-\lambda} L),$$

ce qui montre clairement que v_{m+rk} est, quel que soit k, divisible précisément par la puissance p^λ, parce que M et A_{rk} sont tous deux premiers avec p.

Quant à l'hypothèse $\lambda \geqq \varkappa$, démontrons tout d'abord le lemme suivant:

II. Soit p un diviseur premier régulier de la base a, les deux équations de LAGRANGE

$$u^2 - av^2 = (-1)^\delta \omega, \quad u^2 - ap^2 v^2 = (-1)^\varepsilon \omega \tag{5}$$

sont, pour des exposants convenables δ et ε, en même temps résolubles ou non, et, en cas de résolubilité, ces deux équations sont du même genre.

Quant à la démonstration de ce lemme fondamental, il s'agit évidemment de démontrer que le diviseur p appartient à un couple quelconque de suites coordonnées de la premières des équations (5).

A cet effet, soit (u_1, v_1) le premier élément d'une suite quelconque appartenant à l'équation susdite, la formule récursive générale

$$v_{k+1} = v_1 A_k + u_1 B_k$$

donnera, en vertu des congruences (2) et (3) de l'article XVI,

$$v_{k+1} \equiv A_1^{k-1} (A_1 v_1 + k u_1 B_1), \quad 1 \leqq k \leqq p-1, \tag{6}$$

et il est évident que les deux congruences

$$v_{k+1} \equiv 0 \pmod{p} \tag{7}$$

$$v_1 A_1 + k u_1 B_1 \equiv 0 \pmod{p} \tag{8}$$

sont équivalentes.

Cela posé, introduisons, dans (8), successivement

$$u_1 = 1, 2, 3, \ldots, p-1, \tag{9}$$

puis supposons les congruences ainsi obtenues satisfaites respectivement par

$$v_1 = \alpha_1^{(k)}, \alpha_2^{(k)}, \ldots, \alpha_{p-1}^{(k)}, \tag{9}$$

il est évident que la différence

$$\alpha_\mu^{(k)} - \alpha_\nu^{(k)}, \quad \mu \neq \nu,$$

ne peut jamais être divisible par p; car on aura, dans ce cas,

$$u_1 B_1 (\mu - \nu) \equiv 0 \pmod{p},$$

ce qui est impossible, parce que $u_1 B_1$ est premier avec p, et $|\mu - \nu| < p$.

Divisons maintenant par p les nombres $\alpha_r^{(k)}$, nous aurons les restes

$$1, 2, 3, \ldots, p-1,$$

pris dans un ordre inconnu; c'est-à-dire que la congruence (8) est satisfaite par les $p-1$ couples des valeurs différentes de u_1 et v_1:

$$(1, \alpha_1^{(k)}), (2, \alpha_2^{(k)}), \ldots, (p-1, \alpha_{p-1}^{(k)}). \tag{10}$$

Démontrons ensuite que les deux congruences

$$v A_1 + k_1 u B_1 \equiv 0 \pmod{p}$$

$$v A_1 + k_2 u B_1 \equiv 0 \pmod{p},$$

où $k_1 \neq k_2$, ne sont jamais satisfaites par le même couple (u, v).

On aura, en effet, dans ce cas,

$$(k_1 - k_2) u B_1 \equiv 0 \pmod{p},$$

ce qui est impossible.

Cela posé, introduisons, dans (10), successivement

$$k = 1, 2, 3, \ldots, p-1,$$

nous aurons tous les $(p-1)^2$ couples de la forme

$$(\alpha, \beta), \quad 1 \leqq \alpha \leqq p-1, \quad 1 \leqq \beta \leqq p-1,$$

et il est évident qu'il existe de telles valeurs α et β que

$$u_1 \equiv \alpha \pmod{p}, \quad v_1 \equiv \beta \pmod{p};$$

c'est-à-dire qu'un seul des nombres

$$v_1, v_2, v_3, \ldots, v_p$$

est toujours divisible par p, de sorte que le diviseur p appartient à une suite quelconque formée des solutions de l'équation (5).

Appliquons ensuite la méthode développée dans l'article XVI, nous verrons que les deux équations

$$u^2 - av^2 = (-1)^{\delta}\omega, \quad u^2 - ap^{2\lambda}v^2 = (-1)^{\varepsilon}\omega$$

sont en même temps résolubles ou non, et, en cas de résolubilité, elles sont du même genre.

Étudions maintenant la base régulière

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \tag{11}$$

où $p_1 p_2 \ldots p_r$ sont des facteurs premiers inégaux, puis posons

$$K = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}, \tag{12}$$

la méthode appliquée dans l'article XVI, donnera ici le théorème fondamental:

III. Soit a une base régulière, les deux équations indéterminées

$$u^2 - av^2 = (-1)^{\delta_1}\omega, \quad u^2 - aK^2v^2 = (-1)^{\delta_2}\omega, \tag{11}$$

sont, pour des valeurs convenables des exposants δ_1 et δ_2, en même temps résolubles ou non, et, en

cas de résolubilité, les deux équations sont du même genre.

Exemple I. Le nombre $a = 10$ est une base régulière de première espèce, car l'équation de FERMAT

$$x^2 - 10y^2 = \pm 1$$

donnera

$$A_1 = 3\,, \quad B_1 = 1\,,$$

de sorte que l'on aura

$$A_2 = 19\,, \quad B_2 = 6\,; \quad A_3 = 117\,, \quad B_3 = 37.$$

Supposons ensuite résoluble l'équation de LAGRANGE

$$u^2 - 10v^2 = \pm\omega\,, \tag{12}$$

cette autre équation

$$u^2 - 2^{2n+1}5^{2p+1}v^2 = (-1)^\delta\omega \tag{13}$$

est aussi résoluble, quels que soient les exposants n et p, et les équations (12) et (13) sont du même genre.

Étudions un peu plus profondément l'équation spéciale da la forme (13)

$$u^2 - 1000v^2 = (-1)^\delta\omega\,, \tag{14}$$

puis désignons par (u_1, v_1) le premier élément d'une suite quelqonque des solutions de l'équation (12), nous pouvons nous borner à étudier le cas où u_1 et v_1 sont tous deux impairs et non multiples par 5. En effet, soit v_1 divisible par 10, nous aurons immédiatement une solution de (14); soit ensuite u_1 multiple de 5, ou soit v_1 un nombre pair, les deux nombres

$$3v_1 \pm u_1$$

sont premiers avec 10.

Or, supposons u_1 et v_1 tous deux premiers avec 10, je dis que nous aurons toujours une des quatre congruences

$$3v_1 \pm u_1 \equiv 0 \pmod{10} \tag{15}$$

$$117v_1 \pm 37u_1 \equiv 0 \pmod{10}. \tag{16}$$

En effet, supposons

$$u_1 \equiv \alpha \pmod 5, \quad v_1 \equiv \beta \pmod 5,$$

ce que nous désignons par le symbole (α, β), une des congruences (15) est satisfaite pour les 8 combinaisons

$$(1, 2),\ (2, 1),\ (1, 3),\ (3, 1),\ (2, 4),\ (4, 2),\ (3, 4),\ (4, 3),$$

tandis que qu'une des congruences (16), ou, ce qui est la même chose,

$$v_1 \pm u_1 \equiv 0 \pmod{10}$$

est satisfaite pour une des 8 combinaisons

$$(1, 1),\ (2, 2),\ (3, 3),\ (4, 4),\ (1, 4),\ (4, 1),\ (2, 3),\ (3, 2).$$

Considérons par exemple l'équation

$$u^2 - 10v^2 = \pm 39,$$

ses deux couples de suites coordonnées sont déterminés par les solutions

$$1^2 - 10 \cdot 2^2 = -39, \quad 17^2 - 10 \cdot 5^2 = 39$$

ce qui donnera, pour l'équation

$$u^2 - 1000v^2 = -39,$$

deux couples de suites coordonnées, déterminées par les solutions

$$31^2 - 1000 \cdot 1^2 = 5191^2 - 1000 \cdot 167^2 = -39.$$

Le premier de ces deux couples provient des réduites de la fraction continue qui représente $\sqrt{1000}$.

Revenons maintenant aux équations (1) et (4), dans lesquelles $\lambda \geq z$, puis posons, dans l'équation (3),

$$a_1 = ap^{2z}, \tag{17}$$

p est un diviseur régulier de la base a_1, de sorte que p appartient à une suite quelconque des solutions de l'équation

$$u^2 - a_1 v^2 = (-1)^\varepsilon \omega. \tag{18}$$

Exemple II. Soit $a = 7$, on aura $A_1 = 8$, $B_1 = 3$, de sorte que le nombre premier 2 est du rang 2 et de la hauteur 4.

L'equation de Lagrange

$$u^2-7v^2=57$$

est du rang 4, en ayant les solutions primitives

$$8^2-7\cdot 1^2=13^2-7\cdot 4^2=57,$$

de sorte que nous aurons

$$13^2-28\cdot 2^2=45^2-28\cdot 8^2=57,$$

donc l'équation

$$u^2-28v^2=57$$

est aussi du genre 4, et c'est la même chose pour

$$u^2-112v^2=57,$$

tandis que les équations

$$u^2-7\cdot 2^{2n}v^2=57,\quad n\geqq 3,$$

toujours résolubles, ne sont que du genre 2.

Exemple III. Le nombre 2 est, par rapport à la base 14, du rang 1, parce que l'on aura $A_1=15$, $B_1=4$; l'équation

$$u^2-14v^2=-55$$

est du genre 4, car on aura

$$1^2-14\cdot 2^2=29^2-14\cdot 8^2=-55,$$

c'est-à-dire que l'équation

$$u^2-56v^2=-55$$

est aussi du genre 4, tandis que

$$u^2-224v^2=-55,\quad u^2-14\cdot 2^{2n}v^2=-55,\quad n\geqq 2$$

ne sont que du genre 2.

L'équation

$$u^2-14v^2=275$$

est du genre 4, car

$$17^2-14\cdot 1^2=31^2-14\cdot 7^2=275,$$

tandis que les équations

$$u^2-14\cdot 2^{2n}v^2=275,\quad n\geqq 1,$$

sont irrésolubles.

Exemple IV. Soit $a = 41$, on aura $A_1 = 32$, $B_1 = 5$, de sorte que le nombre premier 5 est, par rapport à la base 41, du rang 1.

L'équation de LAGRANGE

$$u^2 - 41v^2 = \pm 664$$

est du genre 4, et ses deux couples de suites coordonnées sont déterminés par les solutions

$$19^2 - 41 \cdot 5^2 = -664, \quad 75^2 - 41 \cdot 11^2 = 664,$$

donc l'équation

$$u^2 - 1025\, v^2 = \pm 664$$

n'est que du genre 2.

Ces exemples, pris au hasard dans ma Table des solutions des équations de LAGRANGE, sont typiques pour la nature de ces équations.

XIX. Des diviseurs 2, 3, 5.

La seconde partie de la Table de DEGEN qui contient les solutions A_1 et B_1 de l'équation de FERMAT

$$A_1^2 - aB_1^2 = -1 \tag{1}$$

est d'un aspect curieux, parce que beaucoup des nombres B_1 ou A_1 sont multiples de 5.

Or, ce fait curieux est une conséquence immédiate des deux propositions suivantes concernant le diviseur 5:

I. Soit a une base de première espèce de la forme $4k \pm 1$, le nombre premier 5 est, par rapport à la base a, du rang 1 ou du rang 2.

Remarquons que, dans l'équation (1), la congruence

$$A_1^2 \equiv 1 \pmod 5$$

est exclue, parce qu'elle donnera

$$aB_1^2 \equiv 2 \pmod 5,$$

ce qui est impossible. On aura donc ou

$$A_1^2 \equiv -1 \pmod 5$$

ce qui donnera

$$B_1 \equiv 0 \pmod 5,$$

de sorte que 5 est du rang 1, ou

$$A_1^2 \equiv 0 \pmod 5$$

ce qui donnera le rang de 5 égal à 2.

On voit que, dans ce cas, un des nombres B_1 et A_1 est toujours multiple de 5.

II. Soit a une base de première espèce de la forme $5k \pm 2$, le nombre premier 5 est, par rapport à la base a, du rang 1 ou du rang 3.

Dans ce cas, il est évident que A_1 ne peut jamais être multiple de 5, de sorte que l'on aura ou

$$A_1^2 \equiv -1 \pmod 5,$$

ce qui donnera

$$B_1 \equiv 0 \pmod 5,$$

et 5 est du rang 1, ou

$$A_1^2 \equiv 1 \pmod 5,$$

et la formule

$$B_3 = B_1(4A_1^2 + 1)$$

donnera immédiatement

$$B_3 \equiv 0 \pmod 5,$$

de sorte que 5 est du rang 3.

Remarquons que la proposition II donnera, comme corollaire, cette autre:

III. Soit $a = 5k \pm 2$ une base de première espèce, les nombres $5^{2n}a$ sont aussi, quel que soit l'exposant n, des bases de première espèce.

Soit maintenant $a = 5k \pm 1$ un base de seconde espèce, savoir

$$A_1^2 - B_1^2 = 1,$$

la congruence

(1) $$A_1^2 \equiv -1 \pmod 5$$

est toujours exclue, de sorte que l'on aura ou

$$A_1^2 \equiv 1 \pmod 5, \tag{2}$$

ce qui donnera

$$B_1 \equiv 0 \pmod 5$$

et 5 est du rang 1, ou

$$A_1 \equiv 0 \pmod 5, \tag{3}$$

donc 5 est du rang 2.

Dans ce cas, un des nombres A_1 et B_1 est toujours multiple de 5.

Soit ensuite $a = 5k \pm 2$ une base de seconde espèce, on aura aussi à considérer la congruence (1), de sorte que le rang du nombre 5 est égal à 1, 2 ou 3.

Quant au diviseur 3, nous avons à démontrer la proposition:

IV. Soit

$$a = 3k + l, \quad l = 1, 2 \tag{4}$$

une base de première espèce, le nombre premier 3 est, par rapport à la base a, du rang $2l$.

En effet, l'équation de FERMAT donnera

$$A_1^2 = aB_1^2 - 1$$
$$A_2^2 = aB_2^2 + 1;$$

soit donc $a = 3k+1$, on aura

$$A_1 \equiv 0 \pmod 3$$

et 3 est du rang 2, tandis que l'hypothèse $a = 3k+2$ donne

$$A_2 \equiv 0 \pmod 3,$$

donc 3 est du rang 4, parce que

$$B_2 = 2A_1B_1$$

ne peut jamais être multiple de 3.

Quant au diviseur 3, nous avons encore à démontrer la proposition:

V. Soit $a = 3k+2$ une base de première espèce, les deux équations de LAGRANGE

(5) $$u^2 - av^2 = \pm\omega, \quad u^2 - 9av^2 = (-1)^\delta\omega$$

sont, pour une valeur convenable de l'exposant δ, en même temps résolubles ou non, et, en cas de résolubilité, elles sont du même genre.

En effet, soit (u_n, v_n) l'élément général d'une suite S appartenant à la première des équations (5), et soit v_1 multiple de 3, il est évident que le diviseur 3 appartient à la suite S. Soit ensuite u_1 multiple de 3, on aura

$$v_3 = A_2 v_1 + B_2 u_1 \equiv 0 \pmod 3,$$

car A_2 est multiple de 3.

Étudions maintenant le cas général où ni u_1 ni v_1 n'est multiple de 3, un des deux nombres

$$v_2 = v_1 A_1 + u_1 B_1$$
$$v_1' = |v_1 A_1 - u_1 B_1|$$

aura nécessairement cette propriété, et (u_1', v_1') est la solution réciproque de (u_1, v_1); c'est-à-dire que v_4 est divisible par 3.

Remarquons que les propositions II et IV donnent immédiatement cette autre:

VI. Le nombre 15 est, par rapport aux bases de première espèce de la forme $15\nu+2$ ou $15\nu+8$, du rang 12.

Quant au diviseur 2, nous avons à demontrer les deux propositions:

VII. Soit a une base paire de première espèce, la puissance 2^ν est, quel que soit l'exposant ν, égal à son rang par rapport à la base a.

Remarquons qu'une base paire de première espèce est toujours un nombre de la forme $4k+2$, il est évident que

A_1 et B_1 sont tout deux impairs, de sorte que B_2 est aussi de la forme $4l+2$; c'est-à-dire que 2 est un diviseur régulier de la base a. De plus, on aura cette autre proposition:

VIII. Soit a une base paire de première espèce, les deux équations de LAGRANGE

$$u^2 - av^2 = \pm\omega, \quad u^2 - 2^{2r}av^2 = (-1)^{\delta}\omega$$

sont, pour une valeur convenable de l'exposant δ, en même temps résolubles ou non, et, en cas de résolubilité, elles sont du même genre.

On voit que cette dernière proposition se présente sous une forme élégante, dans le cas spécial $a = 2$.

CHAPITRE V

Des conditions de résolubilité.

XX. Remarques générales sur la résolubilité.

Revenons maintenant à la proposition I de l'article I concernant la résolubilité d'une équation de LAGRANGE

$$u^2 - av^2 = (-1)^\delta \omega , \tag{1}$$

puis posons

$$u = as \pm r , \tag{2}$$

il résulte, en vertu de (1),

$$(-1)^\delta \omega \equiv r^2 \pmod{a}, \tag{3}$$

congruence qui détermine r, et l'équation (1) donnera

$$(as \pm r)^2 - (-1)^\delta \omega = av^2, \tag{4}$$

équation qui permet souvent de résoudre immédiatement l'équation (1), à l'aide d'une table des nombres carrés plus petits que 100.

Posons ensuite, conformément à la congruence (3),

$$(-1)^\delta \omega = r^2 \pm ka , \tag{5}$$

il résulte, en vertu de (4),

$$as^2 \pm 2rs \mp k = v^2, \tag{6}$$

équation qui est souvent plus facile à résoudre que (4).

De plus, cette dernière équation (6) indique immédiatement beaucoup des cas dans lesquels l'équation (1) est irrésoluble; un de ces cas est indiqué par la proposition suivante:

I. L'équation (1) est irrésoluble, pourvu que l'on ait à la fois

(7) $$a = 4\lambda + 2, \quad k = 4\mu + 2, \quad r = 2\nu + 1.$$

En effet, il résulte, en vertu de (6), que v doit être un nombre pair; soit $v = 2\nu_1$, on aura donc

$$(2\lambda+1)s^2 \pm (2\nu+1)s \mp (2\mu+1) = 2\nu_1^2,$$

équation qui est impossible, parce que son premier membre est un nombre impair.

On aura de même ces deux autres propositions:

II. Soit $a = 8\nu + 1$ la puissance d'un nombre premier, l'équation de LAGRANGE

(8) $$u^2 - 2av^2 = \omega^2$$

est irrésoluble pour $\omega = 8\mu \pm 3$.

En effet, l'équation (8) donnera ou

$$u \pm \omega = 2p^2, \quad u \mp \omega = 4aq^2$$

ou

$$u \pm \omega = 4q^2, \quad u \mp \omega = 2ap^2$$

où nous avons posé

$$v = 2pq,$$

de sorte que p est impair, ce qui donnera respectivement

(9) $$p^2 - 2aq^2 = \pm\omega, \quad 2q^2 - ap^2 = \pm\omega,$$

donc on aura nécessairement $\omega = 8\mu \pm 1$.

III. Soit $a = 8\nu + 1$ la puissance d'un nombre premier, et soit ω^2 la puissance primitive qui correspond à la base $2a$, l'équation de LAGRANGE (8) n'est résoluble, à moins que

(10) $$a \pm \omega = 2z \pmod 8, \quad z = 0, 1.$$

Dans ce cas, nous avons seulement la seconde des congruences (9), et la congruence (10) est évidente.

Or, il est très curieux, ce me semble, que la proposition suivante admette beaucoup plus d'applications que les précédentes:

IV. Supposons résoluble l'équation de LAGRANGE

$$u^2 - av^2 = (-1)^\delta p^\varrho q^\sigma, \tag{11}$$

où p et q sont des nombres premiers inégaux, ces deux autres équations

$$u^2 - av^2 = (-1)^\varkappa p^\varrho, \quad u^2 - av^2 = (-1)^\lambda q^\sigma, \quad \varkappa + \lambda = \delta, \tag{12}$$

sont en même temps résolubles ou non.

En effet, supposons résoluble une des équations (12), l'équation (11) est décomposable, de sorte que la seconde des équations (12) est aussi résoluble.

Exemple I. Soit $a = 37$, $q^\varrho = 3$, j'ai annoté plus de 50 valeurs de q^σ, pour lesquelles l'équation (11) est résoluble, l'équation (12) irrésoluble, parce que

$$u^2 - 37v^2 = \pm 3$$

est irrésoluble.

Exemple II. Soit $a = 101$, $p^\varrho = 4$, je connais plus de 40 valeurs de q^σ, pour lesquelles l'équation (11) est résoluble, tandis que les équations (12) sont toutes deux irrésolubles, parce que

$$u^2 - 101v^2 = \pm 4$$

est irrésoluble.

XXI. Théorème sur les bases 2, 3, 5.

Dans ce qui suit, nous désignons par a un quelconque des trois nombres premiers

$$2, 3, 5,$$

par ω un nombre impair, premier avec a, et nous avons à démontrer le théorème:

I. L'équation de LAGRANGE

$$u^2 - av^2 = (-1)^\delta \omega \tag{1}$$

est toujours résoluble, pourvu que a soit résidu quadratique de chacun des facteurs premiers de ω,

et que $(-1)^{\delta}\omega$ soit résidu quadratique de a, condition qui est à la fois nécessaire et suffisante.

Ce théorème est bien connu, au moins pour $a = 2, 3$, parce que l'on connaît une solution de l'équation (1) correspondante, mais je ne me rappelle pas avoir vu autrefois l'équation (1) qui correspond à $a = 5$.

C'est pourquoi il nous semble utile de démontrer de nouveau notre théorème, en appliquant une méthode analogue à celle des démonstrations de l'expression

$$p = x^2 + ay^2, \quad a = 1, 2, 3, 4,$$

où p est un nombre premier.

A cet effet, supposons tout d'abord que ω soit égal à un nombre premier p, de sorte que les deux conditions susdites soient remplies, il existe un positif entier $q < p$ qui satisfait à la congruence

$$q^2 \equiv a \pmod{p}.$$

De plus, il est possible de déterminer deux nombres entiers x et y qui satisfont à la congruence

$$x^2 - q^2y^2 = (x+qy)(x-qy) \equiv 0 \pmod{p},$$

car p et q sont premiers entre eux.

Cela posé, nous aurons évidemment

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

où M est un nombre entier. De plus, choisissons x et y, tels que

$$|x| < \frac{p}{2}, \quad |y| < \frac{p}{2},$$

ce qui est permis, nous aurons, en vertu de (2),

$$|M| < p,$$

car $a - 1 \leqq 4$.

Soit maintenant $M = \pm 1$, l'équation (2) n'est autre chose que l'équation (1) pour $\omega = p$; soit, au contraire

$|M| > 1$, nous aurons, en vertu de (2),

$$(3) \qquad (x-\alpha M)^2 - a(y-\beta M)^2 = MM_1,$$

où α et β sont des positifs entiers quelconques, et où M_1 est un nombre entier, et il est facile de démontrer que l'hypothèse $M_1 = 0$ est inadmissible.

En effet, soit $M_1 = 0$, on aura, en vertu de (3),

$$x = \alpha M, \quad y = \beta M,$$

donc il résulte,

$$(\alpha^2 - a\beta^2) M = p,$$

de sorte que l'on aura nécessairement un des systèmes d'équations indéterminées

$$\alpha^2 - a\beta^2 = \pm 1, \quad M = \pm p$$
$$\alpha^2 - a\beta^2 = \pm p, \quad M = \pm 1,$$

ce qui est impossible, parce que $1 < |M| < p$.

Choisissons maintenant α et β, de sorte que

$$|x - \alpha M| \leqq \tfrac{1}{2}|M|, \quad |y - \beta M| \leqq \tfrac{1}{2}|M|,$$

ce qui est possible, l'équation (3) donnera immédiatement

$$(4) \qquad |M_1| < |M|,$$

à moins que

$$a = 5, \quad x - \alpha M = \pm \tfrac{1}{2} M, \quad y - \beta M = \pm \tfrac{1}{2} M,$$

savoir

$$a = 5, \quad x = (\alpha \pm \tfrac{1}{2}) M, \quad y = (\beta \pm \tfrac{1}{2}) M.$$

Or, introduisons, dans (2), ces trois valeurs, il résulte

$$\left[(\alpha \pm \tfrac{1}{2})^2 - 5(\beta \pm \tfrac{1}{2})^2\right] M^2 = p.$$

ce qui est impossible, parce que $1 < |M| < p$.

Cela posé, on aura, en multipliant les équations (2) et (3),

$$\left[x(x-\alpha M) - ay(y-\beta M)\right]^2 - a\left[x(y-\beta M) - y(x-\alpha M)\right]^2 = \\ = pM^2 M_1,$$

ou, ce qui est la même chose,

$$(\alpha x - a\beta y)^2 - a(\beta x - \alpha y)^2 = pM_1,$$

équation qui est de la même forme que (2), mais $|M_1| < |M|$.

En continuant de cette manière, on trouvera finalement une équation de la forme

$$x^2 - ay^2 = (-1)^{\delta} p, \tag{5}$$

savoir l'équation (1) pour $\omega = p$.

Remarquons maintenant que p est un nombre impair, il résulte, en vertu du théorème II de l'article XIII, que cette autre équation indéterminée

$$x^2 - ay^2 = (-1)^{n\delta} p^n, \tag{6}$$

où n désigne un positif entier quelconque, est aussi résoluble.

Enfin, supposons résolubles les ν équations de la forme (6)

$$x^2 - ay^2 = (-1)^{\delta r} p_r^{nr}, \quad r = 1, 2, \ldots, \nu,$$

où les p_r sont des nombres premiers inégaux, nous savons, en vertu du théorème I de l'article VI, que l'équation indéterminée

$$x^2 - ay^2 = (-1)^{\delta_1 + \delta_2 \ldots + \delta_\nu} p_1^{n_1} p_2^{n_2} \ldots p_\nu^{n\nu} \tag{7}$$

est aussi résoluble, et cette dernière équation est précisément l'équation proposée (1).

En se rappellant que l'équation indéterminée

$$x^2 - y^2 = \omega,$$

supposée résoluble, savoir que ω n'est pas de la forme $4\lambda + 2$, n'admet qu'un nombre fini de solutions, il est bien curieux, ce me semble, que cette autre équation

$$x^2 - ay^2 = (-1)^{\delta} \omega, \quad a = 2, 3, 5,$$

supposée résoluble, n'admette pas seulement une infinité des solutions, mais, abstraction faite du cas particulier $a = 3$, $\omega = 2$, au moins deux suites infinies de solutions.

Or, notre théorème général démontré, nous avons à étudier séparément les trois valeurs susdites de la base a.

XXII. Sur la base $a = 2$.

Soit tout d'abord $a = 2$, le théorème I de l'article précédent donnera immédiatement, comme corollaire:

I. L'équation de LAGRANGE

$$u^2 - 2v^2 = \pm\omega \tag{1}$$

est toujours résoluble, pourvu que tous les facteurs premiers de ω soient de la forme $8\nu \pm 1$, et seulement dans ce cas.

Quant à l'équation (1), on aura la proposition curieuse:

II. Soit (u_1, v_1) l'élément primitif d'un couple quelconque de suites coordonnées appartenant à l'équation (1), on aura toujours, quel que soit le paramètre ω,

$$u_1 < v_1, \tag{2}$$

et inversement.

En effet, remarquons que la plus petite solution (A_1, B_1) de l'équation de FERMAT

$$x^2 - 2y^2 \pm 1$$

est déterminée par $A_1 = B_1 = 1$, la multiplication négative donnera, en vertu de (1),

$$(u-2v)^2 - 2(u-v)^2 = \mp\omega. \tag{3}$$

Soit maintenant $u > 2v$, on aura

$$u - 2v < u, \quad u - v > v;$$

c'est-à-dire que l'indice de la solution $(u-2v, u-v)$ est plus petit que celui de (u, v).

Soit ensuite $v < u < 2v$, on aura de même

$$2v - u < u, \quad u - v < v,$$

de sorte que l'indice de la solution $(2v-u, u-v)$ est plus petit que celui de (u, v), tandis que l'hypothèse $u < v$ donnera

$$2v - u > u, \quad v - u < v;$$

c'est-à-dire que l'indice de la solution $(2v-u,\ v-u)$ est plus grand que celui de (u, v).

De plus, nous aurons à démontrer la proposition:

III. Soit (u_1, v_1) l'élément primitif d'un couple de suites coordonnées appartenant à l'équation (1), on aura toujours

$$\sqrt{\frac{\omega+1}{2}} \geqq v_1 > \sqrt{\frac{\omega}{2}}. \tag{4}$$

En effet, il résulte, en vertu de (2),

$$u_1^2 - 2v_1^2 = -\omega,$$

ce qui donnera immédiatement les relations (4).

Étudions par exemple l'équation indéterminée

$$u^2 - 2v^2 = \pm 4991 = \pm 7 \cdot 23 \cdot 31, \tag{5}$$

nous prenons pour point de départ les deux équations

$$u^2 - 2v^2 = \pm 7, \quad u^2 - 2v^2 = \pm 23,$$

dont les solutions primitives sont déterminés par les égalités

$$1^2 - 2\cdot 2^2 = -7, \quad 3^2 - 2\cdot 4^2 = -23,$$

d'où il résulte, en multipliant ces deux équations,

$$19^2 - 2\cdot 10^2 = 161, \quad 13^2 - 2\cdot 2^2 = 161;$$

donc les éléments primitifs des deux couples de suites coordonnées de l'équation

$$u^2 - 2v^2 = \pm -161$$

sont déterminés par les égalités

$$1^2 - 2\cdot 9^2 = -161, \quad 9^2 - 2\cdot 11^2 = -161, \tag{6}$$

tandis que les solutions réciproques sont déterminées par

$$17^2 - 2\cdot 8^2 = 161, \quad 13^2 - 2\cdot 2^2 = 161.$$

Remarquons ensuite que l'équation indéterminée

$$u^2 - 2v^2 = \pm 31$$

a sa solution primitive déterminée par

$$1^2-2\cdot 4^2=-31,$$

il résulte, en vertu de (6), que les quatre éléments primitifs des huit suites coordonnées de l'équation (5) sont déterminés par les égalités

$$3^2-2\cdot 50^2=29^2-2\cdot 54^2=47^2-2\cdot 60^2=61^2-2\cdot 66^2=-4991.$$

XXIII. Sur la base 3.

Remarquons que 3 est résidu quadratique des nombres premiers de la forme $12k\pm 1$, tandis que $12k+1$ est résidu, $12k-1$ non résidu de 3, nous aurons, en vertu du théorème I de l'article XXI:

I. L'équation de LAGRANGE

$$u^2-3v^2=(-1)^{\delta}\omega,\quad \omega=12\nu+(-1)^{\delta}, \tag{1}$$

est toujours résoluble, pourvu que tous les facteurs premiers de ω soient de la forme $12k\pm 1$, et seulement dans ce cas.

On voit que $\omega=11$ est le plus petit paramètre, applicable dans l'équation (1) supposée résoluble, et l'on aura la solution primitive déterminée par

$$1^2-3\cdot 2^2=-11,$$

d'où il résulte, en multipliant cette équation par l'équation de FERMAT

$$2^2-3\cdot 1^2=1,$$

ces deux égalités

$$8^2-3\cdot 5^2=-11,\quad 4^2-3\cdot 3^2=-11,$$

et les deux solutions de l'equation indéterminée

$$u^2-3v^2=-11, \tag{2}$$

ainsi obtenues, sont situées respectivement dans les intervalles I_3 et I_2, de sorte que tous les intervalles I_n contiennent, pour $n\geq 3$, précisément deux solutions de l'équation (2).

Multiplions maintenant par l'égalité

(3) $$1-3\cdot 1^2=-2,$$

l'équation (1), il résulte cette autre proposition:

II. Supposons résoluble l'équation (1), cette autre équation

(4) $$u^2-3v^2=(-1)^{\delta+1}2\omega,\quad \omega=12\nu+(-1)^{\delta},$$

est aussi résoluble, et inversement.

La multiplication susdite donnera, en effet,

$$(u\pm 3v)^2-3(u\pm v)^2=(-1)^{\delta+1}2\omega,$$

tandis que l'on aura, en multipliant cette dernière équation par (3),

$$\left(\frac{u\pm 3v}{2}\right)^2-3\left(\frac{u\pm v}{2}\right)^2=(-1)^{\delta}\omega.$$

On aura, par exemple, en vertu de (2),

$$5^2-3\cdot 1^2=7^2-3\cdot 3^2=22,$$

de sorte que tous les intervalles I_n contiennent, pour $n\geqq 2$, précisément deux solutions de l'équation

(5) $$u^2-3v^2=22$$

qui n'a aucune solution située dans l'intervalle I_1.

Quant aux équations (1) et (4), posons $\omega_1=\omega$ respectivement $\omega_1=2\omega$, nous avons à démontrer la proposition:

III. Soit (u, v) la solution primitive d'un couple de suites coordonnées appartenant à l'équation

(5) $$u^2-3v^2=-\omega_1$$

supposée résoluble, on aura toujours, quel que soit le paramètre ω_1,

(6) $$u<v,$$

ce qui donnera

(7) $$\sqrt{\frac{\omega_1+1}{3}}\geqq v>\sqrt{\frac{\omega_1}{3}}.$$

En effet, supposons $u > 2v$, la multiplication négative donnera

$$v_1 = u - 2v < v;$$

soit ensuite $2v > u > v$, on aura de même

$$v_1 = u - 2v > v,$$

tandis que l'hypothèse $u < v$ donnera

$$v_1 = 2v - u > v.$$

Cela posé, on aura, en vertu de (5),

$$v^2 + \omega_1 > 3v^2 = u^2 + \omega_1 \geqq \omega_1 + 1,$$

ce qui donnera immédiatement les inégalités (7).

Étudions par exemple le paramètre

$$\omega = 143 = 11 \cdot 13,$$

les solutions

$$1^2 - 3 \cdot 2^2 = -11, \quad 4^2 - 1 \cdot 3^2 = 13$$

donnent pour l'équation indéterminée

$$u^2 - 3v^2 = -143 \tag{8}$$

les deux solutions primitives

$$2^2 - 3 \cdot 7^2 = -143, \quad 7^2 - 3 \cdot 8^2 = -143,$$

dont les solutions réciproques deviennent respectivement

$$17^2 - 3 \cdot 12^2 = -143, \quad 10^2 - 3 \cdot 9^2 = -143,$$

qui sont toutes deux situées dans l'intervalle I_8, tandis que la multiplication négative donnera

$$25^2 - 3 \cdot 16^2 = -143, \quad 38^2 - 3 \cdot 23^2 = -143.$$

On voit que la dernière de ces solutions appartient à l'intervalle I_4, tandis que la première est irrégulière, mais la multiplication positive donnera

$$98^2 - 3 \cdot 57^2 = -143,$$

et, cette solution appartenant à l'intervalle I_5, il est évident que tous les intervalles I_n contiennent, pour $n \geqq 5$, précisément quatre solutions de l'équation (8).

Étudions encore, comme second exemple, l'équation

$$u^2 - 3v^2 = -506, \tag{9}$$

les deux solutions primitives

$$1^2 - 3\cdot 2^2 = -11, \quad 2^2 - 3\cdot 3^2 = -23$$

donnent immédiatement

$$16^2 - 3\cdot 1^2 = 253, \quad 20^2 - 3\cdot 7^2 = 253.$$

de sorte que l'on trouve, pour l'équation (9), les deux solutions primitives

$$1^2 - 3\cdot 13^2 = -506, \quad 13^2 - 3\cdot 15^2 = -506.$$

XXIV. Sur la base 5.

Il nous reste encore à étudier la base 5 qui est de première espèce.

A cet effet, remarquons tout d'abord que 5 est un premier de la forme $4k+1$ ayant les deux résidus quadratiques ± 1, il est évident que 5 est résidu quadratique des nombres premiers de la forme $10k \pm 1$.

Cela posé, nous aurons la proposition:

I. Soit ω un nombre impair, l'équation de LAGRANGE

$$u^2 - 5v^2 = \pm\omega \tag{1}$$

est toujours résoluble, pourvu que tous les facteurs premiers de ω soient de la forme $10k \pm 1$, et seulement dans ce cas.

Quant à l'équation (1), remarquons que les solutions de l'équation correspondante de FERMAT

$$x^2 - 5y^2 = \pm 1$$

sont

(2, 1), (9, 4), (38, 17), (161, 72), (682, 305), ...

On voit que les nombres premiers 11 et 19 représentent les plus petites valeurs de ω pour lesquelles l'équation (1)

soit résoluble, et les plus petites solutions correspondantes

$$3^2-5\cdot 2^2=-11\,,\quad 1^2-5\cdot 2^2=-19$$

donnent

$$17^2-5\cdot 4^2=209\,,\quad 23^2-5\cdot 8^2=209.$$

Les solutions

$$4^2-5\cdot 1^2=11\,,\quad 1^2-5\cdot 2^2=19$$

donnent de même

$$6^2-5\cdot 7^2=-209\,,\quad 14^2-5\cdot 9^2=-209\,,$$

et l'on voit que la seconde de ces solutions est située dans l'intervalle I_3, tandis que la première est irrégulière.

Appliquons maintenant la multiplication positive, nous trouvons, dans l'intervalle I_4, les quatre solutions

$$47^2-5\cdot 20^2=209\,,\quad 54^2-5\cdot 25^2=-209$$
$$73^2-5\cdot 32^2=209\,,\quad 86^2-5\cdot 39^2=-209\,,$$

de sorte que tous les intervalles I_n contiennent, pour $n\geqq 4$, précisément quatre solutions de l'équation indéterminée

$$u^2-5v^2=\pm 209. \tag{2}$$

Multiplions maintenant l'équation (1) par cette autre

$$1^2-1\cdot 5^2=-4\,, \tag{3}$$

il résulte la proposition:

II. Supposons résoluble l'équation (1), cette autre équation

$$u^2-5v^2=\pm 4\omega \tag{4}$$

est aussi résoluble, et inversement.

En effet, la méthode susdite donnera

$$(u\pm 5v)^2-5\,(u\pm v)^2=\mp 4\omega\,,$$

et u et v étant de parité différente, cette équation donne deux solutions de (3).

Multiplions maintenant les équations (3) et (4), il existe un exposant σ, telle que nous aurons les deux équations résolubles

$$\left(\frac{u+(-1)^{\sigma}5v}{4}\right)^2-5\left(\frac{u+(-1)^{\sigma}v}{4}\right)^2=\pm\omega$$
$$\left(\frac{u-(-1)^{\sigma}5v}{2}\right)^2-5\left(\frac{u-(-1)^{\sigma}v}{2}\right)^2=\pm 4,$$

ce qui nous conduira de l'équation (5) à l'équation (1).

Soit par exemple $\omega = 11$, les deux équations

$$3^2-5\cdot 2^2=-11,\quad 4^2-5\cdot 1^2=11$$

donnent respectivement

$$7^2-5\cdot 1^2=44,\quad 13^2-5\cdot 5^2=44$$
$$1^2-5\cdot 3^2=-44,\quad 9^2-5\cdot 5^2=-44,$$

de sorte que l'intervalle I_3 contient les quatre solutions

$$9^2-5\cdot 5^2=-44,\quad 13^2-5\cdot 5^2=44$$
$$17^2-5\cdot 7^2=44,\quad 19^2-5\cdot 9^2=-44;$$

c'est-à-dire que tous les intervalles I_n contiennent, pour $n\geqq 3$, précisément quatre solutions de l'équation de Lagrange

(5) $$u^2-5v^2=\pm 44.$$

Étudions encore l'équation

(6) $$u^2-5v^2=\pm 836;$$

les deux couples de solutions réciproques

$$6^2-5\cdot 7^2=-209,\quad 23^2-5\cdot 8^2=209$$
$$14^2-5\cdot 9^2=-209,\quad 17^2-5\cdot 4^2=209$$

donnent les solutions suivantes de (6):

$$29^2-5\cdot 1^2=836,\quad 41^2-5\cdot 13^2=836$$

qui sont toutes deux irrégulières,

$$59^2-5\cdot 23^2=836,\quad 31^2-5\cdot 5^2=836,$$

appartenant à I_4 respectivement à I_2,

$$3^2-5\cdot 13^2=-836,\quad 37^2-5\cdot 21^2=-836$$

qui sont toutes deux irrégulières,

$$53^2-5\cdot 27^2=-836,\quad 17^2-5\cdot 15^2=-836$$

appartenant à I_4 respectivement à I_8.

Cela posé, on verra que l'intervalle I_5 contient les huit solutions de l'équation (6):

$$179^2 - 5 \cdot 79^2 = 836, \quad 233^2 - 5 \cdot 105^2 = -836$$
$$241^2 - 5 \cdot 107^2 = 836, \quad 281^2 - 5 \cdot 125^2 = 836$$
$$287^2 - 5 \cdot 129^2 = -836, \quad 377^2 - 5 \cdot 169^2 = 836$$
$$453^2 - 5 \cdot 203^2 = -836, \quad 629^2 - 5 \cdot 281^2 = 836,$$

de sorte que tous les intervalles I_n contiennent, pour $n \geq 5$, précisément huit solutions de l'équation susdite.

TABLE DES MATIÈRES

CHAPITRE V

Des conditions de résolubilité.

Forelagt paa Mødet d. 3. November 1922.
Færdig fra Trykkeriet d. 9. Marts 1923.