Det Kgl. Danske Videnskabernes Selskab.
Mathematisk-fysiske Meddelelser. **VI,** 6.

SUR UNE
ÉQUATION DE LAGRANGE

PAR

NIELS NIELSEN

KØBENHAVN
HOVEDKOMMISSIONÆR: ANDR. FRED. HØST & SØN, KGL. HOF-BOGHANDEL
BIANCO LUNOS BOGTRYKKERI
1924

AVANT-PROPOS

CAYLEY[1], dans une petite note de trois pages, a publié une table des plus petites solutions des équations résolubles

$$(1) \qquad u^2 - av^2 = \pm 4,$$

qui correspondent aux valeurs de a inférieures à 1000.

De nos jours, M. E.-E. WHITFORD[2] a continué la table de CAYLEY en s'occupant des valeurs de a situées entre 1000 et 2000.

De plus, soit (u, v) la plus petite solution de (1), et soit (A_1, B_1) la plus petite solution de l'équation de FERMAT correspondante, savoir

$$(2) \qquad A_1^2 - aB_1^2 = \pm 1,$$

CAYLEY a démontré les formules

$$(3) \qquad A_1 = \frac{u^3 \mp 3u}{2}, \quad B_1 = \frac{v(u^2 \mp 1)}{2}.$$

Quant à l'établissement de sa table, CAYLEY dit expressément qu'il a appliqué le Canon Pellianus de DEGEN; c'est-à-dire que CAYLEY a calculé les réduites de la fraction continue de $\sqrt{a}$ jusqu'à la premiére qui correspond au paramètre 4.

Et M. WHITFORD a évidemment suivi son illustre prédécesseur.

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

[2] Annals of Mathematics (2) t. 15, p. 157—160; 1914.

Or, supposons résoluble l'équation (1), nous aurons les décompositions

$$a = p^2 \mp 4q^2, \qquad \pm v = \alpha^2 \mp 4\beta^2, \tag{4}$$

où p et q sont impairs et premiers entre eux, et il est à attendre que ces nombres p et q jouent un rôle fondamental, en ce qui concerne la résolubilité de l'équation (1).

Dans la première Partie du Mémoire que j'ai l'honneur de présenter aujourd'hui à l'Académie Royale des Sciences, je suppose que la base a se présente sous la forme

$$a = p^2 \pm k q^2, \tag{5}$$

k étant un nombre premier quelconque ou une puissance quelconque d'un tel nombre, et je trouve la condition nécessaire et suffisante pour que l'équation

$$u^2 - a v^2 = \mp k \tag{6}$$

soit résoluble.

A cet effet, remarquons que cette autre équation

$$u^2 - a v^2 = q^2 \tag{7}$$

est toujours résoluble, pourvu que (6) le soit; désignons ensuite par (u_n, v_n) (u_n', v_n') un couple de suites coordonnées appartenant à (7), la résolubilité de (6) exige qu'un des éléments primitifs de ces suites, par exemple (u_1, v_1), satisfasse à la congruence

$$u_1 - p v_1 \equiv 0 \pmod{q^2}. \tag{8}$$

Soit maintenant a un nombre premier, l'équation (7) n'est jamais résoluble, à moins que cette autre équation

$$u^2 - a v^2 = \pm \varrho q, \quad \varrho = 1 \text{ ou } \varrho = 2, \tag{9}$$

ne le soit aussi. Désignons par (s_n, t_n) (σ_n, τ_n) un couple de suites coordonnées appartenant à cette équation, (8) peut être remplacé par la congruence équivalente

$$s_1 - at_1 \equiv 0 \pmod{q}. \tag{10}$$

La deuxième Partie du présent Mémoire contient des applications au cas spécial

$$k = 4,$$

la résolution numérique de certaines équations de ce genre et une extension des bases connues $(2p+1)^2+4$ à celles-ci

$$a = p^2 q^2 \pm 4p, \tag{11}$$

où p et q sont des nombres impairs, quelconques du reste.

Quant à la troisième Partie, elle contient des applications à certaines autres valeurs spéciales du facteur k.

Copenhague, le 25 avril 1924.

Niels Nielsen.

PREMIÈRE PARTIE

Recherches sur l'équation généralisée.

I. Conditions de résolubilité.

Dans ce qui suit, nous designons par ω un nombre premier quelconque ou une puissance quelconque d'un tel nombre, par a une base qui se présente sous la forme

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

où deux quelconques des trois nombres p, q, ω sont premiers entre eux, et nous avons à étudier l'équation de Lagrange

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

A cet effet, supposons tout d'abord résoluble cette équation, puis remarquons que l'équation

$$u^2 - a v^2 = (-1)^\delta \omega q^2 \tag{3}$$

est toujours résoluble, parce qu'elle admet, en vertu de (1), la solution

$$u = p, \quad v = 1; \tag{4}$$

c'est-à-dire que cette autre équation

$$u^2 - a v^2 = q^2, \tag{5}$$

obtenue en multipliant (2) et (3), est résoluble aussi.

Désignons ensuite par

$$(u,\ v) \quad (\pi,\ \varrho)$$

les deux suites coordonnées de (2), par

$$(k, l) \quad (\varkappa, \lambda)$$

un couple de suites coordonnées de (5), il existe un couple de suites coordonnées

$$(s, t) \quad (\sigma, \tau)$$

de (3), de sorte que nous aurons, quels que soient les indices μ et ν,

$$(6) \qquad \sigma_{\mu+\nu-1} = \varkappa_\mu \pi_\nu + a \lambda_\mu \varrho_\nu, \quad \tau_{\mu+\nu-1} = \varkappa_\mu \varrho_\nu + \lambda_\mu \pi_\nu$$

$$(7) \qquad s_{\mu+\nu} = k_\mu u_\nu + a l_\mu v_\nu, \qquad t_{\mu+\nu} = k_\mu v_\nu + l_\mu u_\nu,$$

de sorte que l'élément primitif (s_1, t_1) de la suite (s, t) ne peut pas être trouvé par ces multiplications positives, mais il est facile de déduire cet élément par une multiplication négative, nous le verons, dans ce qui suit.

Resolvons maintenant par rapport à (π_ν, ϱ_ν), respectivement (u_ν, v_ν), les équations (6) et (7), puis remarquons que les déterminants de ces équations sont

$$\varkappa_\mu^2 - a\lambda_\mu^2 = (-1)^{\delta'_\mu} q^2, \quad k_\mu^2 - a l_\mu^2 = (-1)^{\delta_\mu} q^2,$$

nous aurons, en posant respectivement

$$\mu + \nu - 1 = m, \quad \mu = n$$
$$\mu + \nu = m, \quad \mu = n,$$

les formules inverses de (6) et (7)

$$(8) \quad \begin{cases} q^2 \pi_{m-n+1} = (-1)^{\delta'_n} (\varkappa_n \sigma_m - a \lambda_n \tau_m) \\ q^2 \varrho_{m-n+1} = (-1)^{\delta'_n} \varkappa_n \tau_m - \lambda_n \sigma_m), \end{cases}$$

$$(9) \quad \begin{cases} q^2 u_{m-n} = (-1)^{\delta_n} (k_n s_m - a l_n t_m) \\ q^2 v_{m-n} = (-1)^{\delta_n} (k_n t_m - l_n s_m), \end{cases}$$

où il faut supposer respectivement

$$m \geqq n, \quad m > n.$$

Or, il est facile de voir que l'on aura de même

$$(10)\quad \begin{cases} q^2 u_1 = (-1)^{\delta_1}(k_1 s_1 - a l_1 t_1) \\ q^2 v_1 = (-1)^{\delta_1}(k_1 t_1 - l_1 s_1), \end{cases}$$

car ces deux nombres satisfont à l'équation (2), et un calcul direct donnera

$$\pi_1 u_1 + a\varrho_1 v_1 = \omega A_1, \quad \pi_1 v_1 + \varrho_1 u_1 = \omega B_1,$$

où (A_n, B_n) est la solution générale de l'équation de FERMAT ayant la base a, savoir

$$A_n^2 - aB_n^2 = (-1)^{n\varepsilon},$$

où il faut admettre $\varepsilon = 1$, $\varepsilon = 0$, selon que a est une base de première ou de seconde espèce. Et l'on aura, quels que soient les indices μ et ν,

$$(11)\quad k_\mu \varkappa_\nu + a l_\mu \lambda_\nu = q^2 A_{\mu+\nu-1}, \quad k_\mu \lambda_\nu + l_\mu \varkappa_\nu = q^2 B_{\mu+\nu-1}.$$

Cela posé, nous aurons, en vertu de (6),

$$k_\alpha \sigma_{\mu+\nu-1} + a l_\alpha \tau_{\mu+\nu-1} = (\pi_\nu A_{\mu+\alpha-1} + a\varrho_\nu B_{\mu+\alpha-1})\, q^2$$
$$k_\alpha \tau_{\mu+\nu-1} + l_\alpha \sigma_{\mu+\nu-1} = (\pi_\nu B_{\mu+\alpha-1} + \varrho_\nu A_{\mu+\nu-1})\, q^2,$$

d'où, en vertu des formules récursives générales,

$$k_\alpha \sigma_{\mu+\nu-1} + a l_\alpha \tau_{\mu+\nu-1} = q^2 \pi_{\mu+\nu+\alpha-1}$$
$$k_\alpha \tau_{\mu+\nu-1} + l_\alpha \sigma_{\mu+\nu-1} = q^2 \varrho_{\mu+\nu+\alpha-1}.$$

Posons ensuite

$$\mu + \nu - 1 = m, \quad \alpha = n,$$

il résulte finalement

$$(12)\quad \sigma_m k_n + a\tau_m l_n = q^2 \pi_{m+n}, \quad \sigma_m l_n + \tau_m k_n = q^2 \varrho_{m+n},$$

formules qui sont valables pour une valeur quelconque des deux indices m et n.

Et il est évident que les formules (7) donnent, par le même procédé, les formules analogues

$$(13) \quad s_m \varkappa_n + a t_m \lambda_n = q^2 u_{m+n}, \quad t_m \varkappa_n + s_m \lambda_n = q^2 v_{m+n},$$

où il faut admettre

$$m \geqq 2, \quad n \geqq 1.$$

Quant à la valeur exclue $m = 1$, il n'existe aucune formule de la forme (13), de sorte qu'il faut, dans ce cas, appliquer (10).

Revenons maintenant aux suites coordonnées

$$(s, t) \quad (\sigma, \tau)$$

de l'équation (3), nous avons remarqué qu'il existe une seule solution appartenant à ces suites, qui ne peut pas être déterminée par la multiplication positive, indiquée dans les formules (6) et (7), savoir la solution (s_1, t_1); c'est-à-dire que nous aurons, en vertu de (4),

$$(14) \qquad s_1 = p, \quad t_1 = 1.$$

Cela posé, les formules (10) se présentent sous la forme

$$(15) \quad \begin{cases} p k_1 - a l_1 = (-1)^{\delta_1} q^2 u_1 \\ k_1 - p l_1 = (-1)^{\delta_1} q^2 v_1 ; \end{cases}$$

introduisons ensuite, dans ces formules, l'expression (1) de la base a, nous aurons la seule congruence

$$(16) \qquad p l_1 - k_1 \equiv 0 \pmod{q^2},$$

car p est premier avec q.

Et nous aurons évidemment une congruence analogue pour tous les autres couples de suites coordonnées appartenant à l'équation (5), de sorte que nous avons démontré le théorème général:

I. La condition suffisante et nécessaire pour la résolubilité de l'équation (2) est que l'équation (5) soit résoluble, de sorte qu'une des deux solutions primitives (u, v) d'un de ses couples de suites coordonnées satisfasse à la congruence

$$u - pv \equiv 0 \pmod{q^2}; \tag{17}$$

dans ce cas, une solution primitive de chacun des autres couples de suites coordonnées de (5) satisfait à une congruence analogue.

Remarquons maintenant que l'équation

$$u^2 - av^2 = \omega^2 q^2 \tag{18}$$

est résoluble, pourvu que (2) le soit, parce que cette équation provient de la multiplication de (2) et (3), il est évident que la multiplication de (3) et (18) conduira de nouveau à l'équation (2); c'est-à-dire que chacun des suites coordonnées de (18) a un élément primitif (u, v) qui satisfait à la congruence

$$u - pv \equiv 0 \pmod{\omega q^2}, \tag{19}$$

de sorte que cette congruence est équivalente à (17).

Supposons maintenant que la décomposition (1) admette plusieurs solutions, savoir

$$a = p_n^2 - (-1)^\delta \omega q_n^2, \quad n = 1, 2, 3, \ldots,$$

la méthode que nous venons de développer est applicable pour chacune de ces décompositions, ce qui donnera, quel que soit l'indice n, les congruences

$$u - p_n v \equiv 0 \pmod{q_n^2}$$
$$u' - p_n v' \equiv 0 \pmod{\omega q_n^2}.$$

Remarquons encore, en passant, qu'une infinité de solutions (u_n, v_n) et (u'_m, v'_m) satisfont aux congruences susdites, ce qui est sans valeur pour les applications, parce que ces solutions sont des grands nombres et la détermination de l'indice des solutions ainsi obtenues est assez difficile.

II. La base est un nombre premier.

Dans l'article précédent, nous avons concidéré une base quelconque de la forme susdite

$$a = p^2 - (-1)^{\delta} \omega q^2; \tag{1}$$

soit maintenant a un nombre premier, aucune des équations

$$u^2 - a v^2 = q^2 \tag{2}$$

$$u^2 - a v^2 = \omega^2 q^2 \tag{3}$$

ne peut être primitive, de sorte que ces équations ne sont jamais résolubles, à moins que les deux autres

$$u^2 - a v^2 = (-1)^{\varphi} \varrho q \tag{4}$$

$$u^2 - a v^2 = (-1)^{\psi} \varrho \omega q \tag{5}$$

ne le soient aussi; dans ces équations, on aura

$$\varrho = 1 \quad \text{ou} \quad \varrho = 2,$$

tandis que φ et ψ sont des exposants convenablement choisis. Et les équations (2) et (3) proviennent de (4) et (5) par l'opération itérative du second ordre.

Étudions tout d'abord l'équation (4), supposée résoluble, cette équation admet deux suites coordonnées

$$(s, t) \quad (\sigma, \tau)$$

qui permettent de représenter la solution (k_1, l_1), figurant dans les congruences fondamentales (15) de l'article précédent, sous la forme

$$\varrho k_1 = s_1^2 + a t_1^2, \quad \varrho l_1 = 2 s_1 t_1 \tag{6}$$

ou sous la forme

$$s_1 \sigma_1 - a t_1 \tau_1 = \pm \varrho k_1, \quad s_1 \tau_1 - t_1 \sigma_1 = \pm \varrho l_1 \tag{7}$$

Quant aux formules (6), multiplions par ϱ les deux congruences susdites, puis introduisons les expressions (6), il résulte après une simple transformation

$$\begin{aligned} s_1 (p s_1 - a t_1) - a t_1 (s_1 - p t_1) &\equiv 0 \pmod{\varrho q^2} \\ t_1 (p s_1 - a t_1) - s_1 (s_1 - p t_1) &\equiv 0 \pmod{\varrho q^2}. \end{aligned}$$

Résolvons maintenant par rapport aux expressions

$$p s_1 - a t_1, \quad s_1 - p t_1$$

ces deux congruences linéaires dont le déterminant est égal à

$$s_1^2 - a t_1^2 = \pm \varrho q,$$

il résulte la seule congruence

$$s_1 - p t_1 \equiv 0 \pmod{q}. \tag{8}$$

Partons ensuite des congruences (7), le même procédé donnera

$$\begin{aligned} s_1 (p \sigma_1 - a \tau_1) + a t_1 (\sigma_1 - p \tau_1) &\equiv 0 \pmod{\varrho q^2} \\ t_1 (\sigma_1 - p \tau_1) + s_1 (p \sigma_1 - p \tau_1) &\equiv 0 \pmod{\varrho q^2}, \end{aligned}$$

de sorte que nous aurons ici la seule congruence

$$\sigma_1 - p \tau_1 \equiv 0 \pmod{q}. \tag{9}$$

Cela posé, nous avons démontré la proposition fondamentale:

I. *Supposons résoluble l'équation (4), cette autre équation*

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

est également résoluble, pourvu qu'une solution primitive (s, t) d'un couple de suites coordonnées de (4) satisfasse à la congruence

$$s - pt \equiv 0 \pmod{q}, \tag{11}$$

et seulement dans ce cas.

Partons ensuite de l'équation (5), supposé résoluble, nous verrons par le même procédé que chacune des suites coordonnées de cette équation a également une solution primitive (s, t) qui satisfait à la congruence

$$s - pt \equiv 0 \pmod{\omega q}, \tag{12}$$

Dans l'article qui suit, nous avons à développer des propriétés curieuses des congruences que nous venons de démontrer.

III. Sur les congruences fondamentales.

Afin de mettre en pleine lumière la nature singulière des congruences que nous venons d'établir, nous avons à étudier à un autre point de vue l'équation qui nous occupe ici.

A cet effet, nous posons, pour simplifier les significations,

$$k = (-1)^{\delta+1}\omega,$$

de sorte que la base a se présente sous la forme

$$a = p^2 + kq^2, \tag{1}$$

et nous cherchons à résoudre l'équation

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

où r est un positif entier, premier avec a, au moyen des deux hypothèses suivantes:

1° L'inconnue v se présente sous la forme

$$(3) \qquad v = \alpha^2 + k\beta^2;$$

c'est-à-dire que l'équation (1) deviendra

$$(4) \qquad u^2 + kr^2 = (p^2 + kq^2)(\alpha^2 + k\beta^2)^2,$$

et l'identité

$$av^2 = \left[p(\alpha^2 - k\beta^2) \pm 2kq\alpha\beta\right]^2 + k\left[q(\alpha^2 - k\beta) \mp 2p\alpha\beta\right]^2$$

conduira, en vertu de (4), à la seconde des hypothèses susdites:

2° Les inconnues α et β sont à déterminer, de sorte que

$$(5) \qquad p(\alpha^2 - k\beta^2) \pm 2kq\alpha\beta = \pm u$$

$$(6) \qquad q(\alpha^2 - k\beta^2) \mp 2p\alpha\beta = \pm r,$$

ce qui conduira certainement à une solution de l'équation (2).

Quant à l'équation (6), nous avons déjà supposé premiers entre eux les deux nombres p et q, mais il est nécessaire que α et β aient la même propriété; car soit λ un diviseur commun de α et β, λ divise aussi r, ce qui est impossible, parce que a et r sont premiers entre eux.

De plus, il résulte immédiatement de l'équation (6), que

soit f le plus grand commun diviseur de β et r, f est aussi le plus grand commun diviseur de β et q, de sorte que β^2 et qr ont le plus grand commun diviseur f^2;

soit f_1 le plus grand commun diviseur de α et r, f_1 est aussi le plus grand commun diviseur de α et kq, de sorte que f_1^2 est le plus grand commun diviseur de α^2 et kqr.

Résolvons maintenant par rapport à α l'équation (6), il resulte

$$q\alpha = \pm p\beta \pm \sqrt{a\beta^2 \pm qr},$$

ce qui exige que le nombre qui figure sous le signe radical soit un carré exact γ^2, de sorte que nous aurons

$$(7) \qquad \gamma^2 - \alpha\beta^2 = \pm qr;$$

c'est-à-dire que γ^2 est divisible par le plus grand commun diviseur f^2 de β^2 et qr, de sorte que le facteur f^2 peut être supprimé dans l'équation (7), et les trois termes de l'équation ainsi obtenue sont deux à deux premiers entre eux.

De plus, il résulte

$$(8) \qquad q\alpha = \pm p\beta \pm \gamma;$$

c'est-à-dire que β et γ satisfont à une des congruences

$$(9) \qquad p\beta \pm \gamma \equiv 0 \pmod{q},$$

et α est déterminé par l'équation (8).

L'équation (6) donnera de même

$$kq\beta = \mp p\alpha \pm \sqrt{a\alpha^2 \mp kqr};$$

le nombre qui figure sous le signe radical est donc un carré exaxt δ^2, et l'on aura

$$(10) \qquad \delta^2 - a\alpha^2 = \mp kqr;$$

c'est-à-dire que δ est divisible par le plus grand commun facteur f_1, de α et r, de sorte que le facteur f_1^2 peut être supprimé dans l'équation (10), et les trois termes de l'équation ainsi obtenue sont deux à deux premiers entre eux.

Dans ce cas, on aura de même

$$(10) \qquad kq\beta = \mp p\alpha \pm \delta,$$

de sorte que α et δ satisfont à la congruence

$$(11) \qquad p\alpha \pm \delta \equiv 0 \pmod{kq},$$

et β est déterminé par l'équation (10).

Remarquons maintenant que les congruences (9) et (11) sont identiques aux congruences fondamentales, développées dans l'article précédent, nous avons démontré une proposition curieuse en ce qui concerne l'équation

$$u^2 - a v^2 = (-1)^\delta \omega, \tag{12}$$

savoir:

I. Soit (u, v) la solution de (12) qui correspond aux congruences (11) et (12) de l'article précédent, les deux hypothèses appliquées dans la solution de (4) sont nécessaires, de sorte que v est un nombre de la même forme que a, savoir

$$\pm v = \alpha^2 - (-1)^\delta \omega \beta^2. \tag{13}$$

De plus, supposons résolue une des équations (7) ou (10), l'autre est resolue aussi au moyen des congruences susdites, et la multiplication de ces deux équations conduira à une des solutions primitives de (12).

Du reste, la multiplication susdite n'est pas nécessaire, car l'inconnue v est déterminée par la formule (13), et nous aurons, en résolvant par rapport aux expressions

$$\alpha^2 - k\beta^2, \quad \alpha\beta$$

les équations (5) et (6),

$$qu \pm pr = 2a\alpha\beta, \tag{14}$$

où les signes doubles sont à choisir, tels que u deviendra un positif entier, ce qui détermine parfaitement l'inconnue u.

Quant aux applications de la methode susdite, nous pouvons simplement renvoyer le lecteur aux deux dernières Parties du présent Mémoire.

DEUXIÈME PARTIE

Sur le paramètre ± 4.

IV. Applications des formules générales.

Les applications les plus intéressantes de la théorie précédente se rattachent évidemment au paramètre 4, savoir à l'équation étudiée par Cayley.

En effet, supposons résoluble l'équation

$$u^2 - a v^2 = (-1)^\delta 4,$$

nous aurons nécessairement

$$a = p^2 - (-1)^\delta 4q^2, \quad \pm v = \alpha^2 - (-1)^\delta 4\beta^2,$$

où p et q, α et β sont premiers entre eux, et où p et q sont tous deux impair.

Étudions tout d'abord l'hypothèse $\delta = 1$, savoir

(1) $$u^2 - a v^2 = \pm 4, \quad a = p^2 + 4q^2,$$

il s'agit de résoudre une des équations

(2) $$s^2 - a t^2 = \pm q, \quad \sigma^2 - a\tau^2 = \mp 4q,$$

tandis que les congruences fondamentales donnent ici

(3) $$q\tau = \pm p t \pm s, \quad 4qt = \mp p\tau \pm \sigma,$$

où les premiers signes doubles correspondent, tandis qu'il faut choisir l'ensemble de ces signes, de sorte que τ et t deviennent des positifs entiers, ce qui est possible, pourvu que l'équation (1) soit résoluble.

La multiplication des équations (2) donnera ensuite la solution (u, v) de (1), determinée par les formules

$$(4) \qquad qu = |s\tau \pm at\sigma|, \quad qv = |s\tau \pm t\sigma|,$$

et il est évident que cette solution est la solution primitive de l'équation (1), parce qu'elle correspond au paramètre -4, et elle est nécessairement le premier élément d'une des deux suites coordonnées appartenant à (1).

Quant à la solution (u, v), elle peut être calculée aussi au moyen des formules

$$(5) \qquad v = \tau^2 + 4t^2, \quad qu \pm p = \pm 2at\tau,$$

où les signes doubles sont à choisir, de sorte que u devienne un positif entier.

Supposons maintenant que la base a soit un nombre premier, les équations

$$(6) \qquad \alpha^2 - a\beta^2 = \pm p, \quad \sigma^2 - a\tau^2 = \pm 4q$$

sont toutes deux résolubles, de sorte que la hauteur de q par rapport à la base a est égale ou à 1 ou à 3.

Soit l'équation (1) résoluble, q est de la hauteur 1, et σ et τ satisfont en outre aux congruences fondamentales. Soit maintenant q un nombre premier, ces congruences sont toujours satisfaites, pourvu que q soit de la hauteur 1.

Il nous semble utile d'éclaircir la théorie précédente en étudiant certaines bases spéciales, choisis hors des Tables calculées, savoir plus grandes que 2000.

Exemple I. Le nombre premier

$$2549 = 50^2 + 7^2$$

correspond aux valeurs

$$p = 7, \quad q = 25.$$

Appliquons ensuite l'identité évidente

$$101^2 - 2549 \cdot 2^2 = 5,$$

l'opération itérative du second ordre donnera

$$20397^2 - 2549 \cdot 404^2 = 25; \quad s = 20397, \ t = 404,$$

et il résulte, en vertu des formules (3),

$$25\tau = 7 \cdot 404 + 20397, \quad \tau = 929$$
$$100 \cdot 404 = -7 \cdot 929 + \sigma, \quad \sigma = 46903,$$

de sorte que

$$46903^2 - 2549 \cdot 929^2 = -100.$$

Cela posé, nous aurons

$$v = 808^2 + 929^2 = 1515905$$
$$25u - 7 = 808 \cdot 929 \cdot 2549, \quad u = 76534439,$$

ce qui donnera la solution primitive de l'équation

$$u^2 - 2549 \cdot v^2 = \pm 4,$$

savoir

$$76534439^2 - 2549 \cdot 1515905^2 = -4.$$

Exemple II. On aura, pour le nombre premier

$$2677 = 39^2 + 34^2,$$

à introduire dans les formules générales

$$p = 39, \quad q = 17.$$

Remarquons que 19 est diviseur premier de la forme quadratique $x^2 - 2677\, y^2$, nous trouvons

$$51^2 - 2677 \cdot 1^2 = -4 \cdot 19, \quad 63^2 - 2677 \cdot 1^2 = -4 \cdot 17 \cdot 19,$$

et la multiplication positive de ces équations donnera

$$155^2 - 2677 \cdot 3^2 = 4 \cdot 17; \quad \sigma = 155, \quad \tau = 3,$$

de sorte que les équations (3) deviennent

$$68t = 3 \cdot 39 + 155, \quad t = 4$$
$$17 \cdot 3 = -4 \cdot 39 + s, \quad s = 207,$$

savoir

$$207^2 - 2677 \cdot 4^2 = 17,$$

et nous aurons finalement la solution primitive

$$3777^2 - 2677 \cdot 73^2 = -4.$$

Exemple III. Pour le nombre premier

$$2693 = 47^2 + 22^2; \quad p = 47, \quad q = 11,$$

on aura

$$52^2 - 2693 \cdot 1^2 = 11,$$

ce qui donnera

$$467^2 - 2693 \cdot 9^2 = -4 \cdot 11,$$

et l'on trouve finalement

$$4411^2 - 2693 \cdot 85^2 = -4.$$

Exemple IV. Le nombre premier

$$3741 = 46^2 + 25^2; \quad p = 25, \quad q = 23$$

donnera

$$157^2 - 2741 \cdot 3^2 = -4 \cdot 5,$$

de sorte que le paramètre ± 4 est applicable.

On trouve du reste

$$21^2 - 2741 \cdot 1^2 = -4 \cdot 5^2 \cdot 23$$

$$24659^2 - 2741 \cdot 471^2 = 4 \cdot 5^2,$$

et la multiplication de ces deux équations conduira au paramètre $-4 \cdot 23$.

Exemple V. On aura pour les deux nombres premiers

$$9661 = 69^2 + 70^2, \quad 9941 = 70^2 + 71^2$$

les égalités curieuses

$$99^2 - 9661 \cdot 1^2 = 4 \cdot 5 \cdot 7, \quad 99^2 - 9941 \cdot 1^2 = -4 \cdot 5 \cdot 7,$$

égalités que nous avons à éclaircir dans l'article VII.

On voit que les solutions susdites ne satisfont pas aux congruences fondamentales, ce qui a lieu pour les solutions réciproques, car j'ai démontré que les deux bases en question sont des bases élémentaires, savoir que les deux équations

$$u^2 - 9641\, v^2 = \pm\, \omega, \quad u^2 - 9961\, v^2 = \pm\, \omega$$

sont résolubles et du genre maximum, pourvu que tous les facteurs premiers de ω soient diviseurs premiers de la forme quadratique correspondante

$$x^2 - 9641\, y^2, \quad x^2 - 9961\, y^2.$$

V. Sur les bases non-réduites.

Afin de mettre en pleine lumière les développements de l'article qui suit, nous avons à étudier la base non-réduite

(1) $$a_1 = ak^2,$$

où k est impair et plus grand que l'unité, tandis que a est un nombre de la forme $8\nu + 5$.

A cet effet, remarquons tout d'abord que a_1 ne peut jamais être une base de première classe, c'est-à-dire admettre le paramètre 4, pourvu que a ne le soit, nous aurons immédiatement la proposition:

I. Soient p et k des positifs entiers quelconques, les nombres

(2) $$a_1 = [(4p+2)^2+1](2k+1)^2$$

sont toujours des bases de seconde classe.

Exemple: Le nombre

$$2525 = 5^2 \cdot 101$$

est une base de seconde espèce et de seconde classe.

Pour obtenir d'autres règles de ce genre, nous partons de l'équation

(3) $$u^2 - av^2 = (-1)^\delta 4,$$

supposée résoluble, et de l'équation de Fermat correspondante

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

et nous avons à démontrer les propositions suivantes:

II. La base a_1, définie par la formule (1), est toujours de seconde classe, pourvu que k soit un diviseur de B_1, qui ne divise pas v.

En effet, soient (u, v) et (u'_1, v'_1) deux solutions quelconques de (3), on aura toujours

(5) $$\pm v' = A_n v \pm B_n u,$$

et, k étant diviseur de B_n, parce que B_n est multiple de B_1, k est premier avec A_n, de sorte que k ne peut jamais diviser v'.

Exemple: Le nombre

$$2277 = 9 \cdot 253$$

est une base de seconde classe, parce que B_1 appartenant à la base 253 est multiple de 3, et l'on aura

$$1177^2 - 253 \cdot 74^2 = 4.$$

III. La base a_1 est de seconde classe, pourvu que k soit un diviseur de A_1, qui ne divise ni u ni v.

Soit, dans la formule récursive (5), n impair, k divise A_n qui est multiple de A_1; soit, au contraire, n un nombre pair, B_n est multiple de A_1 et par conséquent aussi multiple de k, de sorte que k ne peut jamais diviser le nombre v'.

Exemple: Le nombre

$$2541 = 21 \cdot 11^2$$

est une base de seconde classe, car on aura

$$55^2 - 21 \cdot 12^2 = 1, \quad 5^2 - 21 \cdot 1^2 = 4.$$

Cela posé, nous avons à étudier des bases non-réduites de première classe, et nous citons en premier lieu la règle évidente:

IV. Soit k diviseur de v, la base a_1 est toujours de première classe et de la même espèce que a pourvu que la solution (u, v) corresponde au paramètre -4, sinon a_1 peut être de seconde espèce.

Exemples: Le nombre

$$3725 = 149 \cdot 5^2$$

est une base de première classe et de première espèce, car

$$61^2 - 149 \cdot 5^2 = -4.$$

V. Soit k un diviseur quelconque de u, la base a_1 est toujours de première classe, mais de seconde espèce, quelle que soit la base a.

En effet, l'opération itérative du second ordre donnera, en vertu de (3),

$$\left(u^2-(-1)^{\delta}2\right)^2-a(uv)^2=4,$$

de sorte que a_1 est certainement une base de première classe.

Quant à l'espèce de la base a_1, la formule de Cayley

$$A_m=\frac{u^3-(-1)\,3u}{2},$$

où m est un indice convenablement choisi, montre clairement qu'un diviseur de u est aussi diviseur d'un A_m, et ces nombres sont premiers avec les B_{2n+1}; c'est-à-dire que a_1 est une base de seconde espèce.

Exemple: La base

$$10309=61\cdot 13^2$$

est de première classe et de seconde espèce, car

$$39^2-61\cdot 5^2=-4$$

VI. La base a_1 est toujours de première classe, pourvu que k est diviseur de a et premier avec B_1.

Supposons résoluble l'équation

$$u^2-av^2=(-1)^{\delta}\omega, \tag{6}$$

cette autre équation

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

est résoluble aussi, pourvu que l'exposant ε soit convenablement choisi.

Exemple: La base

$$2125=85\cdot 5^2$$

est de première espèce et de première classe, parce que $B_1=41$, et 5 est du rang 5 par rapport à la base 85.

Le même procédé donnera cette autre proposition du même genre:

VII. Soit k un nombre premier du rang $k \pm 1$ par rapport à la base a, a_1 est toujours de première classe et de seconde espèce.

Dans ce cas, les équations (6) et (7) sont simultanément résolubles ou non, mais il faut supposer $\varepsilon = 0$, car k est toujours de la forme $4\nu + 3$.

Exemple: La base

$$2637 = 3^2 \cdot 293$$

est de première classe, parce que 3 est du rang 4 par rapport à la base $293 = 17^2 + 4$.

VI. Sur une classe d'équations immédiatement résolubles.

Soit a une base de la forme

$$(2k+1)^2 + (-1)^\delta 4,$$

il est bien connu que l'équation

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

a la solution primitive

$$u = 2k+1, \quad v = 1.$$

Mais, chose curieuse, il semble être resté inaperçu jusqu'ici qu'il est très facile de généraliser beaucoup cette équation et sa solution primitive, ce qui donnera une classe infinie d'équations, dont les solutions sont dès à présent connues.

Partons des identités évidentes

$$pq^2 - (pq^2 \pm 4) \cdot 1^2 = \mp 4 \tag{1}$$

$$(pq^2 \pm 2)^2 - (p^2q^2 \pm 4p)\, q^2 = 4, \tag{2}$$

où p et q sont impairs, le nombre

$$a = p^2q^2 \pm 4p \tag{3}$$

n'est jamais un carré exact, parce que les deux facteurs

$$p, \quad pq^2 \pm 4$$

sont premier entre eux, et ces facteurs ne sont jamais tous deux des carrés exacts.

Cela posé, il est évident que l'équation de LAGRANGE

$$(4) \qquad u^2 - av^2 = 4$$

est toujours résoluble, parce qu'elle admet, en vertu de (2), la solution

$$(5) \qquad u = pq^2 \pm 2, \quad v = q.$$

De plus, je dis que la base a est toujours de seconde espèce, pourvu que $p > 1$.

En effet, supposons tout d'abord que le nombre

$$(6) \qquad pq^2 \pm 4$$

ne soit pas un carré exact, l'équation (1) est une équation de LEGENDRE admettant le paramètre 4, donc a est de seconde espèce.

Soit, au contraire, le nombre (5) un carré exact s^2, savoir

$$s^2 - pq^2 = \pm 4,$$

l'opération itérative du second ordre donnera

$$(s^2 \mp 2)^2 - (ps^2)\, q^2 = 4,$$

savoir l'équation (2), et ps^2 est, en vertu de la proposition V de l'article précédent, une base de seconde espèce.

Cela posé, nous avons démontré le théorème général:

I. Soient d_1 et d_2 diviseurs, quelconques du reste, du nombre impair D,

$$a = d_1^2 (D^2 \pm 4 d_2)$$

est toujours une base de première classe, mais de seconde espèce, pourvu que $d_1 d_2 > 1$.

En effet, posons

$$D = d_1 d_2 d_3, \quad a = d_1^2 (d_1^2 d_2 d_3^2 \pm 4 d_2),$$

il résulte, en vertu de (3),

$$p - d_1^2 d_2, \quad q - d_3,$$

de sorte que l'équation

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

admet la solution

$$u = d_1^2 d_2 d_3^2 \pm 2, \quad v = d_2,$$

et nous savons que a est toujours une base de seconde espèce.

Quant à la portée de ces recherches, remarquons que nous avons démontré cet autre théorème général:

II. *Supposons que le nombre* (6) *ne soit aucun carré exact, l'équation*

$$u^2 - (p^2 q^2 \pm p) v^2 = 4 \tag{7}$$

a la solution primitive $(pq^2 \pm 2, q)$.

On a calculé, au moyen des fractions continues, les solutions primitives de toutes les équations résolubles

$$u^2 - a v^2 = \pm 4$$

qui correspondent aux bases inférieures à 2000. Or, en continuant ce calcul, on aurait peut-être trouvé les deux théorèmes que nous venons de démontrer; car parmi les douze nombres $8\nu + 5$ situés entre 2000 et 2100, huit sont de la forme susdite, savoir

$$\begin{array}{lll} 2005 = 45^2 - 20 & 2013 = 45^2 - 12 & 2021 = 45^2 - 4 \\ 2029 = 45^2 + 4 & 2037 = 45^2 + 12 & 2045 = 45^2 + 20 \\ 2061 = 45^2 + 36 & 2085 = 45^2 + 60, & \end{array}$$

et les solutions primitives des équations correspondantes se déterminent immédiatement en introduisant, dans les formules générales, les valeurs de p et q, diviseurs de 45.

VII. Sur certaines sommes de deux carrés.

Les sommes de deux carrés consécutifs présentent un certain intérêt.

En premier lieu citons la formule curieuse

$$(1) \qquad [(p-1)^2+p^2]\,[p^2+(p+1)^2] = 4p^4+1,$$

puis étudions le reste obtenu en extrayant la racine carrée d'une somme de deux carrés consécutifs, il s'agit évidemment d'étudier l'équation

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

ou, ce qui est la même chose.

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

de sorte que r est nécessairement multiple de 4, et tous les facteurs premiers de $2r-1$ sont de la forme $8\nu\pm 1$.

Soit, au contraire,

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

on aura de même

$$(5) \qquad (2x+1)^2-2y^2 = -(2r+1),$$

de sorte que tous les facteurs premiers de $2r+1$ sont de la forme $8\nu\pm 1$.

Posons particulièrement, dans (2) et (3), $r=4$, il résulte

$$(6) \qquad x^2+(x+1)^2 = y^2+4$$

$$(7) \qquad u^2-2v^2 = 7, \quad u = 2x+1, \quad v = y;$$

remarquons ensuite que l'équation (7) a les solutions primitives

$$(3, 1) \quad (5, 3)$$

puis posons

$$(8) \qquad A_n^2-2B_n^2 = (-1)^n, \quad n = 1, 2, 3, \ldots,$$

les solutions générales de (7) se présentent sous la forme

$$u_n = 3A_{2n}+2B_{2n}, \quad v_n = A_{2n}+3B_{2n}$$
$$u_n' = 5A_{2n}+6B_{2n}, \quad v_n' = 3A_{2n}+5B_{2n}$$

de sorte que l'équation (7) a les solutions générales

$$(9) \qquad \begin{cases} x_n = A_{2n}+B_{2n}+\dfrac{A_{2n}-1}{2}, & y_n = A_{2n}+3B_{2n} \\[2ex] \xi_n = 2A_{2n}+3B_{2n}+\dfrac{A_{2n}-1}{2}, & \eta_n = 3A_{2n}+5B_{2n}, \end{cases}$$

et pour la valeur

$$x = x_n, \quad x = \xi_n,$$

le nombre

$$x^2 + (x+1)^2$$

est toujours une base de première espèce.

Revenons ensuite aux égalités curieuses, en ce qui concerne les deux nombres premiers

$$9661 = 69^2 + 70^2, \quad 9941 = 70^2 + 71^2,$$

mentionnées dans l'article VI, il s'agit de l'équation

$$y^2 - [x^2 + (x \pm 1)^2] = \mp 2x, \tag{10}$$

ou, ce qui est la même chose,

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

de sorte que nous aurons, en vertu (8)

$$y = A_{2n}, \quad x = B_{2n}. \tag{11}$$

Or, dans le cas susdit, x est de la forme $4k+2$, ce qui exige que, dans (11), n soi un nombre impair, ce qui donnera, pour les sommes de deux carrés consécutifs, l'expression générale

$$B_{4n-2}^2 + (B_{4n-2} \pm 1)^2. \tag{12}$$

Les deux premiers couples de ces nombres deviennent

$$2^2 + 1^2, \qquad 2^2 + 3^2$$
$$70^2 + 69^2, \quad 70^2 + 71^2.$$

Quant aux nombres $(2p+1)^2 + 4$, nous aurons la formule analogue à (1),

$$(4p^2 + 1)\left((2p+2)^2 + 1\right) = (2p+1)^4 + 4, \tag{13}$$

de sorte qu'il n'existe que le seul nombre premier 5 de la forme

$$(4p+1)^{4n} + 4. \tag{14}$$

Les nombres

$$a = (2p+1)^2 + 4 \tag{15}$$

présentent aussi un certain intérêt à un autre point de vue.

En effet, l'équation

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

n'est résoluble que pour deux valeurs de ω inférieures à $\sqrt{a}$, savoir

$$\omega = 4; \quad \omega = 2p+1;$$

c'est-à dire qu'un diviseur premier de la forme quadratique

$$x^2 - ay^2,$$

qui est plus petit que $2p+1$, est certainement d'une hauteur plus grande que l'unité, par rapport à la base a.

TROISIÈME PARTIE

Sur certains paramètres spéciaux.

VIII. Sur les paramètres 2 et 8.

Il est bien connu que le nombre premier 2 joue, dans la théorie des résidus quadratiques, un triple rôle, selon qu'il se présente sous la forme.

$$2 \quad 4 \quad 2^n, \quad n \geqq 3.$$

Et c'est la même chose dans la théorie des équations de LAGRANGE, ce qui entraîne que les nombres premiers ont des propriétés différentes, selon qu'ils se présentent sous la forme

$$8k+1 \quad 8k+3 \quad 8k+5 \quad 8k+7.$$

Dans la deuxième Partie du Mémoire présent nous avons étudié la troisiéme de ces formes, de sorte qu'il nous reste ici à étudier les trois autres.

Soit tout d'abord $a = 8k+3$, nous aurons une et seulement une décomposition de la forme

$$a = p^2 + 2q^2, \tag{1}$$

de sorte que c'est précisément ces deux nombres p et q qui figurent dans les congruences fondamentales qui correspondent à la valeur

$$\omega = 2.$$

Quant aux nombres premiers $a = 8k+7$, nous avons à résoudre l'équation de LAGRANGE

$$u^2 - 2v^2 = \pm a; \tag{2}$$

soit donc

$$(3) \qquad (s_n, t_n) \quad (\sigma_n, \tau_n)$$

les deux suites coordonnées de cette équation, de sorte que

$$(4) \qquad s_1^2 - 2t_1^2 = -a,$$

nous pouvons appliquer, dans les congruences fondamentales, une quelconque des décompositions

$$(5) \qquad a = s_{2n}^2 - 2t_{2n}^2 = \sigma_{2n-1}^2 - 2\tau_{2n-1}^2,$$

où t_{2n} et τ_{2n-1} sont tous des nombres impairs.

On aura, au contraire, pour les autres éléments des suites (3),

$$-a = s_{2n-1}^2 - 2t_{2n-1}^2 = \sigma_{2n}^2 - 2\tau_{2n}^2,$$

décompositions qui sont de la forme

$$-a = p_n^2 - 8q_n^2 = \pi_n^2 - 8\varrho_n^2.$$

Restent encore les nombres premiers $a = 8k+1$, qui unissent les propriétes des deux cas précédents, parce que nous avons à la fois une seule décomposition de la forme

$$(6) \qquad a = p^2 + 8q^2$$

et l'équation résoluble de Lagrange

$$(7) \qquad u^2 - 2v^2 = \pm a.$$

Soient donc, avec la condition (4), (3) les suites coordonnées qui correspondent à cette équation, les nombres t_{2n} et τ_{2n-1} sont pairs, tandis que t_{2n-1} et τ_{2n} sont impairs, de sorte que nous avons ici

$$a = p_n^2 - 8q_n^2 = \pi_n^2 - 8\varrho_n^2$$

$$-a = p_n^2 - 2q_n^2 = \pi_n^2 - 2\varrho_n^2.$$

Afin de mettre en pleine lumière la nature singulière du nombre premier 2, nous avons encore à démontrer les deux propositions suivantes, où a désigne un nombre premier:

I. Les deux équations

$$(8) \qquad u^2 - av^2 = p^{2^n} \quad u^2 - av^2 = p,$$

où p est impair, sont simultanément résolubles ou non.

En effet, la première de ces équations n'étant pas primitive, parce que la base a est un nombre premier, nous aurons cette autre équation résoluble

$$u^2 - av^2 = \pm p^{2^{n-1}}, \quad a = 4k+1 \tag{9}$$

$$u^2 - av^2 = \pm p^{2^{n-1}}, \quad a = 4k+3; \tag{10}$$

mais, dans ce dernier cas, l'équation

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

est résoluble aussi, de sorte que nous aurons toujours l'équation résoluble

$$u^2 - av^2 = p^{2^{n-1}},$$

et ainsi de suite.

II. Les deux équations

$$u^2 - av^2 = \pm 2^{2^n+2}, \quad u^2 - av^2 = \pm 8 \tag{11}$$

sont simultanément résolubles ou non.

Remarquons tout d'abord que le nombre premier a est, dans ce cas, nécessairement de la forme $8k+1$, il est évident que les signes doubles sont applicables dans les équations (11).

Cela posé, le même procédé que dans le cas précédent conduira ici à cette autre équation résoluble

$$u^2 - av^2 = \pm 2^{2^{n-1}+2},$$

et ainsi de suite.

Cette proposition établie, il est par exemple facile de démontrer que le nombre premier

$$4993 = 63^2 + 32^2$$

est une base élémentaire, de sorte que l'équation

$$u^2 - 4993\, v^2 = \pm \omega$$

est toujours résoluble et du genre maximum, pourvu que tous les facteurs premiers de ω soient diviseurs premiers de la forme quadratique

$$x^2 - 4993\, y^2,$$

IX. Sur le paramètre 3.

Supposons résoluble l'équation de LAGRANGE

$$u^2 - a v^2 = (-1)^\delta 3, \tag{1}$$

nous aurons toujours

$$a = p^2 - (-1)^\delta 3 q^2, \tag{2}$$

de sorte que les congruences fondamentales sont toujours applicables dans ce cas.

Or, ces applications ne présentant aucun intérêt spécial, nous nous bornerons à résoudre le problème:

Déterminer les bases a qui permettent de résoudre l'équation

$$(x+1)^2 - a y^2 = x. \tag{3}$$

Il est évident que l'équation proposée se transforme en celle-ci

$$x^2 + x + 1 = a y^2,$$

ou, se qui est la même chose,

$$(2x+1)^2 - a(2y)^2 = -3, \tag{4}$$

de sorte que a est nécessairement un nombre impair de la forme

$$a = p^2 + 3q^2, \quad a = 6\nu + 1. \tag{5}$$

Cela posé, il est facile de démontrer la proposition:

I. L'équation (3) est toujours résoluble, pourvu que la base a admette le paramètre -3, et que le nombre premier 2 soit du rang 2 par rapport à a, conditions qui sont à la fois nécessaires et suffisantes.

En effet, soit, dans l'équation (4), savoir

$$u^2 - a v^2 = -3 \tag{6}$$

a un nombre impair, et soit 2 du rang 2 par rapport à la base a, le nombre A_1, tiré de l'équation de Fermat

$$A_n^2 - a B_n^2 = (-1)^{n\varepsilon}, \tag{7}$$

est nécessairement un nombre pair, parce que B_1 est impair.

Soient donc

$$(u_1, v_1) \quad (u_1', v_1')$$

les éléments primitifs des deux suites coordonnées de (5), il résulte immédiatement des formules fondamentales

$$u_1 u_1' + a v_1 v_1' = 3 A_1, \quad u_1 v_1' + u_1' v_1 = 3 B_1$$

que u_1 et v_1' ou u_1' et v_1 sont toujours des nombres pairs.

Supposons ensuite v_1 pair, les éléments généraux

$$(x_n, y_n) \quad (\xi_n, \eta_n)$$

des deux suites coordonnées, appartenant à l'équation (3), se présentent sous la forme

$$\left\{ \begin{aligned} x_n &= \frac{u_{2n-1} - 1}{2}, \quad & y_n &= \frac{v_{2n-1}}{2} \\ \xi_n &= \frac{u_{2n}' - 1}{2}, \quad & \eta_n &= \frac{v_{2n}'}{2}. \end{aligned} \right. \tag{8}$$

Quant à la proposition I, nous aurons immédiatement comme corollaire cette autre:

II. L'équation (3) est toujours résoluble, pourvu que a soit une base impaire de première espèce qui correspond au paramètre 3.

En effet, il résulte immédiatement de (6) que v est toujours un nombre pair, parce que a est de la forme $4k+1$.

Soit ensuite a une base de seconde espèce qui admet le paramètre -3, et par rapport à laquelle le nombre premier 2 est du rang 1, l'équation (3) est tantôt résoluble tantôt irrésoluble.

Pour la base
$$a = 259$$
on aura par exemple
$$A_1 = 847225, \quad B_1 = 52644,$$
de sorte que 2 est du rang 1, et l'on aura
$$16^2 - 259 \cdot 1^2 = -3;$$
c'est-à-dire qu'aucun des nombres v, tirés de l'équation (6), ne peut être pair, et l'équation (3) est irrésoluble.

Soit, au contraire
$$a = 217,$$
on aura
$$A_1 = 3844063, \quad B_1 = 260952,$$
de sorte que 2 est, aussi dans ce cas, du genre 1, mais on aura
$$383^2 - 217 \cdot 26^2 = -3;$$
c'est-à-dire que tous les v sont pairs, et l'équation (3) est résoluble pour $a = 217$.

X. Sur le paramètre 5.

Comme dernière application, nous aurons à étudier l'équation

(1) $$u^2 - av^2 = (-1)^\delta 5;$$

soit $\delta = 0$, la base a est toujours de la forme

(2) $$a = p^2 - 5q^2,$$

de sorte que les congruences générales sont immédiatement applicables.

Or, ces applications ne présentant aucun intérêt spécial, nous nous bornerons ici à résoudre un problème assez curieux.

En effet, il résulte immédiatement de l'identité évidente
$$x(x+1)(x+2)(x+3) + 1 = (x^2 + 3x + 1)^2$$
que le produit de quatre nombres consécutifs plus un est toujours un carré exact.

Mais ce carré, peut-il contenir des facteurs biquadratiques? A cet effet, il faut étudier l'équation indéterminée à trois inconnues

$$x^2 + 3x + 1 = y^2 z, \tag{3}$$

ou, ce qui est la même chose,

$$(2x+3)^2 = z(2y)^2 + 5;$$

c'est-à-dire que le facteur z est nécessairement une base a qui permet de résoudre l'équation de Lagrange.

$$u^2 - a v^2 = 5, \tag{4}$$

de sorte que v est un nombre pair.

Cela posé, remarquons que av^2 est, dans l'équation (4), de la forme $4k+2$, a est nécessairement impair, savoir

$$a = 10\nu \pm 1, \tag{5}$$

parce que a est résidu de 5. Et il est facile de démontrer la proposition:

I. Le rang du nombre 10 par rapport à une base de la forme $a = 5\nu \pm 1$ est au plus égal à 2.

En effet, l'équation de Fermat

$$A_1^2 - (5\nu \pm 1) B_1^2 = (-1)^\delta$$

donnera immediatement la congruence

$$A_1^2 \mp B_1^2 \equiv (-1)^\delta \pmod{5},$$

congruence qui n'est possible, à moins qu'un des nombres A_1 et B_1 ne soit multiple de 5; c'est-à-dire que

$$B_2 = 2 A_1 B_1$$

est toujours multiple de 10.

Supposons maintenant que a soit de la forme $8k+1$, savoir, en vertu de (5)

$$a = 20\nu + 1, \quad a = 20\nu + 9, \tag{6}$$

il est évident que l'équation (4) n'est jamais résoluble, à moins que l'inconnue v ne soit de la forme $4k+2$, ce qui a par conséquent toujours lieu pour les bases de première espèce, et nous avons démontré la proposition:

II. L'équation (3) est toujours résoluble, pourvu que z, savoir la base a, soit de la forme (6).

Désignons ensuite par

$$(u_n,\, v_n)\ (u'_n,\, v'_n) \tag{7}$$

les deux suites coordonnées de l'équation (4), puis supposons que a soit une base de première espèce, il est possible de choisir les suites (7), telles que la solution complète de (3) est présentée par les formules

$$\left\{\begin{aligned} x_n &= \frac{u_{2n-1}-3}{2}, \quad & y_n &= v_{2n-1} \\ \xi_n &= \frac{u'_{2n}-3}{2}, \quad & \eta_n &= v'_{2n}. \end{aligned}\right. \tag{8}$$

Soit, au contraire, a une base de seconde espèce, on aura de même

$$\left\{\begin{aligned} x_n &= \frac{u_n-3}{2}, \quad & y_n &= v_n \\ \xi_n &= \frac{u'_n-3}{2}, \quad & \eta'_n &= v'_n. \end{aligned}\right. \tag{9}$$

Quant aux bases $a = 4k+3$, savoir, en vertu de (5),

$$a = 20\nu + 11\,, \quad a = 20\nu + 19\,, \tag{10}$$

j'ai en vain cherché à démontrer que 10 soit du rang 2 par rapport à ces bases, mais plus tard j'ai vu que cela n'est pas juste pour

$$a = 1051\,, \quad a = 1159\,,$$

tandis que les autres 58 bases de la forme (10) et inférieures à 1500 ont bien la propriété susdite.

Supposons applicable une base de la forme (10), les solutions de (3) se déterminent aussi par les formules (9).

Remarquons, en passant, que les recherches précédentes permettent de résoudre cet autre problème:

Déterminer les bases a qui permettent de résoudre les équations simultanées

(11) $\quad (x+1)^2 - ay^2 = -x, \quad (x+2)^2 - ay^2 = x+3.$

Soustrayons ces deux équations, il est évident qu'elles sont simultanément résolubles ou non, de sorte que nous pouvons nous borner à étudier par exemple la première, et nous aurons immédiatement

$$x^2 + 3x + 1 = ay^2,$$

savoir l'équation (3).

TABLE DES MATIÈRES

Forelagt paa Mødet den 25. April 1924.
Færdig fra Trykkeriet den 28. Juli 1924.