Det Kgl. Danske Videnskabernes Selskab.

Mathematisk-fysiske Meddelelser. **VI,** 1.

SUR L'OPÉRATION ITÉRATIVE

DES

ÉQUATIONS DE LAGRANGE

PAR

NIELS NIELSEN

KØBENHAVN

HOVEDKOMMISSIONÆR: ANDR. FRED. HØST & SØN, KGL. HOF-BOGHANDEL

BIANCO LUNOS BOGTRYKKERI

1924

AVANT-PROPOS

Le Mémoire que j'ai l'honneur de présenter aujourd'hui à l'Académie Royale des Sciences termine assez harmonieusement, ce me semble, la première partie de mes recherches sur les équations de LAGRANGE, recherches qui sont indispensables pour le calcul d'une Table contenant les solutions primitives (u, v) des équations résolubles de la forme

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

déterminées par les conditions

$$2 \leqq a \leqq 100, \quad 2 \leqq \omega \leqq 1000$$

et de quelques autres qui correspondent à des valeurs plus grandes de la base a.

Et je ne vois pour le moment aucun moyen de pousser plus loin de telles recherches d'un caractère assez général.

En effet, soit le nombre premier impair p diviseur de la forme quadratique

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

on peut démontrer qu'il existe un positif entier α, qui peut être égal à l'unité, la hauteur de p par rapport à la base a, de sorte que l'équation

$$u^2 - a v^2 = (-1)^\delta p^n$$

est, avec un choix convenable de l'exposant δ, toujours résoluble, pourvu que n soit multiple de α, et seulement dans ce cas.

Quant à la puissance p^β, sa hauteur par rapport à la base a est le plus petit commun multiple de α et β.

Ces définitions adoptées, je démontre, dans l'article XV, un théorème généralement valable pour toutes les bases décomposées, avec des réserves pour certaines bases de seconde espèce ne contenant que deux facteurs premiers inégaux.

En effet, partons du paramètre

$$\omega = \pi_1^{\alpha_1} \pi_2^{\alpha_2} \ldots . \pi_n^{\alpha_n},$$

décomposé en facteurs premiers, puis supposons que tous les facteurs $\pi_r^{\alpha_r}$ soient des hauteurs 1 ou 2 par rapport à la base a, il existe toujours une décomposition

$$a = pq, \quad 1 \leq p < q \leq a,$$

telle que l'équation

$$p\sigma^2 - q\tau^2 = (-1)^\delta \omega \tag{3}$$

est résoluble, et le genre de cette équation a sa valeur maximum 2^{n-1} ou 2^n, selon que $\omega = 4k+2$ ou non.

Soit, dans l'équation (3),

$$p = 1, \quad q = a,$$

nous aurons une équation de Lagrange, sinon je la désigne comme une équation de Legendre, parce que ce géomètre, aussi modeste que distingué, mais souvent trop peu apprécié, a étudié de telles équations qui correspondent à l'hypothèse $\omega = 1$.

Et c'est précisément la théorie des équations de Legendre qui permet de démontrer le théorème susdit.

Désignons maintenant par

$$p_1 \, p_2 \, p_3 \ldots . p_n \ldots .$$

l'ensemble des diviseurs premiers impairs de la forme quadratique (2), par

$$h_1\ h_2\ h_3\ \ldots\ h_n\ \ldots$$

leurs hauteurs par rapport à la base a, on peut démontrer que le plus petit commun multiple H_a de ces hauteurs ne dépend que d'un certain nombre des premières valeurs des h_s.

Ce nombre H_a, que nous désignons comme la hauteur absolue de la base a, est diviseur du nombre de classes de la forme quadratique (2).

A ce point de vue, on démontrera aussi facilement que la hauteur absolue H_a est impair, pourvu que a soit un nombre premier, mais toujours pair, pourvu que a contienne au moins trois facteurs premiers inégaux.

Mais, soit p un diviseur premier impair de la forme quadratique susdite, nous ne possédons pour le moment aucun moyen général de déterminer de la hauteur de p par rapport à la base a, nous savons seulement que cette hauteur est diviseur de la hauteur absolue H_a. Et la connaissance des hauteurs de tous les facteurs premiers d'un paramètre ω est indispensable pour la résolution numérique de l'équation de Lagrange en question.

Quant au genre d'une équation de Lagrange, ce nombre n'a aucune analogie dans la théorie des formes quadratiques, et sa détermination générale, à l'aide des hauteurs des facteurs premiers du paramètre ω, semble un peu compliquée.

Dans le Chapitre V du présent Mémoire, on trouvera des théorèmes fondamentaux, en ce qui concerne le cas $H_a = 3$, théorèmes qui sont nécessaires pour démontrer par exemple que le genre de l'équation

$$u^2 - 37\,v^2 = \pm 924$$

est égal à 6.

Et, chose curieuse, le genre de toutes les autres équations, résolues dans ma Table susdite, est une puissance de 2.

On trouvera bien, dans cette Table, la valeur absolue $H_a = 3$ pour les bases

$$79 \quad 101 \quad 141 \quad 142 \quad 197 \quad 257,$$

mais les produits de quatre diviseurs premiers de la hauteur 3 dépassent, pour ces bases, toujours la limite fixée 1000 du paramètre ω.

Dans le Chapitre Premier, j'ai résolu un autre problème qui se rattache à la hauteur absolue d'une base.

A cet effet, supposons résolubles les équations de LAGRANGE

$$u^2 - av^2 = (-1)^{\delta_r} \omega_r, \quad r = 1, 2, 3, \ldots\ldots,$$

puis désignons par

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_n^{\alpha_n}$$

un positif entier décomposé en facteurs premiers et étant premier avec tous les paramètres ω_r, la hauteur d'un quelconque de ces paramètres, par rapport à la base ak^2, est une aliquote du nombre

$$\Omega = k(p_1^2 - 1)(p_2^2 - 1) \ldots\ldots (p_n^2 - 1).$$

Quant aux équations de LEGENDRE

$$p\sigma^2 - q\tau^2 = (-1)^{\delta} \omega$$

nous avons déjà remarqué qu'elles jouent un rôle essentiel dans la théorie des équations de LAGRANGE de la hauteur 2 et par conséquent aussi pour de telles équations d'une hauteur paire.

Quant à la hauteur d'une équation de LAGRANGE, supposons que l'équation

$$u^2 - av^2 = \pm \omega^m \tag{4}$$

soit résoluble, pourvu que m soit multiple du positif entier n, et seulement dans ce cas, nous disons que les suites coordonnées de cette équation sont de la hauteur n.

Soit l'équation (4) du genre maximum, pourvu que m soit multiple du positif entieur ν, et seulement dans ce cas, nous disons que cette équation est de la hauteur ν.

De plus, on démontrera aussi facilement, à ce point de vue, que la hauteur absolue H_a de la base a est toujours un nombre pair, pourvu que a ne soit ni un nombre premier ni une base de seconde espèce de la forme $4k+1$ ou de la forme $4k+2$, qui ne contient que deux facteurs premiers inégaux. Ces nombres sont par conséquent les seules bases qui n'admettent aucune équation de Legendre.

Il est bien connu que la théorie des formes quadratiques est restée jusqu'ici insuffisante, en ce qui concerne l'espèce d'une base composée qui est une somme de deux carrés premiers entre eux, et que les règles de Dirichlet sont trouvées à un autre point de vue.

Dans le Chapitre VI du présent Mémoire, j'ai donné des suppléments aux règles susdites, et j'ai examiné les vingt-trois nombres de la forme

$$(10\,a \pm b) + (10\,b \mp a)^2 = 101\,(a^2 + b^2)$$

qui sont inférieurs à 10000. Parmi ces vingt-trois nombres six seulement sont des bases de seconde espèce.

Les Tables numériques, jointes à ce Mémoire, sont calculées par moi, revues et contrôlées par M. G. Rash.

Copenhague, le 14 décembre 1923.

Niels Nielsen.

CHAPITRE PREMIER

Applications de l'opération générale.

I. Congruences fondamentales.

Soit, comme ordinairement, (A_n, B_n) la solution générale de l'équation de Fermat

(1) $$x^2 - a y^2 = (-1)^{\delta},$$

de sorte que

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

et soit k un positif entier quelconque, il existe un indice r, le rang du nombre k par rapport à la base a, tel que B_n est toujours multiple de k, pourvu que l'indice n soit multiple de r, et inversement; c'est-à-dire que la solution générale (α_n, β_n) de cette autre équation de Fermat

(3) $$x^2 - (a k^2) y^2 = (-1)^{n\varepsilon}, \quad \varepsilon = r\delta,$$

se présente sous la forme

(4) $$\alpha_n = A_{nr}, \quad \beta_n = \frac{B_{nr}}{k}.$$

Cela posé, il est évident que nous pouvons nous borner à étudier les équations de Fermat, dont la base ne contient aucun facteur quadratique; ces bases, que nous désignons comme des bases réduites, jouent un rôle essentiel dans plusieurs de nos recherches suivantes.

Quant à l'équation de Lagrange

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

désignons par k un positif entier, premier avec le paramètre ω, cette autre équation de Lagrange

$$u^2 - (ak^2)v^2 = (-1)^{\varepsilon}\omega \tag{6}$$

n'est pas généralement résoluble; c'est-à-dire qu'il n'existe généralement aucune solution (u, v) de l'équation (5), pour laquelle le nombre v est multiple de k.

Mais supposons impair le paramètre ω, il existe toujours un positif entier ϱ, la hauteur de ω par rapport à la base ak^2, de sorte que cette autre équation de Lagrange

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

est résoluble, pourvu que l'exposant n soit multiple de ϱ, et seulement dans ce cas.

A cet effet; nous avons tout d'abord à étudier plus profondément l'opération itérative de l'équation (5), définie par les formules

$$\begin{cases} s_1 = u, \quad t_1 = v \\ s_{n+1} = s_1 s_n + a t_1 t_n, \quad t_{n+1} = s_1 t_n + t_1 s_n, \end{cases} \tag{8}$$

de sorte que nous aurons, quel que soit l'indice n,

$$s_n^2 - a t_n^2 = (-1)^{n\delta}\omega^n, \tag{9}$$

équation qui est toujours résoluble, pourvu que (5) le soit, et pourvu que ω soit impair.

Soit, au contraire, le paramètre ω un nombre pair, il faut supprimer, dans l'équation (9), une certaine puissance de 2, qui est diviseur commun de s_n, t_n, ω. Et, dans ce cas, l'équation (9) présente, à ce point de vue, des difficultés singulières, nous le verrons dans ce qui suit.

Quoi qu'il en soit, on aura, comme dans la théorie de l'équation de Fermat,

$$(10) \quad \begin{cases} s_{nr} = \sum\limits_{\mu=0}^{\leqq \frac{n}{2}} \binom{n}{2\mu} a^{\mu} t_r^{2\mu} s_r^{n-2\mu} \\ t_{nr} = \sum\limits_{\mu=0}^{\leqq \frac{n-1}{2}} \binom{n}{2\mu+1} a^{\mu} t_r^{2\mu+1} s_r^{n-2\mu-1}, \end{cases}$$

formules qui sont valables, quels que soient les deux indices n et r.

Cela posé, nous aurons immédiatement les congruences suivantes

$$(11) \quad \begin{cases} s_{nr} \equiv s_r^n \pmod{a}, \quad t_{nr} \equiv n\, t_r\, s_r^{n-1} \pmod{a}, \\ s_{2nr+r} \equiv 0 \pmod{s_r}, \quad s_{2nr} \equiv a^n t_r^{2n} \pmod{s_r}, \\ t_{nr} \equiv 0 \pmod{t_r}, \quad s_{nr} \equiv s_r^n \pmod{t_r}, \end{cases}$$

congruences qui sont analogues à celles connues de la théorie de l'équation de Fermat, et qui donnent des éclaircissements essentiels sur l'opération itérative.

Ici nous nous bornerons à indiquer la proposition suivante, tirée directement de la première des congruences (11), en y posant $r = 1$:

I. Soit k un diviseur de la base a, qui est premier avec t_1, les deux congruences

$$(12) \qquad t_n \equiv 0 \pmod{k}, \quad n \equiv 0 \pmod{k}$$

sont équivalentes.

Posons ensuite, dans les formules (10), $r = 1$, puis remplaçons n par le nombre premier impair

$$(13) \qquad p = 2r + 1,$$

les congruences

$$\binom{p}{\mu} \equiv 0 \pmod{p}, \quad 1 \leqq \mu \leqq p-1,$$

donnent immédiatement, en vertu du théorème de FERMAT,

(14) $$s_p \equiv s_1 \pmod p,$$

congruence qui est valable, quels que soient du reste a et p.

De plus, supposons que le nombre premier p en question ne divise pas la base a, nous aurons

(15) $$t_p \equiv \left(\frac{a}{p}\right) t_1 \pmod p,$$

où

$$\left(\frac{a}{p}\right) = \pm 1 \equiv a^{\nu} \pmod p$$

désigne, comme ordinairement, le symbole de LEGENDRE.

Les congruences ainsi obtenues sont fondamentales pour nos recherches suivantes, mais leurs applications exigent des recherches ultérieures sur l'opération itérative.

II. Le paramètre est un nombre impair.

La définition générale de l'opération itérative donnera immédiatement les formules récursives générales

(1) $$s_{n+p} = s_n s_p + a t_n t_p, \quad t_{n+p} = s_n t_p + t_n s_p,$$

analogues à celles connues de la théorie des équations de FERMAT et de LAGRANGE.

Résolvons maintenant par rapport à s_n et t_n les deux équations (1), puis remplaçons n par $n-p$, il résulte, en vertu de la formule (9) de l'article précédent,

(2) $$\begin{cases} s_n s_p - a t_n t_p = (-1)^{p\delta} \omega^p s_{n-p} \\ s_p t_n - t_p s_n = (-1)^{p\delta} \omega^p t_{n-p} \end{cases}$$

où il faut supposer, bien entendu, $n > p$.

Posons ensuite, à cause des applications suivantes,

$$n + p = \mu + 2\nu, \quad n - p = \mu,$$

ce qui donnera

$$n = \mu + \nu, \quad p = \nu,$$

nous aurons, en ajoutant les formules (1) et (2) ainsi obtenues,

$$(3) \qquad \begin{cases} s_{\mu+2\nu} + (-1)^{\nu\delta}\omega^{\nu} s_{\mu} = 2 s_{\nu} s_{\mu+\nu} \\ t_{\mu+2\nu} + (-1)^{\nu\delta}\omega^{\nu} t_{\mu} = 2 t_{\nu} t_{\mu+\nu}, \end{cases}$$

tandis qu'il résulte, en soustrayant les formules susdites,

$$(4) \qquad \begin{cases} s_{\mu+2\nu} - (-1)^{\nu\delta}\omega^{\nu} s_{\mu} = 2 a t_{\nu} t_{\mu+\nu} \\ t_{\mu+2\nu} - (-1)^{\nu\delta}\omega^{\nu} t_{\mu} = 2 t_{\nu} s_{\mu+\nu}. \end{cases}$$

Introduisons maintenant, dans les formules (3) et (4),

$$\mu = 1 \quad \nu = \frac{p-1}{2},$$

où p est un nombre premier impair qui ne divise pas la base a, nous avons à étudier séparément les cas suivants:

1° ν est un nombre pair, savoir $p = 4k+1$; les premières formules (3) et (4) se présentent sous la forme

$$s_p + \omega^{\nu} s_1 = 2 s_{\nu} s_{\nu+1}$$

$$s_p - \omega^{\nu} s_1 = 2 a t_{\nu} t_{\nu+1},$$

ce qui donnera

$$(5) \qquad \begin{cases} t_{\frac{p-1}{2}} t_{\frac{p+1}{2}} \equiv 0 \pmod{p} \\ t_{p-1} t_{p+1} \equiv 0 \pmod{p}, \end{cases}$$

selon que a est résidu ou non-résidu de p.

2° ν est impair, ce qui donnera $p = 4k+3$; les formules fondamentales deviennent ici

$$s_p - \omega^{\nu} s_1 = 2 s_{\nu} s_{\nu+1}$$

$$s_p + \omega^{\nu} s_1 = 2 a t_{\nu} t_{\nu+1},$$

de sorte que nous retrouvons les congruences (5), valables selon que ω est non-résidu ou résidu de p.

Cela posé, nous avons encore à étudier le cas, où le nombre premier p divise la base a, sans diviser bien entendu t_1; car dans ce cas, ω est de la hauteur 1 par rapport à la base ak^2.

Or, la proposition I de l'article précédent donnera immédiatement

$$t_p \equiv 0 \pmod p, \tag{6}$$

de sorte qu'il résulte, en vertu de (5) et (6), la proposition générale:

I. Soit p un nombre premier impair qui ne divise pas t_1, mais quelconque du reste, nous aurons toujours la congruence

$$t_\varrho \equiv 0 \pmod p, \tag{7}$$

où ϱ est une aliquote de $p(p^2-1)$.

Supposons ensuite que le nombre impair k soit décomposé en facteurs premiers comme suit

$$k = p_1^{\alpha_2} p_2^{\alpha_2} \dots p_n^{\alpha_n}, \tag{8}$$

nous aurons, en vertu de la proposition précédente,

$$t_\varrho \equiv 0 \pmod k, \tag{9}$$

où l'indice ϱ est une aliquote du nombre

$$\Omega = k(p_1^2-1)(p_2^2-1) \dots (p_n^2-1), \tag{10}$$

ce qui donnera le théorème fondamental:

II. La hauteur du paramètre impair ω par rapport à la base ak^2, où k est impair, est une aliquote du nombre Ω, défini par la formule (10).

On voit que le nombre Ω ne dépend ni de la base a ni du paramètre ω, mais, bien entendu, la détermination exacte de la hauteur, qui est un problème assez difficile, exige la connaissance de ces deux nombres.

Supposons que l'équation de LAGRANGE

$$u^2 - a v^2 = (-1)^{\delta} \omega, \tag{11}$$

dont il s'agit, soit d'un genre plus élevé que 2, les différents couples de ses suites coordonnées ont généralement des hauteurs inégales par rapport à la base ak^2.

Soit par exemple

$$a = 2, \quad k = 5,$$

la base 50 a la hauteur absolue 2.

Le couple de suites coordonnées auquel appartient la solution (u, v) est de la hauteur 1, pourvu qu'un des nombres

$$v, \quad u \pm v$$

soit multiple de 5, mais de la hauteur 2, pourvu qu'un des nombres

$$u, \quad u \pm 2v$$

ait cette propriété.

Soit, comme second exemple,

$$a = 13, \quad k = 5,$$

la base 325 a la hauteur absolue 6.

Il résulte, en vertu des congruences

$$\begin{aligned} s_3 &= u^3 + 39 u v^2 \equiv u (u^2 - v^2) \pmod 5 \\ t_3 &= 3 u^2 v + 13 v^3 \equiv 3 v (u^2 + v^2) \pmod 5, \end{aligned}$$

que le couple de suites coordonnées, auquel appartient la solution (u, v), est de la hauteur 1, 2, 3, 6 selon que

$$v, \quad u, \quad u^2 + v^2, \quad u^2 - v^2$$

est divisible par 5.

III. Le paramètre est un nombre pair.

Dans l'étude de l'équation de LAGRANGE au paramètre pair, savoir l'équation

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

où ω est supposé impair, nous ne trouvons aucun théorème général, parce qu'il faut considérer séparément les trois cas suivants:

1° $r = 1$; dans ce cas, l'opération itérative donnera

$$\left\{\begin{aligned} s_{2n}^2 - a\, t_{2n}^2 &= \omega^{2n} \\ s_{2n+1}^2 - a\, t_{2n+1}^2 &= (-1)^{\delta}\, \omega^{2n+1}. \end{aligned}\right. \tag{2}$$

2° $r = 2$; ici nous aurons

$$\left\{\begin{aligned} s_{3n\pm1}^2 - a\, t_{3n\pm1}^2 &= (-1)^{n\delta\pm\delta}\, 4\, \omega^{3n\pm1} \\ s_{3n}^2 - a\, t_{3n}^2 &= (-1)^{n\delta}\, \omega^{3n}. \end{aligned}\right. \tag{3}$$

3° $r \geqq 3$, hypothèse qui donnera

$$s_n^2 - a\, t_n^2 = (-1)^{n\delta}\, 2^{nr-2n+2}\, \omega^n, \tag{4}$$

et il est évident que les résultats généraux, en ce qui concerne la congruence

$$t_n \equiv 0 \pmod{k}, \tag{5}$$

où k est nécessairement impair, obtenus dans l'article précédent, sont applicables aussi dans ce cas; c'est-à-dire que le théorème II de l'article précédent n'a aucune analogie, dans les deux premiers cas que nous venons de considérer.

Cela posé, il est évident que le nombre premier 2 ne présente, à ce point de vue, aucune analogie avec les nombres premiers impairs, mais qu'il faut le remplacer par 8.

En effet, supposons résoluble l'équation de Lagrange

$$u^2 - a v^2 = (-1)^{\delta} 8, \tag{6}$$

l'opération itérative du n-ième ordre conduira, quel que soit n, à cette autre équation résoluble

$$s_n^2 - a t_n^2 = (-1)^{n\delta} 2^{n+2}. \tag{7}$$

Supposons donc résoluble l'équation

$$u^2 - a v^2 = (-1)^{\delta} 2^n, \quad n \geqq 3, \tag{8}$$

tandis qu'aucune puissance inférieure de 2 n'est applicable comme paramètre de la base a, nous disons que 2 est de la hauteur $n-2$ par rapport à la base a.

Quant à l'équation (4), supposons résoluble cette autre équation

$$\alpha^2 - a \beta^2 = (-1)^{\varepsilon} 2^{\mu}, \quad \mu \geqq 3, \tag{9}$$

nous avons à démontrer la proposition:

I. Il existe une infinité d'exposants n qui admettent la résolution de l'équation

$$u^2 - a v^2 = (-1)^{\varphi} (2^r \omega)^n. \tag{10}$$

En effet, l'opération itérative de l'ordre m donnera, en vertu de (9),

$$\sigma_m^2 - a \tau_m^2 = (-1)^{m\varepsilon} 2^{\mu m - 2m + 2}; \tag{11}$$

multiplions ensuite les équations (4) et (11), nous aurons, en choisissant convenablement le signe appliqué dans cette multiplication, une équation de la forme

$$u^2 - a v^2 = (-1)^{n\delta + m\varepsilon} 2^{nr - 2n + \mu m - 2m + 2} \omega^n,$$

de sorte qu'il s'agit de déterminer m et n, tels que

$$2(u-1) = m(\mu - 2), \tag{12}$$

ce qui donnera une infinité de valeurs du couple (m, n).

Mais, les nombres v tirés de l'équation (10) présentent-ils des multiples du nombre impair k?

A cet effet, supposons que t_n et τ_m soient tous deux multiples de k, de sorte que n et m sont les plus petits indices qui correspondent à cette propriété, il est évident que les nombres $t_{n\varkappa}$ et $\tau_{m\lambda}$ sont aussi multiples de k, quels que soient les positifs entiers $\varkappa$ et λ; c'est-à-dire que nous aurons, en vertu de (12), à résoudre l'équation indéterminée

$$\mu(m\varkappa - 2) = 2(n\nu - 1), \tag{13}$$

équation qui n'est pas généralement résoluble en positifs entiers de $\varkappa$ et λ.

Quant au problème qui nous occupe ici, nous démontrerons encore la proposition:

II. *Il existe une infinité d'exposants n qui permettent de résoudre l'équation*

$$u^2 - a v^2 = (-1)^{\varepsilon} \omega^n. \tag{14}$$

En effet, il résulte des formules (4) et (9) que l'équation (14) est résoluble, pourvu que m et n satisfassent à l'équation

$$m(s-2) = n(\nu - 2),$$

équation qui est toujours résoluble en positifs entiers.

IV. Sur le facteur $k = 2^n$.

Le facteur

$$k = 2^n$$

a aussi, comme il était à prévoir, des propriétés singulières.

En effet, supposons que le nombre premier 2 soit, par rapport à la base a, du rang σ, nous aurons nécessairement

$$\sigma = 1,\ 2;$$

car le nombre

$$B_2 = 2 A_1 B_1$$

est toujours pair. Soit donc

$$B_\sigma = 2^\varkappa (2l+1), \tag{1}$$

tandis que

$$\tau = 2^\lambda \sigma,$$

on aura

$$B_\tau = 2^{\varkappa+\lambda} (2l_1+1); \tag{2}$$

c'est-à-dire qu'il existe des nombres B_n divisibles par une puissance quelconque de 2, dont l'exposant est plus grand que $\varkappa$.

Quant à l'équation de Lagrange

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

il n'est pas sûr qu'aucun des nombres v ne soit pair. Mais supposons que

$$2^\nu, \quad \nu \geqq 0,$$

soit la plus petite puissance de 2 qui divise un nombre v tiré de l'équation (3), savoir

$$v = 2^\nu (2\alpha + 1), \tag{4}$$

puis supposons $\nu \geqq \varkappa$, il existe un indice ϱ, tel que

$$B_\varrho = 2^\nu (2\beta + 1);$$

c'est-à-dire que les nombres

$$v A_\varrho \pm u B_\varrho$$

sont tous deux divisibles par $2^{\nu+1}$, et ainsi de suite, de sorte que nous aurons la proposition curieuse:

I. S o i t, d a n s l e s f o r m u l e s (1) e t (4), $\nu \geqq \varkappa$, l'é q u a t i o n

$$u^2 - (2^n a) v^2 = (-1)^\varphi \omega \tag{5}$$

e s t t o u j o u r s r é s o l u b l e, q u e l q u e s o i t l'e x p o s a n t n.

Supposons maintenant $\nu < \varkappa$, toutes les valeurs paires de v, appartenant au même couple de suites coordonnées, sont précisément divisibles par la puissance 2^ν, de sorte que ces nombres sont tous de la forme (4).

Appliquons maintenant l'opération itérative du second ordre, nous trouvons des nombres t_2 précisément divisibles par $2^{\nu+1}$, et ainsi de suite, ce qui donnera des $t_{\varkappa-\nu+1}$ qui sont divisibles par $2^\varkappa$, de sorte que la proposition I est applicable.

V. Sur les bases $2^{2n}+1$.

La première des Tables numériques jointes au présent Mémoire exige des éclaircissements sur les bases

(1) $$a = 2^{2n}+1, \quad n \geqq 2.$$

A cet effet, remarquons tout d'abord que

(2) $$\omega = 2^{n+1}$$

est la plus petite valeur du paramètre ω qui permet de résoudre l'équation de LAGRANGE

(3) $$u^2 - a v^2 = \pm \omega,$$

de sorte que le nombre premier 2 est par rapport à la base a de la hauteur $n-1$, il est facile de démontrer la proposition:

I. Supposons résoluble l'équation

(4) $$u^2 - a v^2 = \pm 2^r p, \quad 3 \leqq r \leqq n,$$

où p est un nombre premier impair, la hauteur de p par rapport à la base a est diviseur de $n-1$.

En effet, posons

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

l'opération itérative de l'ordre μ donnera

$$s_\mu^2 - a t_\mu^2 = \pm 2^{\mu n - \mu + 2}, \tag{5}$$

tandis que l'opération de l'ordre ν donnera, en vertu de (4),

$$s_\nu^2 - a t_\nu^2 = \pm 2^{\nu r - 2\nu + 2} p^\nu, \tag{6}$$

et il nous reste à déterminer μ et ν, de sorte que les deux puissances de 2 qui figurent aux seconds membres de (5) et (6) auront le même exposant, ce qui exige

$$(n-1)\mu = (r-2)\nu. \tag{7}$$

Soit maintenant f le plus grand commun diviseur de $n-1$ et $r-2$, et soient

$$n-1 = n_1 f, \quad r-2 = r_1 f,$$

il résulte, en vertu de (7),

$$n_1 \mu = r_1 \nu,$$

de sorte que ν est nécessairement multiple de n_1, donc p est de la hauteur n_1 par rapport à la base a, et n_1 est bien diviseur de $n-1$.

Il résulte de la formule (7) que p est precisément de la hauteur $n-1$, pourvu que $r = 3$.

Soit ensuite

$$n-1 = 2^\varrho,$$

toutes les hauteurs en question sont des puissances de 2, et leurs exposants sont au plus égaux à ϱ.

Posons par exemple $n = 5$, ce qui donnera

$$a = 2^{10} + 1 = 1025 = 41 \cdot 5^2,$$

puis partons de l'équation

$$u^2 - 41 v^2 = \pm \omega, \tag{8}$$

supposée résoluble, ω est de la hauteur 1, 2, 4 par rapport à 1045, selon que v, u, $u \pm 7v$ est multiple de 5.

En effet, soit ni u ni v divisible par 5, il est possible de choisir le signe, de sorte que

$$u \pm 7v \equiv u \pm 2v \pmod 5$$

devienne multiple de 5, et la multiplication de l'équation (8) par celle-ci

$$7^2 - 41 \cdot 1^2 = 8$$

donnera

$$(7u \pm 41v)^2 - 41(v \pm 7u)^2 = \pm 8\omega.$$

La Table Première, contenant les solutions des équations résolubles de la forme (8), permet donc de déterminer immédiatement la hauteur de ω par rapport à la base 1045.

Quant aux bases spéciales qui nous occupent ici, nous avons encore à démontrer deux autres propositions, savoir:

II. Supposons $3 \leqq \sigma \leqq n$, il existe une infinité d'équations résolubles de la forme

$$u^2 - av^2 = \pm 2^\sigma(2\varkappa + 1). \tag{9}$$

En effet, partons de l'équation

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

puis posons

$$u = 2^s k + 1, \quad v = 1, \quad s \geqq 2, \tag{10}$$

où k est un nombre impair, nous aurons

$$\pm \omega = (2^{2n} + 1) - (2^s k + 1)^2, \tag{11}$$

ou, ce qui est la même chose,

$$\pm \omega = 2^{s+1}(2^{2n-s-1} - 2^{s-1}k - k), \tag{12}$$

et ce paramètre est précisément de la forme susdite, de sorte qu'il ne nous reste qu'à démontrer que l'équation (9), ainsi obtenue soit résoluble; c'est-à-dire que a et ω ou a et u sont premiers entre eux.

Or, choisissons arbitrairement le nombre impair k, puis supposons que a et $2^s k+1$ ne soient pas premiers entre eux, il est évident que a et $2^s(k+2)+1$ auront nécessairement cette propriété, parce que tous les facteurs communs de a et $2^s k+1$ sont impairs.

III. Supposons que la base a soit résidu quadratique du nombre premier impair p, puis supposons donné l'exposant s qui figure dans la formule (10), il est possible de déterminer le nombre impair k, tel que le paramètre ω, défini par la formule (12), soit multiple de p.

En effet, il existe un positif entier b, de sorte que

$$2^{2n}+1 \equiv b^2 \pmod{p},$$

ce qui donnera, en vertu de (11),

$$\pm\omega \equiv b^2-(2^s k+1) \equiv 0 \pmod{p},$$

ou, ce qui est la même chose,

$$2^s k \equiv b^2-1 \pmod{p}, \tag{13}$$

congruence qui est toujours résoluble, parce que 2^s et p sont premiers entre eux.

Soit ensuite k_1 une solution quelconque de (13), la solution générale de cette congruence se présente sous la forme

$$k = k_1+pm, \tag{14}$$

où m est un entier quelconque, et il est évident que la formule (14) détermine une infinité de valeurs impaires de k.

CHAPITRE II

Sur les nombres A_n et u_n.

VI. Résidus par rapport à la base.

Dans ce qui suit, nous avons souvent besoin des résidus obtenus en divisant par la base a les nombres A_n et u_n, tirés de l'équation de FERMAT

(1) $$A_\mu^2 - a B_\mu^2 = (-1)^{\mu\varepsilon}$$

et de l'équation de LAGRANGE

(2) $$u_\lambda^2 - a v_\lambda^2 = (-1)^{\delta_\lambda} \omega;$$

c'est pourquoi il nous semble utile d'étudier plus profondément de tels résidus.

A cet effet, partons de la formule de LAGRANGE

(3) $$A_{2\mu} = 2\,\partial B_\mu^2 + (-1)^{\mu\varepsilon},$$

nous aurons immédiatement la congruence fondamentale

(4) $$A_{2\mu} \equiv (-1)^{\mu\varepsilon} \pmod{a},$$

de sorte que la formule récursive de LAGRANGE

(5) $$A_{\lambda+2\mu} = A_\lambda A_{2\mu} + a B_\lambda B_{2\mu}$$

conduira à la congruence générale

(6) $$A_{\lambda+2\mu} \equiv (-1)^{\mu\varepsilon} A_\lambda \pmod{a},$$

valable quels que soient les indices λ et μ.

Or, il est bien curieux, ce me semble, que les nombres u_λ, tirés d'une suite quelconque des solutions de (2), satisfont à une congruence analogue à (6).

En effet, la formule récursive

$$u_{\lambda+2\mu} = u_\lambda A_{2\mu} + a v_\lambda B_{2\mu} \tag{7}$$

donnera, en vertu de (4),

$$u_{\lambda+2\mu} \equiv (-1)^{\mu\varepsilon} u_\lambda \pmod{a}, \tag{8}$$

de sorte qu'il s'agit de déterminer seulement les résidus des deux nombres u_1 et u_2 pour connaître les résidus de tous les nombres u_n appartenant à la même suite de solutions.

Supposons ensuite $\omega > 2$, puis désignons par (u'_n, v'_n) l'élément général de la suite coordonnée à la précédente, nous aurons, en désignant par λ et μ les deux indices 1 et 2, pris dans un ordre quelconque,

$$u_\lambda u'_\mu + a v_\lambda v'_\mu = \omega A_2$$
$$v_\lambda u'_\mu + v_\mu u'_\lambda = \omega B_2,$$

ce qui donnera

$$(-1)^\delta u'_\mu = u_\lambda A_2 - a v_\lambda B_2$$
$$(-1)^\delta v'_\mu = u_\lambda B_2 - v_\lambda A_2,$$

où nous avons posé

$$u_\lambda^2 - a v_\lambda^2 = (-1)^\delta \omega, \quad \lambda = 1, 2, \tag{9}$$

de sorte qu'il résulte finalement, en vertu de (4),

$$u'_\mu \equiv (-1)^{\delta+\varepsilon} u_\lambda \pmod{a}; \tag{10}$$

c'est-à-dire que nous venons de démontrer la proposition curieuse:

I. Les restes modulo a de tous les nombres u_m et u'_n, appartenant au même couple de suites coordonnées, sont connus, pourvu que les restes des deux premiers nombres u_1 et u_1' le soient.

Posons maintenant

$$(11) \qquad u_\lambda = a k_\lambda + (-1)^\varrho r, \quad 0 < r < a,$$

le nombre r joue un rôle fondamental, dans la résolution numérique de l'équation (9).

En effet, il résulte, en vertu de (9) et (11),

$$(12) \qquad (-1)^\delta \omega \equiv r^2 \pmod{a},$$

de sorte que $(-1)^\delta \omega$ est nécessairement résidu quadratique de a; posons ensuite

$$(13) \qquad (-1)^\delta \omega = r^2 + s a,$$

nous aurons, en vertu de (9) et (11),

$$(14) \qquad a k_\lambda^2 \pm 2 r k_\lambda - s = v_\lambda^2;$$

c'est-à-dire qu'il faut déterminer le nombre k_λ, tel que le premier membre de (14) devienne un carré exact, et l'équation (9) est résolue.

Quant au quotient k_λ, la formule récursive (7) donnera, en vertu de (3),

$$u_{\lambda+2\nu} = 2 a u_\lambda B_\nu^2 + a v_\lambda B_{2\nu} + (-1)^{\nu\varepsilon} u_\lambda,$$

ou, ce qui est la même chose,

$$u_{\lambda+2\nu} = 2 a B_\nu u_{\lambda+\nu} + (-1)^{\nu\varepsilon} u_\lambda.$$

Posons donc, conformément à (11),

$$(15) \qquad u_{\lambda+2\nu} = a k_{\lambda+2\nu} + (-1)^{\lambda+\nu\varepsilon} r,$$

il résulte, pour les coefficients k_n, la formule récursive

$$(16) \qquad k_{\lambda+2\nu} = 2 B_\nu u_{\lambda+\nu} + (-1)^{\nu\varepsilon} k_\lambda.$$

Quant à la suite coordonnée, nous aurons, en vertu de (9),

$$(-1)^{\delta} u'_{\mu} = a(2B_1^2 u_{\lambda} - B_2 v_{\lambda}) + (-1)^{\varepsilon} u_{\lambda},$$

de sorte que le quotient k'_{μ}, défini par la formule

$$u'_{\mu} = a k'_{\mu} + (-1)^{\delta+\varepsilon+\varrho} r,$$

se détermine par l'expression

$$(17) \qquad (-1)^{\delta} k'_{\mu} = 2B_1(u_{\lambda} B_1 - v_{\lambda} A_1) + (-1)^{\varepsilon} k_{\lambda}.$$

Choisissons maintenant les nombres u_{λ} et u'_{μ}, tels que $\lambda = 1$, $\mu = 2$, il résulte finalement

$$(18) \qquad k'_2 = 2u'_1 B_1 + (-1)^{\delta+\varepsilon} k_1.$$

VII. Sur les bases de seconde espèce.

Les deux congruences (6) et (8) de l'article précédent se présentent sous forme élégante, pourvu que a soit une base de seconde espèce; car, dans ce cas, l'exposant ε est un nombre pair, de sorte que les congruences susdites se présentent sous la forme

$$(1) \qquad A_{2\nu} \equiv 1 \pmod{a}$$

$$(2) \qquad u_{\lambda+2\nu} \equiv u_{\lambda} \pmod{a},$$

congruences qui sont valables, quels que soient les indices λ et ν.

Quant aux résidus des deux nombres

$$A_{2\nu+1}, \; u_{\lambda+2\nu+1},$$

nous ne savons dès à présent rien, pour une valeur quelconque de la base a. Mais, désignons pour abréger a comme une base $4k+3$ de première ou de seconde classe, selon que l'équation

(3) $$u^2 - a v^2 = (-1)^{k-1} 2, \quad a = 4k+3$$

soit résoluble ou non, il est facile de démontrer la proposition:

I. Supposons satisfaite, pour des valeurs convenables des exposants δ et ε, une seule des deux congruences

(4) $$A_{2\nu+1} \equiv (-1)^{\delta} \pmod{a}$$

(5) $$u_{\lambda+2\nu+1} \equiv (-1)^{\varepsilon} u_{\lambda} \pmod{a},$$

la seconde est aussi applicable, et a est une base $4k+3$ de première classe, et inversement.

Partons tout d'abord de la congruence (4), il existe, en vertu de la congruence (6) de l'article précédent, un exposant μ, tel que

(6) $$A_1 \equiv (-1)^{\mu} \pmod{a},$$

congruence qui est impossible, à moins que a ne soit une base de seconde espèce, de sorte que l'équation de FERMAT correspondante se présente sous la forme

(7) $$(A_1 + 1)(A_1 - 1) = a B_1^2.$$

Quant à cette équation, nous supposons que a soit une base réduite, savoir qu'elle ne contient aucun facteur quadratique.

Supposons ensuite que A_1 soit un nombre pair, les deux facteurs qui figurent au premier membre de (7) sont premiers entre eux, donc il existe une décomposition

(8) $$B_1 = \sigma\tau,$$

où σ et τ sont premiers entre eux, de sorte que l'on aura, en vertu de (6),

(9) $$A_1 - (-1)^{\mu} = a\tau^2, \quad A_1 + (-1)^{\mu} = \sigma^2,$$

ce qui conduira immédiatement à l'équation (3).

Soit, au contraire, A_1 un nombre impair, B_1 est nécessairement pair, car a est ou impair ou de la forme $4l+2$, et le terme aB_1^2 est multiple de 4. Posons donc, au lieu de (8),

$$B_1 = 2\sigma\tau, \tag{10}$$

il résulte, en vertu de (7),

$$A_1 - (-1)^\mu = 2a\tau^2, \quad A_1 + (-1)^\mu = 2\sigma^2,$$

ce qui donnera

$$\sigma^2 - a\tau^2 = (-1)^\mu,$$

équation qui est inadmissible.

En effet, l'hypothèse $\mu = 1$ est dès à présent exclue, parce que a est une base de seconde espèce, et c'est la même chose pour la valeur $\mu = 0$, car (A_1, B_1) est la plus petite solution de l'équation de Fermat en question.

Inversement, partons de l'équation (3), il est bien connu que l'opération itérative du second ordre donnera

$$\left(av^2 - (-1)^k\right)^2 - a(uv)^2 = 1,$$

de sorte que l'existence d'une congruence de la forme (4) est évidente.

Enfin, prenons pour point de départ la congruence (5), la formule récursive

$$u_2 = u_1 A_1 + a\nu_1 B_1$$

donnera immédiatement, pour $\lambda = 1$, $\nu = 0$.

$$(-1)^\varepsilon u_1 \equiv u_1 A_1 \pmod{a},$$

ce qui n'est autre chose que la congruence (4), parce que a et u_1 sont premiers entre eux.

Étudions maintenant le cas général, où a est une base de seconde espèce, pour laquelle l'équation (3) n'est pas résoluble.

A cet effet, supposons tout d'abord pair le nombre A_1, il existe des décompositions en deux facteurs premiers entre eux

(11) $$a = pq, \quad B_1 = \sigma\tau,$$

de sorte que

$$A_1 + (-1)^\varepsilon = p\sigma^2, \quad A_1 - (-1)^\varepsilon = q\tau^2,$$

ce qui donnera

(12) $$p\sigma^2 - q\tau^2 = (-1)^\varepsilon 2, \quad 2A_1 = p\sigma^2 + q\tau^2.$$

Soit, au contraire, A_1 un nombre impair, B_1 est pair, de sorte que nous aurons, au lieu de (11), les décompositions

(13) $$a = pq, \quad B_1 = 2\sigma\tau,$$

où p et q, σ et τ sont premiers entre eux, ce qui donnera, par le même procédé que dans le cas précédent,

(14) $$p\sigma^2 - q\tau^2 = (-1)^\varepsilon, \quad A_1 = p\sigma^2 + q\tau^2,$$

résultats qui sont bien connus.

Dans ce qui suit, nous désignons comme décomposition principale de la base a de seconde espèce la décomposition $a = pq$ que nous venons d'étudier.

Et, cette définition adoptée, nous avons à démontrer la proposition:

II. Soit $a = pq$ la décomposition principale de la base a, on aura, quels que soient les indices λ et ν,

(15) $$A_\lambda + (-1)^\varepsilon A_\nu \equiv 0 \pmod{p}, \quad A_\lambda - (-1)^\varepsilon A_\nu \equiv 0 \pmod{q}$$

(16) $$u_\lambda + (-1)^\varepsilon u_\nu \equiv 0 \pmod{p}, \quad u_\lambda - (-1)^\varepsilon u_\nu \equiv 0 \pmod{q}.$$

Quant à la démonstration de cette proposition, nous pouvons nous borner à étudier par exemple les nombres A_n.

A cet effet, la formule récursive de Lagrange donnera

$$A_\lambda \pm (-1)^\varepsilon A_{\lambda-1} = A_{\lambda-1}\left(A_1 \pm (-1)^\varepsilon\right) + a B_1 B_{\lambda-1},$$

ce qui conduira immédiatement aux congruences (15).

En remarquant que nous avons, dans le Chapitre qui suit, à généraliser beaucoup les résultats que nous venons de mentionner, nous nous bonerons ici à démontrer cette autre proposition:

III. Soit $a = 4k+1$ ou $a = 4k+2$ une base réduite de seconde espèce, la décomposition fondamentale $a = pq$ conduira toujours à une équation de la forme

$$p\sigma^2 - q\tau^2 = (-1)^\delta, \tag{17}$$

tandis que l'hypothèse $a = 4k+3$ donnera

$$p\sigma^2 - q\tau^2 = (-1)^\delta 2. \tag{18}$$

En effet, soit p et q tous deux de la forme $4l+1$ ou de la forme $4l+3$, un des nombres σ et τ est pair, ce qui donnera immédiatement une équation de la forme (17). Et c'est la même chose dans le cas où un des nombres p et q est pair, de la forme $4l+2$, le second impair de la forme $4m \pm 1$. Soit enfin $a = 4k+3$, un des facteurs p et q est de la forme $4m+1$ l'autre de la forme $4n+3$, ce qui conduira à une équation de la forme (18).

VIII. Résolution d'une équation indéterminée.

Les résultats obtenus dans les deux articles précédents, nous permettent de résoudre, en positifs entiers, l'équation indéterminée

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

où a est un positif entier donné qui n'est pas un carré exact.

On voit immédiatement que l'équation (1) se transforme en celle-ci

(2) $$(ax \pm 1)^2 - ay^2 = 1,$$

de sorte qu'il s'agit de déterminer les solutions (A_n, B_n) de l'équation de FERMAT ayant la base a, qui satisfont à la condition

(3) $$A_n \mp 1 \equiv 0 \pmod{a};$$

car, cette condition remplie, on aura comme solution de (1)

(4) $$x_n = \frac{A_n \mp 1}{a}, \quad y_n = B_n,$$

ce qui donnera les propositions suivantes:

I. Soit a une base de seconde espèce, l'équation

(5) $$ax^2 + 2x = y^2$$

est toujours résoluble, en admettant les solutions

(6) $$x_n = \frac{A_{2n} - 1}{a}, \quad y_n = B_{2n}.$$

Quant à l'équation

(7) $$ax^2 - 2x = y^2,$$

elle n'est pas généralement résoluble, pourvu que a soit une base de seconde espèce, car la résolubilité de cette équation exige la congruence

(8) $$A_1 \equiv -1 \pmod{a}.$$

Dans ce cas, on aura comme solutions de (7)

(9) $$\xi_n = \frac{A_{2n-1} + 1}{a}, \quad \eta_n = B_{2n-1}.$$

Soit ensuite a une base de seconde espèce qui satisfait à la condition

(10) $$A_1 \equiv 1 \pmod{a}$$

l'équation (5) admet aussi les solutions

$$(11) \qquad \xi_n = \frac{A_{2n-1} - 1}{a}, \quad \eta_n = B_{2n-1}.$$

II. Soit a une base de première espèce, les équations (5) et (7) sont toutes deux résolubles, en admettant les solutions

$$(12) \qquad x_n = \frac{A_{4n} - 1}{a}, \quad y_n = B_{4n}$$

respectivement

$$(13) \qquad \xi_n = \frac{A_{4n-2} + 1}{a}, \quad \eta_n = B_{4n-2}.$$

CHAPITRE III

Équations de Legendre.

IX. Propriété fondamentale des solutions.

Dans les Tables de DEGEN et de CAYLEY, on trouve beaucoup de fractions continues qui conduiront à des équations de la forme

$$(1) \qquad (p\sigma)^2 - pq\tau^2 = (-1)^{\delta} p\omega,$$

où p est le plus grand commun diviseur de deux quelconques des trois termes de cette équation.

Bien que (1) soit irrésoluble, d'après notre définition de la résolubilité d'une équation de LAGRANGE, cette équation joue néanmoins, dans la théorie des équations de LAGRANGE, un rôle si important, qu'elle mérite une étude plus approfondie.

A cet effet, remarquons tout d'abord que l'équation (1) se présente aussi sous la forme

$$(2) \qquad p\sigma^2 - q\tau^2 = (-1)^{\delta}\omega,$$

où deux quelconques des trois coefficients p, q, ω sont premiers entre eux, nous désignons comme résoluble une telle équation, pourvu qu'elle soit satisfaite par des positifs entiers σ et τ, premiers entre eux.

On voit que (2) est une généralisation directe des équations considérées dans l'article VII; c'est pourquoi nous désignons comme équations de Legendre les équations (2); car les équations spéciales susdites jouent un rôle assez important dans les travaux de ce géomètre français, aussi distingué que modeste, mais souvent trop peu apprécié.

Quant à l'équation (2), nous supposons toujours

$$q > p > 1,$$

parce que l'hypothèse $p = 1$ conduira à l'équation de Lagrange ayant la base q. Du reste, nous pouvons permuter simultanément p et q, σ et τ, pourvu que l'exposant δ soit remplacé par $\delta + 1$.

De plus, nous disons pour abréger que l'équation (2), supposée résoluble, et le paramètre correspondant ω appartiennent à la décomposition

$$a = pq$$

de la base a.

Ces définitions adoptées, nous avons à démontrer que les équations de Legendre sont en quelque mesure analogues à celles de Lagrange.

Et, à cet effet, nous démontrerons tout d'abord le lemme fondamental:

I. Une solution quelconque de l'équation (2) est toujours élément d'une suite infinie de solutions de l'équation susdite.

Quant à la démonstration de ce lemme, nous multiplions (1) par l'équation de Fermat correspondante

$$A_n^2 - aB_n^2 = (-1)^{n\varepsilon}, \quad a = pq, \tag{3}$$

ce qui donnera, après la suppression du facteur commun p,

$$\begin{cases} p(\sigma A_n + (-1)^\varrho q\tau B_n)^2 - q(p\sigma B_n + (-1)^\varrho \tau A_n)^2 = \\ \qquad = (-1)^{\delta + n\varepsilon}\,\omega, \end{cases} \tag{4}$$

équation qui est de la même forme que (2), de sorte qu'il ne s'agit que de démontrer que les deux nombres

$$(5) \qquad \sigma A_n + (-1)^\varrho q \tau B_n, \quad p\sigma A_n + (-1)^\varrho \tau A_n$$

sont premiers entre eux, pourvu que σ et τ le soient, tandis que l'exposant ϱ est un nombre quelconque, pair ou impair.

A cet effet, nous supposons $n = 1$, et nous écrivons les formules (5), ainsi obtenues, sous la forme

$$(6) \quad \sigma_m = A_1 \sigma_{m-1} + B_1 q \tau_{m-1}, \quad \tau_m = B_1 p \sigma_{m-1} + A_1 \tau_{m-1}.$$

Cherchons ensuite, de ces deux équations, les valeurs de σ_{m-1} et τ_{m-1}, il résulte, en vertu de (3),

$$(7) \quad (-1)^\varepsilon \sigma_{m-1} = A_1 \sigma_m - B_1 q \tau_m, \quad (-1)^\varepsilon \tau_{m-1} = A_1 \tau_m - B_1 p \sigma_m,$$

et il est évident que σ_m et τ_m sont premiers entre eux, pourvu que σ_{m-1}, et τ_{m-1} le soient, et inversement.

De plus, nous aurons évidemment

$$(8) \qquad \sigma_m > \sigma_{m-1}, \quad \tau_m > \tau_{m-1};$$

c'est-à-dire qu'une solution quelconque (σ, τ) de l'équation (2) est élément d'une suite infinie

$$(9) \qquad (\sigma_1, \tau_1) \; (\sigma_2, \tau_2) \; (\sigma_3, \tau_3) \; \ldots . \; (\sigma_n, \tau_n) \; \ldots .$$

de solutions de l'équation susdite.

Dans l'article qui suit, nous avons à étudier plus profondément la nature des suites ainsi obtenues.

X. Suites fermées et suites coordonnées.

Revenons maintenant aux formules (7) de l'article précédent, savoir

$$(1) \quad (-1)^\varepsilon \sigma_{m-1} = A_1 \sigma_m - B_1 q \tau_m, \quad (-1)^\varepsilon \tau_{m-1} = A_1 \tau_m - B_1 p \sigma_m,$$

où nous avons posé

$$A_1^2 - aB_1^2 = (-1)^\varepsilon, \quad a = pq, \tag{2}$$

il est évident que ces formules sont inapplicables pour $m = 1$, bien que les expressions qui figurent aux seconds membres de ces formules satisfassent à l'équation de Legendre

$$p\sigma^2 - q\tau^2 = (-1)^{\delta+\varepsilon}\,\omega. \tag{3}$$

Cela posé, nous avons à étudier, comme dans la théorie des équations de Lagrange, les deux hypothèses suivantes:

1°. La solution (s_1, t_1), définie par les nombres qui figurent aux seconds membres des formules (1), appartient à la même suite que (σ_1, τ_1), ce qui donnera nécessairement

$$s_1 = \sigma_1, \quad t_1 = \tau_1,$$

d'où il résulte, en vertu de (1),

$$\left(A_1 + (-1)^\varepsilon\right)\sigma_1 = qB_1\tau_1, \quad \left(A_1 - (-1^\varepsilon)\right)\tau_1 = p\sigma_1 B_1; \tag{4}$$

car il est évident que les facteurs de σ_1 et τ_1 qui figurent aux premiers membres de ces formules sont inégaux.

Or, les formules (4) donnent immédiatement

$$A_1^2 - aB_1^2 = 1,$$

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

De plus, il résulte de (4) que B_1 est multiple des deux nombres σ_1 et τ_1, premiers entre eux, de sorte que nous aurons

$$B_1 = k\sigma_1\tau_1, \tag{5}$$

où k est un positif entier; donc il résulte, en vertu de (4),

$$A_1 + (-1)^\varepsilon = kq\tau^2, \quad A_1 - (-1)^\varepsilon = kp\sigma_1^2, \tag{6}$$

ce qui donnera

$$k(p\sigma_1^2 - q\tau_1^2) = (-1)^{\varepsilon+1}\,2,$$

et cette équation n'est possible que pour les deux valeurs

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

Soit maintenant $k = 1$, on aura

$$(7) \qquad \begin{cases} p\sigma_1^2 - q\tau_1^2 = (-1)^{\delta}\,2 \\ 2A_1 = p\sigma_1^2 + q\tau_1^2, \quad B_1 = \sigma_1\tau_1, \end{cases}$$

tandis que l'hypothèse $k = 2$ donnera

$$(8) \qquad \begin{cases} p\sigma_1^2 - q\tau_1^2 = (-1)^{\delta} \\ A_1 = p\sigma_1^2 + q\tau_1^2, \quad B_1 = 2\sigma_1\tau_1. \end{cases}$$

Introduisons ensuite, dans (6), les deux valeurs possibles de k, il résulte la proposition:

I. La décomposition $a = pq$ est la décomposition principale de la base a.

Remarquons ensuite que les dernières équations (7) ou (8) déterminent parfaitement les nombres σ_1 et τ_1, pourvu que p et q, A_1 et B_1 soient connus, nous aurons cette autre proposition:

II. Les solutions des équations de Legendre (7) ou (8) forment une seule suite

$$(9) \qquad (\sigma_1, \tau_1)\ (\sigma_2, \tau_2)\ (\sigma_3, \tau_3)\ \ldots\ (\sigma_n, \tau_n)\ \ldots$$

Dans ce qui suit, nous désignons comme suite fermée la suite (9) ainsi définie.

2° Soit maintenant, dans l'équation (3),

$$\omega > 2,$$

la solution (σ_1, τ_1) est différente de (s_1, t_1), définie par les expressions qui figurent aux seconds membres des équations (1), qui correspondent à l'hypothèse $m = 1$.

Dans ce qui suit, nous désignons comme réciproques les deux solutions (σ_1, τ_1) et (s_1, t_1) ainsi obtenues, et comme coordonnées les deux suites dont ces solutions réciproques sont les éléments primitifs.

Quant aux suites coordonnées, nous aurons, comme dans la théorie des équations de Lagrange,

$$(10)\qquad p s_1 \sigma_1 + q t_1 \tau_1 = \omega A_1, \quad s_1 \tau_1 + t_1 \sigma_1 = \omega B_1,$$

de sorte qu'il résulte, en vertu des formules récursives,

$$(11)\quad p s_\mu \sigma_\nu + q t_\mu \tau_\nu = \omega A_{\mu+\nu-1}, \quad s_\mu \tau_\nu + t_\mu \sigma_\nu = \omega B_{\mu+\nu-1};$$

ces formules générales, valables quels que soient les indices μ et ν, sont analogues à celles connues de la théorie des équations de Lagrange.

De plus, nous désignons comme genre d'une équation de Legendre le nombre total des suites formées de ses solutions, de sorte que les équations (7) ou (8) sont du genre 1, tandis que les genres de toutes les autres équations de Legendre sont des nombres pairs.

XI. Sur la multiplication des équations de Legendre.

Le fondement d'une étude plus approfondie des équations de Legendre est, comme dans la théorie des équations de Lagrange, la multiplication de telles équations qui correspondent à la même base.

A cet effet, supposons applicables les deux décompositions (p, q) et (p_1, q_1) de la base a, savoir supposons résolubles les deux équations

$$(1)\quad p\sigma^2 - q\tau^2 = (-1)^\delta \omega, \quad p_1 \sigma_1^2 - q_1 \tau_1^2 = (-1)^{\delta_1} \omega_1$$

où nous avons posé

$$(2)\qquad a = pq = p_1 q_1,$$

la multiplication de ces deux équations, qui se présentent aussi sous la forme

$$(p\sigma)^2 - a\tau^2 = (-1)^{\delta} p\,\omega, \quad (p_1\sigma_1)^2 - a\tau_1^2 = (-1)^{\delta} p_1\,\omega_1,$$

donnera

$$(3)\quad \begin{cases} \left(pp_1\,\sigma\sigma_1 + (-1)^{\varepsilon} a\,\tau\tau_1\right)^2 - a\left(p\,\sigma\tau_1 + (-1)^{\varepsilon} p_1\,\sigma_1\,\tau\right)^2 = \\ \qquad\qquad = (-1)^{\delta+\delta_1}\,pp_1\,\omega\omega_1. \end{cases}$$

Et il est évident que les résultats formels obtenus pour les équations de Lagrange sont aussi valables pour les équations de Legendre, de sorte qu'il ne nous reste que de discuter la portée de la formule (3).

Quant à cette discussion, nous supposons que la base a se présente sous la forme

$$(4)\qquad a = p\,q\,r\,s,$$

où deux quelconques de ces quatre facteurs sont premiers entre eux, ce qui permet les hypothèses

$$s = 1, \quad r = s = 1, \quad q = r = s = 1,$$

de sorte que la base réduite a peut contenir un nombre quelconque de facteurs premiers.

Supposons ensuite résolubles les deux equations

$$(5)\quad p\,q\,\sigma^2 - r\,s\,\tau^2 = (-1)^{\delta}\,\omega, \quad p\,r\,\sigma_1^2 - q\,s\,\tau_1^2 = (-1)^{\delta_1}\,\omega_1,$$

il résulte, en vertu de (3), une égalité de la forme

$$(6)\qquad p\,s\,\sigma_2^2 - q\,r\,\tau_2^2 = (-1)^{\delta+\delta_1+1}\,\omega\,\omega_1,$$

où nous avons posé pour abréger

$$(7)\quad \sigma_2 = p\,\sigma\tau_1 + (-1)^{\varepsilon}\,r\,\sigma_1\tau, \quad \tau_2 = p\,\sigma\sigma_1 + (-1)^{\varepsilon}\,s\,\tau\tau_1.$$

Cela posé, nous avons à démontrer la proposition essentielle:

I. Un diviseur commun des deux nombres σ_2 et τ_2 est aussi diviseur commun des deux paramètres ω et ω_1.

En effet, cherchons des équations (7) les deux nombres σ et τ, il résulte, en vertu de la dernière des formules (5),

$$(-1)^{\delta_1}\omega_1\sigma = r\sigma_1\tau_2 - s\tau_1\sigma_2, \quad (-1)^{\delta_1+\varepsilon}\omega_1\tau = p\sigma_1\sigma_2 - q\tau_1\tau_2,$$

de sorte qu'un facteur commun de σ_2 et τ_2 est nécessairement diviseur de ω_1, parce que σ et τ sont premiers entre eux.

Cherchons ensuite, des équations (7), les deux nombres σ_1 et τ_1, nous verrons de même qu'un facteur commun de σ_2 et τ_2 divise aussi le paramètre ω.

Partons ensuite des deux équations

$$(8) \quad p\sigma^2 - qrs\tau^2 = (-1)^{\delta}\omega, \quad q\sigma_1^2 - prs\tau_1^2 = (-1)^{\delta_1}\omega_1,$$

nous aurons de même

$$(9) \quad pq(\sigma\sigma_1 \pm rs\tau\tau_1)^2 - rs(p\sigma\tau_1 \pm q\sigma_1\tau)^2 = (-1)^{\delta+\delta_1}\omega\omega_1,$$

et inversement, la multiplication des équations

$$(10) \quad p\sigma^2 - qrs\tau^2 = (-1)^{\delta}\omega, \quad pq\sigma_1^2 - rs\tau_1^2 = (-1)^{\delta_1}\omega_1$$

donnera

$$(11) \quad q(p\sigma\sigma_1 \pm rs\tau\tau_1)^2 - prs(\sigma\tau_1 \pm q\sigma_1\tau)^2 = (-1)^{\delta+\delta_1}\omega\omega_1.$$

Cela posé, remarquons que la proposition I est valable aussi pour ces dernières multiplications, il est évident que nous venons de démontrer une suite de propositions en ce qui concerne la multiplication des équations de LAGRANGE et de LEGENDRE, propositions desquelles nous nous bornerons à citer une seule:

II. Supposons résolubles les deux équations de Legendre

$$(12)\quad pq\sigma^2 - rs\tau^2 = (-1)^{\delta}\varrho^{\varkappa}\omega, \quad pr\sigma_1^2 - qs\tau^2 = (-1)^{\delta_1}\varrho^{\varkappa}\omega_1,$$

où ω et ω_1 sont premiers entre eux, tandis que ϱ est un nombre premier qui ne divise ni ω ni ω_1, cette autre équation

$$(13)\qquad ps\sigma^2 - qr\tau^2 = (-1)^{\delta+\delta_1+1}\omega\omega_1$$

est résoluble aussi.

Quant à la multiplication des équations de Legendre, appartenant à la même décomposition de base, nous aurons le théorème fondamental:

III. Supposons résolubles les deux équations de Legendre

$$(14)\quad p\sigma^2 - q\tau^2 = (-1)^{\delta}\omega, \; p\sigma_1^2 - q\tau^2 = (-1)^{\delta_1}\omega_1, \; pq = a,$$

où les paramètres ω et ω_1 sont premiers entre eux, l'équation de Lagrange

$$(15)\qquad u^2 - av^2 = (-1)^{\delta+\delta_1}\omega\omega_1$$

est résoluble aussi.

De plus, les formules générales donnent cette autre proposition, supplémentaire à la précédente:

IV. Supposons résolubles les deux équations

$$(16)\quad u^2 - av^2 = (-1)^{\delta}\omega, \; p\sigma^2 - q\tau^2 = (-1)^{\delta_1}\omega_1, \; a = pq,$$

où les paramètres ω et ω_1 sont premiers entre eux, l'équation de Legendre

$$(17)\qquad p\sigma^2 - q\tau^2 = (-1)^{\delta+\delta_1}\omega\omega_1$$

est résoluble aussi.

Du reste, tous les résultats généraux, en ce qui concerne la multiplication de deux équations de Lagrange, sont aussi applicables pour la multiplication ou de deux équations de Legendre ou pour les multiplications d'une équation de Lagrange et d'une équation de Legendre.

En effet, la multiplication d'un couple de suites coordonnées, appartenant à chacune des deux équations données, conduira toujours à deux couples de suites coordonnées de l'équation nouvelle, obtenues en appliquant toujours la multiplication positive, parce que la multiplication négative des suites susdites n'est autre chose que la multiplication positive des suites coordonnées.

De plus, appliquons toutes les multiplications, nous aurons trois fois deux des quatre suites de l'équation nouvelle, mais une seule fois les deux autres.

Et la proposition II donnera immédiatement le théorème fondamental:

V. Supposons que le paramètre ω de l'équation de Legendre

$$p\sigma^2 - q\tau^2 = (-1)^{\delta}\omega \tag{18}$$

contienne n facteurs premiers inégaux, le genre de cette équation est au plus égal à 2^{n-1} ou à 2^n, selon que ω est de la forme $4k+2$ ou non.

Enfin, nous avons encore à citer cette autre proposition:

VI. Supposons simultanément résolubles les deux équations de Legendre

$$p\sigma^2 - q\tau^2 = \omega, \quad p\sigma_1^2 - q\tau_1^2 = -\omega, \tag{19}$$

p et q sont tous deux une somme de deux carrés premiers entre eux.

XII. Conditions de résolubilité.

Les résultats obtenus, dans l'article précédent, rattachent la résolubilité de l'équation de Legendre

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

à l'équation de Lagrange

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

En effet, il est facile de démontrer la proposition essentielle:

I. Supposons impair le paramètre ω, la condition suffisante et nécessaire pour la résolubilité de l'équation (1) est, que l'équation (2) est résoluble, en admettant une solution de la forme

$$u = p\sigma^2 + q\tau^2, \quad v = 2\sigma\tau, \tag{3}$$

où σ et τ sont premiers entre eux.

Supposons tout d'abord résoluble l'équation (1), l'opération itérative du second ordre donnera

$$(p\sigma^2 + q\tau^2)^2 - a(2\sigma\tau)^2 = \omega^2;$$

c'est-à-dire que l'équation (2) est résoluble et admet une solution de la forme (3).

Inversement, partons de la formule (3), il est évident que l'équation quadratique

$$z^2 - 2uz + av^2 = 0 \tag{4}$$

a les deux racines

$$2p\sigma^2, \quad 2q\tau^2,$$

et nous aurons, en résolvant (4),

$$z = u \pm \sqrt{u^2 - av^2} = u \pm \omega,$$

ce qui donnera immédiatement l'équation (1).

Soit, au contraire, ω un nombre pair, nous avons à remplacer l'équation (2) par celle-ci

$$u^2 - a v^2 = \left(\frac{\omega}{2}\right)^2, \tag{5}$$

tandis que les conditions (3) deviennent

$$2u = p\sigma^2 + q\tau^2, \quad v = \sigma\tau, \tag{6}$$

et le même procédé que dans le cas précédent conduira de nouveau des formules (5) et (6) à l'équation (1).

Soit particulièrement $\omega = 1$ ou $\omega = 2$, nous retrouvons les équations considérées dans l'article VII.

Quant à la résolubilité de l'équation (1), elle se rattache aussi à l'équation indéterminée

$$pn - qm = (-1)^{\delta}\omega, \tag{7}$$

toujours résoluble, parce que p et q sont premiers entre eux.

En effet, soustrayons les deux équations (1) et (7), il résulte

$$p(\sigma^2 - n) = q(\tau^2 - m), \tag{8}$$

ce qui donnera immédiatement la proposition essentielle:

II. L'équation (1) n'est jamais résoluble, à moins que n et m, déterminés par l'équation (7), ne soient résidus quadratiques, m de p et n de q, condition nécessaire qui n'est pas toujours suffisante aussi.

Soit donc par exemple n résidu quadratique de q, il existe un positif entier r, tel que

$$r^2 \equiv n \pmod{q}, \tag{9}$$

de sorte qu'il s'agit de déterminer le nombre s, tel que

$$\sigma = qs \pm r. \tag{10}$$

A cet effet, posons

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

il résulte, en vertu de (1),

$$as^2 \pm 2prs + k = \tau^2, \tag{11}$$

et ensuite s est à déterminer, de sorte que le premier membre de l'équation (11) devienne un carré exact.

On voit que cette méthode est parfaitement analogue à celle mentionnée dans l'article VI, en ce qui concerne la résolution numérique d'une équation de LAGRANGE.

XIII. Application de l'opération itérative.

Dans mon premier Mémoire sur les équations de LAGRANGE, j'ai développé les formules fondamentales, en ce qui concerne l'opération itérative d'une équation de LAGRANGE.

Or, on voit immédiatement que ces formules sont applicables aussi sur l'équation

$$(p\sigma)^2 - a\tau^2 = (-1)^{\delta} p\omega, \quad a = pq,$$

où p est le plus grand commun diviseur de deux quelconques des trois termes; c'est-à-dire que les formules susdites qui correspondent à l'opération itérative du second ordre conduiront à des relations analogues pour l'équation de LEGENDRE

$$p\sigma^2 - q\tau^2 = (-1)^{\delta} \omega. \tag{1}$$

En effet, supposons tout d'abord impair et plus grand que l'unité le paramètre ω, puis désignons par

$$\left\{ \begin{array}{l} (s_1,\ t_1)\ (s_2,\ t_2)\ \ldots\ (s_n,\ t_n)\ \ldots \\ (\sigma_1,\ \tau_1)\ (\sigma_2,\ \tau_2)\ \ldots\ (\sigma_n,\ \tau_n)\ \ldots \end{array} \right. \tag{2}$$

deux suites coordonnées appartenant à l'équation (1), il existe deux suites coordonnées

$$(3) \quad \begin{cases} (u_1, v_1) \ (u_2, v_2) \ \ldots\ldots \ (u_n, v_n) \ \ldots\ldots \\ (u'_1, v'_1) \ (u'_2, v'_2) \ \ldots\ldots \ (u'_n, v'_n) \ \ldots\ldots \end{cases}$$

appartenant à l'équation de Lagrange

$$(4) \qquad u^2 - a v^2 = \omega^2,$$

telles que

$$(5) \qquad u_{\lambda+\mu-1} = p s_\lambda s_\mu + q t_\lambda t_\mu, \quad v_{\lambda+\mu-1} = s_\lambda t_\mu + s_\mu t_\lambda$$

$$(6) \qquad u'_{\lambda+\mu} = p \sigma_\lambda \sigma_\mu + q \tau_\lambda \tau_\mu, \quad v'_{\lambda+\mu} = \sigma_\lambda \tau_\mu + \sigma_\mu \tau_\lambda.$$

Soit particulièrement $\mu = \lambda$, nous aurons

$$(7) \qquad u_{2\lambda-1} = p s_\lambda^2 + q t_\lambda^2, \quad v_{2\lambda-1} = 2 s_\lambda t_\lambda$$

$$(8) \qquad u'_{2\lambda} = p \sigma_\lambda^2 + q \tau_\lambda^2, \quad v'_{2\lambda} = 2 \sigma_\lambda \tau_\lambda,$$

tandis que l'hypothèse $\mu = \lambda + 1$ donnera

$$(9) \qquad u_{2\lambda} = p s_\lambda s_{\lambda+1} + q t_\lambda t_{\lambda+1}, \quad v_{2\lambda} = s_\lambda t_{\lambda+1} + t_\lambda s_{\lambda+1}$$

$$(10) \qquad u'_{2\lambda+1} = p \sigma_\lambda \sigma_{\lambda+1} + q \tau_\lambda \tau_{\lambda+1}, \quad u'_{2\lambda+1} = \sigma_\lambda \tau_{\lambda+1} + \tau_\lambda \sigma_{\lambda+1}.$$

Quant à la solution primitive (u'_1, v'_1) de la seconde des suites (3), elle ne peut pas être obtenue par ces opérations, mais posons

$$(11) \qquad p s_\lambda^2 - q t_\lambda^2 = (-1)^{\delta_\lambda} \omega,$$

nous aurons, quel que soit l'indice λ,

$$(12) \qquad (-1)^{\delta_\lambda} u'_1 = p s_\lambda \sigma_\lambda - q t_\lambda \tau_\lambda$$

$$(13) \qquad (-1)^{\delta_\lambda} v'_1 = s_\lambda \tau_\lambda - \sigma_\lambda t_\lambda.$$

Soit particulièrement $\omega = 1$, les deux suites (3) coïncident avec la suite formée des solutions (A_n, B_n) de l'équation de Fermat

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

et nous aurons pour la suite (2)

$$\sigma_\lambda = s_{\lambda+1}, \quad \tau_\lambda = t_{\lambda+1}.$$

Quant à l'équation (1) dans laquelle ω est un nombre pair, nous aurons, pour $\omega > 2$,

$$(14) \quad 2\,u_{\lambda+\mu-1} = p s_\lambda s_\mu + q t_\lambda t_\mu, \; 2\,v_{\lambda+\mu-1} = s_\lambda t_\mu + s_\mu t_\lambda$$

$$(15) \quad 2\,u'_{\lambda+\mu} = p \sigma_\lambda \sigma_\mu + q \tau_\lambda \tau_\mu, \quad 2\,v'_{\lambda+\mu} = \sigma_\lambda \tau_\mu + \sigma_\mu \tau_\lambda,$$

tandis que l'hypothèse $\omega = 2$ conduira à des formules analogues, en ce qui concerne l'équation de FERMAT ayant la base a.

Dans ce qui suit, nous désignons comme l'opération quadratique les formules spéciales (7) et (8), formules qui sont intéressantes parce qu'elles montrent que les nombres $u_{2\lambda-1}$ et $u'_{2\lambda}$ sont tous de la forme

$$(16) \qquad p\,\alpha^2 + q\,\beta^2,$$

où α et β sont premiers entre eux.

Soit a une base de première espèce, les solutions (u, v) et (u', v') obtenues par l'opération quadratique épuisent toutes les solutions de l'équation (4), parce que les $(u_{2\lambda}, v_{2\lambda})$ et $(u'_{2\lambda+1}, v'_{2\lambda+1})$ correspondent à l'équation

$$u^2 - a\,v^2 = -\,\omega^2.$$

Soit, au contraire, a une base de seconde espèce, toutes les solutions (u, v) et (u', v') correspondent à l'équation (4), mais il n'existe aucune relation de la forme (16) pour les nombres $u_{2\lambda+1}$ et $u'_{2\lambda}$.

Dans l'article qui suit, nous avons à déduire, pour les nombres susdits, des expressions analogues à (16), mais contenant d'autres nombres que p et q.

XIV. Sur la décomposition principale.

Revenons maintenant à l'équation de Fermat

$$A_1^2 - aB_1^2 = (-1)^\varepsilon \tag{1}$$

et à la congruence

$$A_2 \equiv (-1)^\varepsilon \pmod a \tag{2}$$

qui s'y rattache, puis désignons par (σ_n, τ_n) une suite quelconque appartenant à l'équation de Legendre

$$p\sigma^2 - q\tau^2 = (-1)^\delta \omega, \quad a = pq, \tag{3}$$

les formules récursives

$$\sigma_{\lambda+2} = A_2\sigma_\lambda + B_2 q\tau_\lambda, \quad \tau_{\lambda+2} = B_2 p\sigma_\lambda + A_2\tau_\lambda$$

donnent, en vertu de (2), les congruences

$$\sigma_{\lambda+2} - (-1)^\varepsilon \sigma_\lambda \equiv 0 \pmod p, \quad \tau_{\lambda+2} + (-1)^\varepsilon \tau_\lambda \equiv 0 \pmod q, \tag{4}$$

analogues à celles developpées, dans l'article VI, pour les équations de Lagrange.

Les formules précédentes sont valables quelle que soit la base a.

Supposons maintenant que a soit une base de seconde espèce, ayant la décomposition principale

$$a = \pi\varrho, \tag{5}$$

puis supposons

$$A_1 \equiv (-1)^\varphi \pmod \pi, \quad A_1 \equiv (-1)^{\varphi+1} \pmod \varrho,$$

les formules récursives

$$\sigma_{\lambda+1} = A_1\sigma_\lambda + B_1\varphi\tau_\lambda, \quad \tau_{\lambda+1} = B_1\pi\sigma_\lambda + A_1\tau_\lambda$$

donneront les congruences

$$\sigma_\lambda - (-1)^\varphi \sigma_\nu \equiv 0 \pmod \varrho, \quad \tau_\lambda + (-1)^\varphi \tau_\nu \equiv 0 \pmod \pi, \tag{6}$$

valables quels que soient les indices λ et ν.

Étudions ensuite l'équation (3) pour laquelle $\omega > 2$, puis désignons par (s_n, t_n) la suite coordonnée à (σ_n, τ_n), les formules fondamentales

$$(-1)^{\varepsilon} s_1 = A_1 \sigma_1 - B_1 \varrho \tau_1, \quad (-1)^{\varepsilon} t_1 = B_1 \pi \tau_1 - A_1 \sigma_1,$$

où ε est l'exposant défini par la formule (1), donnent de même

$$(7) \quad s_1 - (-1)^{\varepsilon+\varphi} \sigma_1 \equiv 0 \pmod{\varrho}, \quad t_1 + (-1)^{\varepsilon+\varphi} \tau_1 \equiv 0 \pmod{\pi},$$

de sorte que nous aurons, quels que soient les indices λ et ν,

$$(7 \text{ bis}) \quad \begin{cases} s_\lambda - (-1)^{\varepsilon+\varphi} \sigma_\nu \equiv 0 \pmod{\varrho}, \\ t_\lambda + (-1)^{\varepsilon+\varphi} \tau_\nu \equiv 0 \pmod{\pi}. \end{cases}$$

Cela posé, nous avons à étudier l'équation de LEGENDRE qui correspond à la décomposition principale de la base a, équation que nous supposons tout d'abord de la forme

$$(8) \qquad \pi \alpha^2 - \varrho \beta^2 = (-1)^{\delta},$$

et nous aurons le théorème essentiel:

I. *Les équations de* LAGRANGE *et de* LEGENDRE

$$(9) \qquad u^2 - a v^2 = (-1)^{\varepsilon} \omega, \quad \pi s^2 - \varrho t^2 = (-1)^{\delta+\varepsilon} \omega$$

sont simultanément résolubles ou non, et, en cas de résolubilité, ces équations sont du même genre.

En effet, partons de la première des équations (9), puis multiplions par (8), il résulte

$$\pi (u \alpha \pm \varrho v \beta)^2 - \varrho (\pi v \alpha \pm u \beta)^2 = (-1)^{\delta+\varepsilon} \omega,$$

ce qui est précisément la seconde des équations (9).

Inversement, partons de la dernière des équations (9), la multiplication par (8) donnera

$$(\pi \alpha s \pm \varrho \beta t)^2 - a(\alpha t \pm \beta s)^2 = (-1)^\varepsilon \omega,$$

savoir la première des équations (9).

Supposons ensuite que la base a se présente sous la forme

(10) $$a = pqrs,$$

où deux quelconques de ces quatre facteurs sont premiers entre eux, puis désignons par

(11) $$a = \pi \varrho; \quad \pi = pq, \quad \varrho = rs$$

la décomposition principale de a, nous aurons le théorème curieux:

II. Les deux équations de Legendre

(12) $$pr\sigma^2 - qs\tau^2 = (-1)^\delta \omega, \quad ps\sigma_1^2 - qr\tau_1^2 = (-1)^{\delta+\varepsilon+1} \omega$$

sont en même temps résolubles ou non, et, en cas de résolubilité, ces deux équations sont du même genre.

A cet effet, multiplions par (8) chacune des équations (12), nous aurons la seconde de ces mêmes équations.

Dans ce qui suit, nous désignons comme simultanées les équations (12), de sorte que l'existence des équations simultanées exige que la base a contienne au moins trois facteurs premiers inégaux, car les résultats que nous venons de développer sont applicables aussi pour $s = 1$.

Revenons maintenant à la multiplication des équations (8) et (12), nous aurons, abstraction faite du signe,

(13) $$\sigma_1 = q\alpha\tau \pm r\beta\sigma, \quad \tau_1 = q\alpha\sigma \pm s\beta\tau.$$

Remarquons ensuite que l'opération itérative du second ordre conduira de chacune des équations (12) à l'équation de Lagrange

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

puis posons, conformément aux formules (5) de l'article précédent,

$$u_1 = p r \sigma^2 + q s \tau^2, \quad v_1 = 2 \sigma \tau,$$

les formules

$$A_1 = \pi \alpha^2 + \varrho \beta^2, \quad B_1 = 2 \alpha \beta,$$

conséquences immédiates des formules (13) et (14) de l'article VII, donnent, après un calcul direct,

$$p r (q \alpha \tau \pm r \beta \sigma)^2 + q s (p \alpha \sigma + s \beta \tau)^2 = u_1 A_1 \pm a v_1 B_1$$
$$2 (q \alpha \tau \pm r \beta \sigma) \ (q \alpha \sigma \pm s \beta \tau) = v_1 A_1 \pm u_1 B_1,$$

savoir l'élément (u_2, v_2) et l'élément (u_1', v_1') réciproque de (u_1, v_1); c'est-à-dire que nous venons de démontrer la proposition intéressante qui donnera la solution du problème indiqué à la fin de l'article précédent:

III. L'opération quadratique conduira, des équations simultanées (12), à toutes les solutions (u_n, v_n) et (u_n', v_n') d'un couple de suites coordonnées appartenant à l'équation (14).

Quant aux bases a de seconde espèce pour lesquelles l'équation de LEGENDRE qui correspond à la décomposition principale se présente sous la forme

$$\pi \alpha^2 - \varrho \beta^2 = (-1)^{\delta} 2, \tag{15}$$

les équations simultanées (12) deviennent, pour ω impair,

$$p r \sigma^2 - q s \tau^2 = (-1)^{\varepsilon} \omega, \quad p s \sigma_1^2 - q r \tau_1^2 = (-1)^{\delta+\varepsilon+1} 2 \omega, \tag{16}$$

et, pour ω pair,

$$p r \sigma^2 - q s \tau^2 = (-1)^{\varepsilon} \omega, \quad p s \sigma_1^2 - q r \tau^2 = (-1)^{\delta+\varepsilon+1} \frac{\omega}{2}, \tag{17}$$

tandis que l'équation (14) se présente, pour ω pair, sous la forme

$$u^2 - a v^2 = \left(\frac{\omega}{2}\right)^2. \tag{18}$$

Du reste, les résultats que nous venons d'obtenir sont applicables aussi dans ce cas.

La deuxième des tables numériques jointes au présent Mémoire contient les solutions des diverses équations de LAGRANGE et de LEGENDRE qui correspondent à $a = 30$, la plus petite base qui contienne trois facteurs premiers inégaux.

CHAPITRE IV

Sur les hauteurs paires.

XV. Équations primitives.

Dans les recherches qui nous occupent ici, l'équation

(1) $$u^2 - a v^2 = \omega^2$$

joue un rôle si important qu'il est nécessaire de l'étudier plus profondément, ce qui exige avant tout une définition de l'idée d'une équation primitive.

A cet effet, nous avons à comparer l'équation (1) avec celles-ci

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

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

et nous désignons l'équation (1)

comme primitive, pourvu qu'aucune des équations (2) et (2 bis) ne soit résoluble;

comme semi-primitive, pourvu que son genre soit plus élevé que celui de l'équation résoluble (2) ou (2 bis).

Quant aux équations semi-primitives, il existe donc au moins un couple de suites coordonnées (u_n, v_n) et (u'_n, v'_n) dont les éléments ne proviennent pas, par l'opération itérative du second ordre, d'une équation (2) ou (2 bis).

Nous désignons de telles suites comme suites coordonnées primitives de l'équation (1), et, en étudiant une équation semi-primitive, nous supposons que la solution (u, v) en question appartienne à une suite primitive.

Quant à l'équation (1), supposée primitive, le paramètre ω est nécessairement de la hauteur 2 par rapport à la base a, et l'inverse est vraie aussi, pourvu que a ne soit pas de la forme $4k+3$.

Soit maintenant, dans l'équation (1), supposée primitive, u et ω de parité différente, il existe une décomposition

$$a = pq; \quad q > p > 1, \tag{3}$$

telle que

$$u+(-1)^{\delta}\omega = p\sigma^2, \quad u-(-1)^{\delta}\omega = q\tau^2, \quad v = \sigma\tau, \tag{4}$$

où p et q, σ et τ sont premiers entre eux, ce qui donnera

$$p\sigma^2+q\tau^2 = 2u, \quad p\sigma^2-q\tau^2 = (-1)^{\delta}2\omega. \tag{5}$$

Soit, au contraire, u et ω tous deux impairs, δ est nécessairement pair, parce que av^2 est multiple de 8, et a est une base réduite; posons donc

$$v = 2\sigma\tau, \tag{6}$$

nous aurons, dans ce cas,

$$u+(-1)^{\delta}\omega = 2p\sigma^2, \quad u-(-1)^{\delta}\omega = 2q\tau^2, \tag{7}$$

savoir, au lieu de (5),

$$p\sigma^2+q\tau^2 = u, \quad p\sigma^2-q\tau^2 = (-1)^{\delta}\omega. \tag{8}$$

Cela posé, il est facile de démontrer le théorème, fondamental dans la théorie des équations de LAGRANGE:

I. Les seules bases réduites qui n'admettent aucune équation primitive sont les nombres premiers et les bases de seconde espèce, qui ne contiennent que deux facteurs premiers et qui ne permettent de résoudre aucune des équations

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

où a est la base en question.

Supposons tout d'abord que la base a de seconde espèce contienne au moins trois facteurs premiers, il existe toujours une décomposition

$$a = pq,$$

différente de la décomposition principale. Choisissons ensuite les deux positifs entiers α et β, tels que $p\alpha$ et $q\beta$ sont premiers entre eux, puis posons

(10) $$\pm \omega = p\alpha^2 - q\beta^2,$$

il est évident que l'équation de LEGENDRE

(11) $$p\sigma^2 - q\tau^2 = \pm \omega$$

est résoluble, ayant la solution (α, β).

De plus, il est possible de choisir α et β, tel que ω devienne impair; donc l'équation ainsi déterminée

(12) $$u^2 - a v^2 = \omega^2$$

est primitive.

Quant aux bases de première espèce, nous démontrerons le lemme:

II. Une base de première espèce qui est un nombre composé, admet toujours des équations primitives.

On voit que le développement précédent conduira immédiatement au but, parce qu'une base de première espèce ne possède aucune décomposition principale.

Étudions ensuite les bases de seconde espèce, nous aurons de même:

III. Une base a de seconde espèce qui ne contient que deux facteurs premiers, et pour laquelle l'équation (9) n'est pas résoluble, n'admet aucune équation primitive.

En effet, supposons primitive l'équation (12), puis désignons par (u_m, v_m) et (u_n, v_n) deux solutions quelconques d'une même suite primitive appartenant à l'équation susdite, nous aurons

$$(13) \qquad p\sigma^2 + q\tau^2 = \varkappa u_m, \quad p\sigma_1^2 + q\tau_1^2 = \varkappa u_n$$

$$(14) \quad p\sigma^2 - q\tau^2 = (-1)^\delta \varkappa\omega, \quad p\sigma_1^2 - q\tau_1^2 = (-1)^\delta \varkappa\omega,$$

où $\varkappa$ est un des nombres 1 ou 2, ce qui donnera, en vertu de (14),

$$p(\sigma^2 - \sigma_1^2) = q(\tau^2 - \tau_1^2),$$

de sorte que nous aurons les deux congruences

$$(15) \qquad \sigma^2 - \sigma_1^2 \equiv 0 \pmod q \quad \tau^2 - \tau_1^2 \equiv 0 \pmod p,$$

car p et q sont premiers entre eux.

De plus, il résulte, en vertu de (13),

$$\varkappa(u_m - u_n) = p(\sigma^2 - \sigma_1^2) + (\tau^2 - \tau_1^2),$$

de sorte que les congruences (15) donnent

$$u_m \equiv u_n \pmod a,$$

ce qui est impossible, comme nous venons de le démontrer dans l'article VI.

IV. Une base de seconde espèce qui est un nombre composé, et pour laquelle l'équation (9) est résoluble, admet toujours des équations primitives.

Cette proposition est une conséquence immédiate des formules (10) et (11), parce que la base en question n'admet aucune décomposition principale.

Reste encore le cas où la base est un nombre premier, mais une telle base n'admet aucune équation de Legendre et par conséquent aucune équation primitive.

Cela posé, il est facile de démontrer encore deux théorèmes fondamentaux dans la théorie des équations de Lagrange, dont voici le premier:

V. Les seules bases réduites qui n'admettent pas la hauteur 2 sont les nombres premiers et les bases de seconde espèce des formes $4k+1$ ou $4k+2$, qui ne sont pas une somme de deux carrés, et qui ne contiennent que deux facteurs premiers.

En effet, il est évident que tous les paramètres qui admettent des équations primitives, admettent aussi la hauteur 2.

Quant aux bases de la forme $4k+3$, pour lesquelles l'équation (9) n'est pas résoluble, nous choisissons deux nombres impairs α et β, de sorte que α est premier avec $a\beta$, le nombre ω défini par l'expression

$$\pm 2\omega = \alpha^2 - a\beta^2$$

est impair, de sorte que les équations

$$u^2 - av^2 = \pm 2\omega, \quad u^2 - av^2 = \omega^2 \tag{16}$$

sont toutes deux résolubles. Et il est évident que ω contient au moins un facteur premier de la hauteur 2, parce que le paramètre 2 est inapplicable.

Enfin, soit

$$a = \alpha^2 + \beta^2, \tag{17}$$

je dis que les équations primitives de la base a se présentent toujours sous la forme

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

équation qui est certainement résoluble pour $\omega = \alpha$ et $\omega = \beta$, ayant la solution $(\beta, 1)$ respectivement $(\alpha, 1)$.

En effet, supposons primitive une équation de la forme

$$u^2 - a v^2 = \omega^2,$$

l'équation de LEGENDRE

$$p \sigma^2 - q \tau^2 = (-1)^\delta \omega$$

est résoluble, ce qui est impossible, parce que la multiplication de cette équation par l'équation principale

$$p \alpha^2 - q \beta^2 = (-1)^\varepsilon \omega$$

conduira à cette autre équation résoluble

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

Reste encore le second des deux théorèmes susdits, théorème qui se présente sous la forme la plus simple, pourvu que la base a ne soit ni une base de seconde espèce de la forme $\alpha^2 + \beta^2$ ni une base $4k+3$ qui n'admet pas le paramètre ± 2. Posons ensuite

$$\omega = \pi_1^{\alpha_1} \pi_2^{\alpha_2} \dots \pi_n^{\alpha_n}, \tag{19}$$

où les nombres π_r sont les facteurs premiers de ω, nous avons à démontrer le théorème:

VI. Supposons que les n facteurs $\pi_r^{\alpha_r}$ soient tous des hauteurs 1 ou 2 par rapport à la base a, qui satisfait aux conditions susdites, il existe une décomposition

$$a = pq, \quad 1 \leqq p < q \leqq a, \tag{20}$$

telle que l'équation

$$p \sigma^2 - q \tau^2 = (-1)^\delta \omega \tag{21}$$

est résoluble, et le genre de cette équation a la valeur maximum 2^{n-1} ou 2^n, selon que a est de la forme $4k+2$ ou non.

Soit π_r un des facteurs premiers de ω, il existe une décomposition

$$a = p_r q_r, \quad 1 \leqq p_r < q_r \leqq a,$$

de sorte que l'équation

$$p_r \sigma^2 - q \tau_r^2 = (-1)^{\delta_r} \pi^{\alpha_r}$$

est résoluble, et la multiplication des n équations ainsi obtenues conduira immédiatement au théorème VI.

Les modifications de ce théorème qui exigent les bases exclues sont évidentes.

Remarquons, en passant, que le théorème VI est certainement valable, pourvu que tous les facteurs premiers du paramètre ω soient des hauteurs 1 ou 2 par rapport à la base a.

XVI. Bases de première espèce.

Pour illustrer par un exemple assez général les développements précédents, en ce qui concerne les bases de première espèce, nous partons de l'équation de FERMAT

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

et nous démontrerons tout d'abord la proposition:

I. Soit a une base de première espèce, quelconque du reste, les équations de LAGRANGE

$$u^2 - a v^2 = \pm A_{2\nu+1}^2 \tag{2}$$

sont toujours résolubles, quel que soit l'indice impaire $2\nu+1$.

Supposons tout d'abord a impair, l'équation

$$s^2 - a t^2 = \pm 2 A_{2\nu+1} \tag{3}$$

est résoluble, ayant les solutions

$$(4) \qquad (A_{2\nu+1}+1,\ B_{2\nu+1}) \quad (A_{2\nu+1}-1,\ B_{2\nu+1}).$$

Soit ensuite a un nombre pair, savoir

$$(5) \qquad a = 2a_1,$$

a_1 est nécessairement impair, et, dans ce cas, l'équation de Legendre

$$(6) \qquad 2\sigma^2 - a_1\tau^2 = \pm A_{2\nu+1}$$

est résoluble, admettant les solutions

$$(7) \qquad \left(\frac{A_{2\nu+1}-1}{2},\ B_{2\nu+1}\right) \quad \left(\frac{A_{2\nu+1}+1}{2},\ B_{2\nu+1}\right).$$

Et l'équation (2) provient de (3) respectivement de (6), par l'opération itérative du second ordre.

Posons particulièrement

$$a = \alpha^2+1, \quad A_1 = \alpha,$$

la valeur minimum des paramètres applicables est 2α ou $4\alpha \mp 3$, selon que α est pair ou impair, ce qui donnera immédiatement la proposition:

II. Soit α un nombre impair, plus grand que l'unité, mais quelconque du reste, l'équation

$$(8) \qquad u^2 - (\alpha^2+1) = \alpha^2$$

est toujours primitive.

Supposons maintenant que la base paire α^2+1 contienne au moins deux facteurs premiers impairs, il existe encore une décomposition en somme de deux carrés, savoir

$$(9) \qquad a = \alpha^2+1 = \beta^2+\gamma^2,$$

où β et γ sont tous deux impairs, et les équations

$$(10) \qquad u^2 - av^2 = \beta^2, \quad u^2 - av^2 = \gamma^2,$$

ayant, pour les paramètres négatifs, les solutions $(\gamma, 1)$ respectivement $(\beta, 1)$, sont certainement primitives, parce que $\beta < \alpha$ et $\gamma < \alpha$.

Quant aux équations (10), nous aurons la proposition:

III. Il existe une décomposition

$$a = 2pq, \tag{11}$$

de sorte que la première des équations (10) appartient à $(p, 2q)$, la seconde à $(2p, q)$.

En effet, multiplions les deux équations évidentes

$$\alpha^2 - a \cdot 1^2 = -1, \quad \gamma^2 - a \cdot 1^2 = -\beta^2,$$

nous aurons

$$(\alpha\gamma - a)^2 - a(\alpha - \gamma)^2 = \beta^2; \tag{12}$$

posons donc

$$\alpha - \gamma = 2\sigma\tau,$$

il résulte, en vertu de (12),

$$\left\{ \begin{aligned} \alpha\gamma - a + (-1)^\delta \beta &= 2p\sigma^2 \\ \alpha\gamma - a - (-1)^\delta \beta &= 4q\tau^2, \end{aligned} \right. \tag{13}$$

ce qui donnera l'équation de Legendre correspondante

$$p\sigma^2 - 2q\tau^2 = (-1)^\delta \beta. \tag{14}$$

Partons ensuite des congruences

$$\begin{aligned} \alpha\gamma + (-1)^\delta \beta &\equiv 0 \pmod p \\ \alpha\gamma - (-1)^\delta \beta &\equiv 0 \pmod q), \end{aligned}$$

tirées directement des équations (13), nous aurons, en multipliant par γ ces deux congruences, puis appliquant la formule (9),

$$\left\{ \begin{aligned} \alpha\beta - a + (-1)^\delta \gamma &\equiv 0 \pmod p \\ \alpha\beta - a - (-1)^\delta \gamma &\equiv 0 \pmod q). \end{aligned} \right. \tag{15}$$

De plus, la différence

$$\left(\alpha\beta - a + (-1)^{\delta}\gamma\right) - \left(\alpha\gamma - a - (-1)^{\delta}\gamma\right) = \alpha(\beta-\gamma) + (-1)^{\delta}(\beta+\gamma)$$

étant de la forme $4k+2$, on aura, en vertu de (15),

$$\alpha\beta - a - (-1)^{\delta}\gamma = 4ps^2$$
$$\alpha\beta - \alpha + (-1)^{\delta}\gamma = 2q\tau^2,$$

où

$$a - \gamma = 2st,$$

ce qui donnera finalement la seconde des équations susdites

$$(16) \qquad 2ps^2 - qt^2 = (-1)^{\delta+1}\gamma.$$

Quant aux bases spéciales qui nous occupent ici, il nous reste encore à démontrer cette autre proposition:

IV. Deux couples de suites coordonnées, appartenant à l'équation primitive

$$(17) \qquad u^2 - a\delta = \beta^2\gamma^2, \quad a = 2a_1,$$

qui est au moins du genre 4, correspondent à la décomposition $(2, a_1)$.

En effet, multiplions les deux équations

$$\gamma^2 - a\cdot 1^2 = -\beta^2, \quad \beta^2 - a\cdot 1^2 = -\gamma^2,$$

il résulte

$$(18) \qquad (a \pm \beta\gamma)^2 - a(\beta \pm \gamma)^2 = \beta^2\gamma^2.$$

Posons ensuite

$$u = a + \beta\gamma, \quad v = \beta + \gamma,$$

nous aurons, en vertu de (9),

$$u + \beta + \gamma = (\beta+\gamma)^2 = 4\sigma^2; \quad \sigma = \frac{\beta+\gamma}{2}$$
$$u - \beta\gamma = a = 2a_1\tau^2; \quad \tau = 1,$$

ce qui conduira à l'équation de LEGENDRE

(19) $$2\sigma^2 - a_1\tau^2 = \pm\beta\gamma.$$

La seconde des équations (18) donnera de même

$$u = a - \beta\gamma, \quad v = \beta - \gamma,$$

de sorte que l'on aura ici

$$u + \beta\gamma = a = 2a_1\tau^2; \ \sigma = 1$$
$$u - \beta\gamma = (\beta-\gamma)^2 = 4\sigma^2; \ \sigma = \frac{\beta-\gamma}{2},$$

ce qui conduira de nouveau à l'équation (19), équation qui a par conséquent les deux solutions

(20) $$\left(\frac{\beta-\gamma}{2}, 1\right) \ \left(\frac{\beta+\gamma}{2}, 1\right).$$

XVII. Bases de seconde espèce.

Quant aux bases de seconde espèce, nous partons de l'équation classique

(1) $$A_\nu^2 - 2B_\nu^2 = (-1)^\nu,$$

équation qui conduira immédiatement à la proposition:

I. Soit $\nu \geqq 1$, l'équation

(2) $$u^2 - \left(A_{2\nu+1}^2 + 2\right) v^2 = A_{2\nu+1}^2$$

est toujours primitive.

Quant à l'équation (2), il résulte immédiatement, en vertu de (1), qu'elle admet la solution

(3) $$u = 2B_{2\nu+1}, \quad v = 1.$$

Supposons ensuite impair le paramètre ω, les deux équations

$$u^2 - \left(A_{2\nu+1}^2 + 2\right) v^2 = (-1)^\delta \omega$$
$$u^2 - \left(A_{2\nu+1}^2 + 2\right) v^2 = (-1)^{\delta+1} 2\omega$$

sont simultanément résolubles ou non, et nous savons que ces équations sont toujours irrésolubles, à moins que

$$\omega \geqq 2 A_{2\nu+1} - 1;$$

c'est-à-dire que le paramètre

$$\omega = A_{2\nu+1}$$

est toujours exclu pour $\nu \geqq 1$, et l'équation (2) est primitive.

On voit que l'hypothèse $\nu = 0$ conduira à l'équation

$$u^2 - 3 v^2 = 1,$$

qui ne présente aucun intérêt à ce point de vue.

La plus petite base définie par l'expression

$$a_\nu = A_{2\nu+1}^2 + 2 \tag{4}$$

est le nombre

$$a_1 = 7^2 + 2 = 51, \tag{5}$$

ce qui est précisément la plus petite base composée qui admette un des paramètres ± 2.

La troisième des tables numériques, jointes au présent Mémoire, donnera les solutions des équations de LAGRANGE et de LEGENDRE ayant la base 51.

Revenons maintenant à l'équation (2), puis appliquons les formules

$$2 B_{2\nu+1} - A_{2\nu+1} = A_{2\nu}, \quad 2 B_{2\nu+1} + A_{2\nu+1} = A_{2\nu+2},$$

il est évident que l'équation susdite conduira à l'équation de LEGENDRE

$$A_{2\nu} \sigma^2 - A_{2\nu+2} \tau^2 = -2 A_{2\nu+1}, \tag{6}$$

ayant la solution (1, 1).

Multiplions ensuite (6) par l'équation principale

$$A_{2\nu+1}^2 - \left(A_{2\nu+1}^2 + 2\right) \cdot 1^2 = -2,$$

il résulte l'équation simultanée

(7) $$A_{2\nu}s^2 - A_{2\nu+1}t^2 = A_{2\nu+1},$$

qui admet la solution $(B_{2\nu+1}, B_{2\nu})$.

XVIII. Sur les bases $4p^4+1$.

Il résulte immédiatement du théorème I de l'article XV que le nombre

(1) $$a = 4\alpha^4+1,$$

ne peut jamais être premier, pourvu que $\alpha > 1$, car l'équation

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

est primitive.

Or, l'identité évidente

(3) $$(2\alpha^2-1)^2+(2\alpha)^2 = 4\alpha^4+1$$

donnera, pour $\alpha > 1$, deux décompositions différentes en sommes de deux carrés de la base a; de sorte que a ne peut être un nombre premier que dans le seul cas

$$\alpha = 1, \quad a = 5.$$

Quant à la formule (3), on voit que le carré pair qui figure au second membre est un bicarré, pourvu que

(4) $$\alpha = 2k^2,$$

et seulement dans ce cas.

Quant au carré impair, l'équation classique

(5) $$A_r^2 - 2B_r^2 = (-1)^\nu$$

donnera immédiatement la proposition:

I. Le carré impair qui figure au premier membre de l'équation (3) est un bicarré, pourvu que

(6) $$\alpha = B_{2\nu+1},$$

et seulement dans ce cas.

Appliquons ensuite cette autre identité évidente

$$(7) \qquad 4\alpha^4+1 = \left((\alpha-1)^2+\alpha^2\right)\left(\alpha^2+(\alpha+1)^2\right),$$

il est facile de déterminer α, tel que la base a se présente sous la forme

$$(8) \qquad 4\alpha^4+1 = \gamma^2\left(\alpha^2+(\alpha\pm 1)^2\right),$$

problème qui se rattache aussi à l'équation (5), car nous aurons la proposition:

II. Un des deux facteurs qui figurent au second membre de (8) est un carré exact, pourvu que

$$(9) \qquad \alpha = \frac{A_{2\nu+1}\mp 1}{2},$$

et seulement dans ce cas.

Soit par exemple $\nu = 1$, on aura

$$\alpha = \frac{A_3-1}{2} = 3, \quad a = 325 = 5^2\cdot 13$$

$$\alpha = \frac{A_3+1}{2} = 4, \quad a = 1025 = 5^2\cdot 41.$$

XIX. Applications diverses.

Il nous semble utile d'éclaircir, par des exemples convenables, les développements précédents.

Exemple I. L'équation

$$(1) \qquad u^2-145v^2 = \pm 144$$

du genre 4 est semi-primitive, car la solution (17, 1) de cette équation conduira à l'équation de Legendre

$$(2) \qquad 5\sigma^2-29\tau^2 = \pm 24,$$

ayant la solution (1, 1).

Exemple II. L'équation

$$(3) \qquad u^2-442v^2 = \pm 441$$

du genre 4 est aussi semi-primitive, parce que la solution (47, 2) correspond à l'équation de LEGENDRE

$$13\sigma^2 - 34\tau^2 = -21, \tag{4}$$

satisfaite par (1, 1).

Exemple III. Le nombre

$$130 = 11^2 + 3^2 = 9^2 + 7^2 \tag{5}$$

est la plus petite base de première espèce qui contienne trois facteurs premiers inégaux.

La première des décompositions (5) conduira aux deux équations primitives

$$23^2 - 130\cdot 2^2 = 9, \quad 479^2 - 130\cdot 42^2 = 121 \tag{6}$$

qui correspondent aux équations de LEGENDRE

$$10\sigma^2 - 13\tau^2 = \pm 3, \quad 5\sigma^2 - 26\tau^2 = \pm 11, \tag{7}$$

ayant les solutions (1, 1) respectivement (7, 3).

Quant à la seconde décomposition (5), elle ne conduira qu'à la seule équation primitive

$$137^2 - 130\cdot 12^2 = 49, \tag{8}$$

à laquelle correspond l'équation de LEGENDRE

$$2\sigma^2 - 65\tau^2 = \pm 7, \tag{9}$$

satisfaite par (6, 1).

L'équation primitive du genre 4, déterminée par les égalités

$$67^2 - 130\cdot 8^2 = 163^2 - 180\cdot 14^2 = 33^2 \tag{10}$$

conduira à l'équation de LEGENDRE

$$2\sigma^2 - 65\tau^2 = \pm 33, \tag{11}$$

également du genre 4, car ses deux solutions (4, 1) et (7, 1) n'appartiennent pas au même couple de suites coordonnées.

Les nombres premiers

$$3 \quad 7 \quad 11 \quad 43$$

sont tous de la hauteur 2 par rapport à la base 130.

L'équation

$$u^2 - 130\,v^2 = \pm 129 \tag{12}$$

est résoluble et du genre 4, parce que 3 et 43 appartiennent à la même décomposition de 130.

Au contraire, aucun des nombres

$$21 \quad 33 \quad 77$$

n'est applicable comme paramètre de la base 130, parce que les deux nombres premiers, contenus dans chacun de ces nombres, appartiennent à des décompositions différentes de 130.

Mais l'équation

$$u^2 - 130\,v^2 = \pm 231 \tag{13}$$

est résoluble et du genre 8.

La dernière des quatre tables numériques jointes au présent Mémoire contient les solutions des équations de Lagrange et de Legendre qui se rattachent à la base 130.

CHAPITRE V

Sur l'opération du troisième ordre.

XX. Sur la multiplication des équations.

L'ensemble des équations de LAGRANGE

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

déterminées par les conditions

$$2 \leqq a \leqq 102, \quad 2 \leqq \omega \leqq 1000,$$

ne contient qu'une seule équation dont le genre ne soit pas une puissance de 2, savoir

$$u^2 - 37 v^2 = \pm 924.$$

La détermination du genre de cette équation exige donc, à ce point de vue, des recherches ultérieures sur la multiplication de plusieurs équations de LAGRANGE.

A cet effet, désignons par

$$(s_r, t_r), \quad r = 1, 2, 3, \ldots$$

une solution d'une suite quelconque appartenant à l'équation

(1) $$s_r^2 - a t_r^2 = (-1)^{\delta_r} \omega_r,$$

il est évident que, dans la multiplication positive de ces équations, que nous désignons simplement par le symbole

(2) $$(s_1, t_1)\ (s_2, t_2)\ (s_3, t_3) \ldots,$$

et qui est définie par les formules

$$(3)\quad (s_p s_q + a t_p t_q)^2 - a(s_p t_q + s_q t_p)^2 = (-1)^{\delta_p+\delta_q}\omega_p \omega_q,$$

nous pouvons permuter arbitrairement les facteurs de ce produit symbolique, et que l'on peut remplacer par exemple les deux facteurs (s_2, t_2) et (s_3, t_3) par leur produit, défini par la formule (3), de sorte que le produit (2) se présente aussi sous la forme

$$(4)\quad (s_1, t_1)\ \big((s_2, t_2)\ (s_3, t_3)\big)\ (s_4, t_4)\ldots$$

Posons ensuite pour abréger

$$S_1 = (+)\ (s_1, t_1)\ (s_2, t_2),\quad S_2 = (+)\ (s_1, t_1)\ (s_3, t_3)$$
$$T_1 = (-)\ (s_1, t_1)\ (s_2, t_2),\quad T_2 = (-)\ (s_1, t_1)\ (s_3, t_3),$$

nous avons à démontrer les identités

$$(5)\quad (+)\, S_1 T_2 = (+)\, S_2 T_1 = (+)\ (s_2, t_2)\ (s_3, t_3)$$
$$(6)\quad (-)\, S_1 T_2 = (-)\, S_2 T_1 = (-)\ (s_2, t_2)\ (s_3, t_3).$$

A cet effet, désignons par (s'_r, t'_r) une solution de la suite coordonnée à celle qui contient (s_r, t_r), nous aurons

$$T_1 = (+)\ (s'_1, t'_1)\ (s_2, t_2),\quad T_2 = (+)\ (s'_1, t'_1)\ (s_3, t_3),$$

ce qui donnera la multiplication positive

$$(+)\, S_1 T_2 = (s_1, t_1)\ (s_2, t_2)\ (s'_1, t'_1)\ (s_3, t_3);$$

permutons ensuite les deux premiers de ces facteurs, puis remarquons que la multiplication positive des deux suites coordonnées fait disparaître ces facteurs symboliques, de sorte que nous aurons finalement

$$(+)\, S_1 T_2 = (+)\ (s_2, t_2)\ (s_3, t_3)$$

savoir la première des formules (5).

Et l'on démontrera, par le même procédé, les autres formules en question, formules que l'on trouvera aussi facilement par un calcul direct, en appliquant l'identité (3) et la définition analogue de la multiplication négative, savoir

$$(s_p s_q - a t_p t_q)^2 - a(s_p t_q - s_q t_p)^2 = (-1)^{\delta_p + \delta_q} \omega_p \omega_q.$$

Cela posé, nous partons des quatre nombres

$$\omega_1 \quad \omega_2 \quad \omega_3 \quad \omega_4, \tag{7}$$

premiers entre eux deux à deux, et les six équations de la forme

$$u^2 - a v^2 = (-1)^{\delta} \omega_\alpha \omega_\beta, \tag*{(α, β)}$$

où α et β sont deux quelconques des indices des nombres (7), il est évident que la multiplication des deux équations (α, β) et (γ, δ) conduira toujours à cette autre équation

$$u^2 - a v^2 = (-1)^{\varepsilon} \omega_1 \omega_2 \omega_3 \omega_4. \tag{8}$$

Et nous avons à démontrer la proposition:

I. Les six produits de la forme $(\pm)$ (α, β) (γ, δ) donnent précisément trois couples de suites coordonnées appartenant à l'équation (8).

En effet, appliquons les identités (5) et (6), nous aurons, en appliquant des signes convenables dans les multiplications, des identités de la forme

$$(\alpha, \beta)\ (\alpha, \gamma) = (\beta, \gamma)$$
$$(\alpha, \gamma)\ (\gamma, \delta) = (\alpha, \delta),$$

ce qui donnera, toujours avec des signes convenables dans la multiplication,

$$(\alpha, \delta)\ (\beta, \gamma) = (\alpha, \beta)\ (\gamma, \delta),$$

et il est évident qu'il existe précisément trois identités de cette forme, de sorte que notre proposition est démontrée.

XXI. Sur la hauteur 3.

Désignons maintenant par

$$(1) \qquad \omega_1 \quad \omega_2 \quad \omega_3 \quad \omega_4$$

quatre nombres premiers impairs qui sont tous de la hauteur 3 par rapport à la base a.

Supposons ensuite résolubles les six équations de la forme

$$(\alpha, \beta) \qquad u^2 - a v^2 = (-1)^{\delta_{\alpha,\beta}} \omega_\alpha \omega_\beta,$$

nous avons récemment démontré que ces équations sont du genre 2, et que les quatre équations de la forme

$$(\alpha, \beta, \gamma) \qquad u^2 - a v^2 = (-1)^{\delta_{\alpha,\beta} + \delta_{\alpha,\gamma}} \omega_\alpha \omega_\beta \omega_\gamma$$

sont résolubles aussi et du genre 2.

Cela posé, nous avons ici à démontrer les propositions suivantes:

I. Supposons résolubles les quatre équations (α, β, γ), les six équations (α, β) sont résolubles aussi.

A cet effet, désignons pour abréger par les symboles

$$(\alpha^r) \quad (\alpha^r, \beta^s, \gamma^t, \ldots)$$

les équations qui correspondent aux paramètres

$$\omega_\alpha^r, \quad \omega_\alpha^r \omega_\beta^s \omega_\gamma^t \ \ldots,$$

nous aurons des identités de la forme

$$\begin{aligned}
(\pm) \ (\alpha^3) \ (\alpha, \beta, \gamma) &= (\alpha^2, \beta, \gamma) \\
(\pm) \ (\beta^3) \ (\alpha^2, \beta^2, \gamma) &= (\alpha^2, \beta^2, \gamma) \\
(\pm) \ (\alpha, \beta, \gamma) \ (\alpha^2, \beta^2, \gamma) &= (\alpha, \gamma^2) \\
(\mp) \ (\alpha, \beta, \gamma) \ (\alpha^2, \beta^2, \gamma) &= (\beta, \gamma^2),
\end{aligned}$$

où les signes sont à choisir convenablement dans toutes les multiplications en question, car aucun des paramètres ω_α^2 n'est applicable, parce que ω_α est de la hauteur 3.

Et l'on aura de même, avec un choix convenable du signe,

$$(\pm)\ (\gamma^3)\ (\alpha, \gamma^2) = (\alpha, \gamma),$$

de sorte que ces multiplications conduiront, des quatre équations (α, β, γ), aux six équations (α, β).

II. L'équation

$$u^2 - a v^2 = (-1)^{\varepsilon}\, \omega_1\, \omega_2\, \omega_3\, \omega_4 \tag{2}$$

est résoluble et du genre 6.

Il résulte, en vertu de la proposition I de l'article précédent, que l'équation (2) est résoluble et au moins du genre 6, car nous avons démontré l'existence de trois couples de suites coordonnées appartenant à cette équation.

Supposons ensuite que l'équation (2) admette encore une suite de solutions S, puis désignons par T et T' un des trois couples de suites coordonnées que nous venons de déterminer, nous aurons, en choisissant convenablement les signes,

$$(\pm)\ S\,T = (\alpha^2, \beta^2), \quad (\mp)\ S\,T = (\gamma^2, \delta^2),$$

ce qui donnera, toujours avec un choix convenable du signe,

$$(\pm)\ (S\,T)\,T' = (\alpha^2, \beta^2)\,T' = S,$$

de sorte que S peut être obtenue par une multiplication convenable de certaines équations (α, β), ce qui est impossible, parce que de telles multiplications conduiront seulement aux trois couples, déterminés par la proposition I de l'article précédent.

Remplaçons maintenant un des ω_δ par le nombre 4, posons par exemple

$$\omega_4 = 4,$$

puis supposons résolubles les trois équations

$$(\alpha) \qquad u^2 - a v^2 = (-1)^{\delta_\alpha} 4\,\omega_\alpha; \quad \alpha = 1, 2, 3,$$

les trois équations (α, β) sont résolubles aussi, et nous aurons, par le même procédé que dans le cas précédent, cette autre proposition:

III. L'équation

$$(3) \qquad u^2 - a v^2 = (-1)^\varepsilon 4\,\omega_1\,\omega_2\,\omega_3$$

est résoluble et du genre 6.

Enfin, supposons que 2 soit, par rapport à la base a, de la hauteur 3, savoir qu'une équation de la forme

$$(4) \qquad u^2 - a v^2 = (-1)^\varphi\, 32$$

soit résoluble, puis supposons que les trois équations

$$(5) \qquad u^2 - a v^2 = (-1)^{\delta_\alpha} 8\,\omega_\alpha; \quad \alpha = 1, 2, 3$$

soient résolubles aussi, les trois nombres premiers ω_α sont de la hauteur 3, par rapport à la base a, et nous aurons ici la proposition:

IV. L'équation

$$(6) \qquad u^2 - a v^2 = (-1)^\varepsilon 8\,\omega_1\,\omega_2\,\omega_3$$

est résoluble et du genre 6.

On voit du reste que cette dernière proposition est valable, pourvu que les équations (4) et (5) soient remplacées par celles-ci

$$u^2 - a v^2 = (-1)^\varphi\, 2^{3n-4}, \quad u^2 - a v^2 = (-1)^{\delta_\alpha} 2^n,$$

où il faut supposer $n \geq 3$.

Dans l'article qui suit, nous avons à éclaircir, par des exemples convenables, les développements précédents.

XXII. Exemples.

Les nombres premiers

$$3 \quad 7 \quad 11$$

sont de la hauteur 3 par rapport à la base 37, car on aura

$$(3,4)\ 5^2-37\cdot 1^2=-12,\quad (7,4)\ 3^2-37\cdot 1^2=-28,$$
$$(11,4)\ 9^2-37\cdot 1^2=44,$$

et le paramètre 4 est exclu.

Cela posé, nous aurons de même

$$(3,7)\ 4^2-37\cdot 1^2=-21,\quad (3,11)\ 2^2-37\cdot 1^2=-33,$$
$$(7,11)\ 15^2-37\cdot 2^2=77,$$

ce qui donnera les trois couples de suites coordonnées appartenant à l'équation

$$(1) \qquad u^2-37v^2=\pm 924,$$

savoir

$$\begin{array}{ll} \mathrm{I}_1\ 1^2-37\cdot 5^2=-924 & \mathrm{I}_2\ 179^2-37\cdot 29^2=924 \\ \mathrm{II}_1\ 31^2-37\cdot 1^2=924 & \mathrm{II}_2\ 149^2-37\cdot 25^2=-924 \\ \mathrm{III}_1\ 43^2-37\cdot 5^2=924 & \mathrm{III}_2\ 73^2-37\cdot 13^2=-924. \end{array}$$

Et l'on aura

$$\begin{array}{ll} (-)\ (4,11)\ (3,7)=\mathrm{I}_1, & (+)\ (4,11)\ (3,7)=\mathrm{III}_2 \\ (-)\ (4,7)\ (3,11)=\mathrm{II}_1, & (+)\ (4,7)\ (3,11)=\mathrm{III}_1 \\ (-)\ (4,3)\ (7,11)=\mathrm{I}_1, & (+)\ (4,3)\ (7,11)=\mathrm{II}_2. \end{array}$$

On aura de même

$$\begin{array}{l} (+)\ \mathrm{I}_1\ \mathrm{II}_1 \backsim 18^2-37\cdot 13^2=-7^2\cdot 11^2, \\ (-)\ \mathrm{I}_1\ \mathrm{II}_1 \backsim 1^2-37\cdot 1^2=-4\cdot 3^2, \\ (+)\ \mathrm{I}_1\,\mathrm{III}_1 \backsim 22^2-37\cdot 5^2=-3^2\cdot 7^2, \\ (-)\ \mathrm{I}_1\,\mathrm{III}_1 \backsim 21^2-37\cdot 5^2=-4\cdot 11^2, \\ (+)\ \mathrm{II}_1\,\mathrm{III}_1 \backsim 23^2-37\cdot 3^2=4\cdot 7^2, \\ (-)\ \mathrm{II}_1\,\mathrm{III}_1 \backsim 41^2-37\cdot 4^2=3^2\cdot 11^2. \end{array}$$

Partons ensuite des équations

$$8^2-37\cdot 1^2 = 27,\quad 26^2-37\cdot 3^2 = 343,\quad 1^2-37\cdot 6^2 = -1331,$$

nous aurons, en multipliant les deux premières,

$$97^2-37\cdot 2^2 = 3^3\cdot 7^3,\quad 64^2-37\cdot 19^2 = -3^3\cdot 7^3,$$

multiplions ensuite ces deux équations par celle-ci

$$1^2-37\cdot 6^2 = -1331,$$

nous aurons les quatre solutions primitives de l'équation

$$u^2-37\,v^2 = \pm 231^3 \tag{2}$$

déterminées par les égalités

$$\mathrm{I}_1^3 \backsim 347^2-37\cdot 580^2 = -231^3,\ \mathrm{III}_1^3 \backsim 541^2-37\cdot 584^2 = -231^3$$
$$\mathrm{II}_1^3 \backsim 4154^2-37\cdot 265^2 = 231^3,\ 4282^2-37\cdot 403^2 = 231^3.$$

Les nombres premiers

$$2 \quad 11 \quad 13 \quad 29$$

sont de la hauteur 3 par rapport à la base 257, car on aura

$$13^2-257\cdot 1^2 = -88,\ 19^2-257\cdot 1^2 = 104,\ 5^2-257\cdot 1^2 = -232,$$

et 32 est le plus petit paramètre applicable pour 257.

De plus, on trouve

$$20^2-257\cdot 1^2 = 143,\ 24^2-257\cdot 1^2 = 319,\ 44^2-257\cdot 3^2 = -377,$$

ce qui détermine les trois solutions primitives de l'équation

$$u^2-257\,v^2 = \pm\,\omega,\quad \omega = 8\cdot 11\cdot 13\cdot 29 = 34316 \tag{3}$$

par les égalités

$$157^2-257\cdot 15^2 = -\omega,\quad 199^2-257\cdot 5^2 = \omega,$$
$$357^2-257\cdot 25^2 = -\omega.$$

Enfin, nous avons à étudier la base 79; les nombres premiers

$$3 \quad 5 \quad 7 \quad 13$$

sont de la hauteur 3, et nous aurons

$$8^2-79\cdot 1^2 = -15,\ 10^2-79\cdot 1^2 = 21,\ 26^2-79\cdot 3^2 = -35$$
$$35^2-79\cdot 4^2 = -39,\ 12^2-79\cdot 1^2 = 65,\ 15^2-79\cdot 2^2 = -91,$$

ce qui donnera

$$37^2-79\cdot 4^2 = 105,\quad 11^2-79\cdot 2^2 = -195$$
$$73^2-79\cdot 8^2 = 273,\quad 16^2-79\cdot 3^2 = -355,$$

de sorte que les trois solutions primitives de l'équation

$$u^2-79v^2 = 1365 \tag{4}$$

se déterminent par les égalités

$$38^2-79\cdot 1^2 = 1365,\ 41^2-79\cdot 2^2 = 1365,\ 199^2-79\cdot 22^2 = 1365.$$

CHAPITRE VI

Sur les sommes de deux carrés.

XXIII. Suppléments aux règles de Dirichlet.

Les seules bases dont l'espèce n'est pas évidente sont les nombres qui se présentent sous forme d'une somme de deux carrés, premiers entre eux, savoir

(1) $$a = \alpha^2 + \beta^2,$$

où a est un nombre composé, car les nombres premiers de cette forme sont toujours des bases de première espèce.

Quant aux nombres composés, étudions tout d'abord les deux hypothèses

(2) $$a = pq$$

(3) $$a = 2pq,$$

où p et q sont des nombres premiers impairs et inégaux, de sorte que p et q sont nécessairement tous deux de la forme $4k+1$.

Il est évident que l'équation de Legendre

(4) $$p\sigma^2 - q\tau^2 = \pm 1$$

n'est jamais résoluble, à moins que p et q ne soient résidus quadratiques l'un de l'autre.

De même, le nombre (3) ne peut être une base de seconde espèce, à moins qu'une des trois équations de Legendre

(5) $2\sigma^2 - pq\tau^2 = \pm 1, \; p\sigma^2 - 2q\tau^2 = \pm 1, \; q\sigma^2 - 2p\tau^2 = \pm 1$

ne soit résoluble, ce qui exige respectivement

$$\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = 1, \quad \left(\frac{2}{p}\right) = 1, \quad \left(\frac{2}{q}\right) = 1. \tag{6}$$

Cela posé, nous avons démontré les règles de Lejeune Dirichlet en ce qui concerne les nombres pq et $2pq$ où p et q sont des nombres premiers de la forme $4k+1$, savoir:

1° $a = 2pq$ est une base de première espèce, pourvu que

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1; \tag{7}$$

2° $a = pq$ est une base de première espèce, pourvu que

$$\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = -1. \tag{8}$$

Or, ces règles étant souvent insuffisantes pour la détermination de l'espèce du nombre (1), il faut les suppléer à l'aide de la théorie des équations de Lagrange et de Legendre.

Et l'on trouve immédiatement que le nombre (1) est une base de première espèce dans les cas suivants:

3° l'équation

$$u^2 - av^2 = -4 \tag{9}$$

est résoluble (règle de Cayley);

4° les deux équations

$$u^2 - av^2 = p^n, \quad u^2 - av^2 = -p^n \tag{10}$$

où p est un nombre premier quelconque, sont simultanément résolubles;

5° les deux équations

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

où p est un nombre premier impair, sont simultanément résolubles.

Pour obtenir d'autres règles de ce genre, désignons par p un nombre premier impair, mais quelconque du reste, puis supposons simultanément résolubles les deux équations

$$u^2 - av^2 = (-1)^\delta p^m, \quad u^2 - av^2 = (-1)^\varepsilon p^n, \tag{12}$$

je dis que cette autre équation

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

où f désigne le plus grand commun diviseur de m et n, est résoluble aussi.

En effet, supposons $m \geqq n$, l'équation (13) est certainement résoluble, pourvu que m soit multiple de n. Soit donc

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

il résulte, en vertu de (12) que cette autre équation

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

est résoluble aussi, et ainsi de suite.

Cela posé, on voit immédiatement que a est une base de première espèce, dans les cas suivants:

6° $\varphi = 0$, tandis qu'au moins un des exposants δ et ε est impair;

7° $\varphi = 1$, tandis qu'au moins un des exposants δ et ε est impair.

A ces règles nous ajoutons la suivante, bien connue:

8° les nombres

$$\alpha^2 + 1, \quad (2\alpha + 1)^2 + 4 \tag{14}$$

sont toujours des bases de première espèce.

Quant aux équations de LEGENDRE

$$(15)\qquad p\sigma^2 - q\tau^2 = (-1)^{\delta}\omega, \quad a = pq,$$

la base a est de première espèce dans les cas suivants:

9° les équations

$$(16)\qquad p\sigma^2 - q\tau^2 = r^n, \quad p\sigma^2 - q\tau^2 = -r^n,$$

où r est un nombre premier quelconque, sont simultanément résolubles;

10° les équations

$$(17)\qquad p\sigma^2 - q\tau^2 = 4r^n, \quad p\sigma^2 - q\tau^2 = -4r^n,$$

où r désigne un nombre premier impair, sont simultanément résolubles.

Étudions maintenant des cas, où la base a est de seconde espèce, ce qui a lieu dans les cas suivants:

11° $\qquad a = \alpha^2 \pm 2;$

12° $\qquad a = (2\alpha+1)^2 - 4, \quad \alpha \geqq 2;$

13° $\qquad a = \beta^2(\alpha^2\beta^2+1), \quad \beta = r^2 + s^2,$

où r et s sont premiers entre eux;

14° les équations de LAGRANGE et de LEGENDRE

$$(18)\qquad u^2 - av^2 = \pm r^n, \quad p\sigma^2 - q\tau^2 = \pm r^n; \quad a = pq,$$

où r est un nombre premier quelconque, sont simultanément résolubles;

15° une des équations

$$(19)\left\{\begin{array}{c} p\sigma^2 - q\tau^2 = \pm 1, \; p\sigma^2 - q\tau^2 = \pm 2, \; p\sigma^2 - q\tau^2 = \pm 4; \\ a = pq, \end{array}\right.$$

est résoluble.

Quant à la dernière de ces équations, supposons résoluble celle-ci

$$(20)\qquad u^2 - av^2 = -4$$

de sorte que a est une base de première espèce, puis désignons par (s_n, t_n) et (σ_n, τ_n) les éléments généraux des deux suites coordonnées, appartenant à (20), nous aurons

$$s_{2n} = \sigma_n^2 + (-1)^n 2, \quad \sigma_{2n-1} = s_n^2 - (-1)^n 2$$
$$s_{2n}^2 - a t_{2n}^2 = \sigma_{2n-1}^2 - a \tau_{2n-1}^2 = 4$$
$$s_{2n-1}^2 - a t_{2n-1}^2 = \sigma_{2n}^2 - a \tau_{2n}^2 = -4;$$

c'est-à-dire que la base a de l'équation (20) ne peut jamais admettre des équations primitives.

La règle 15° est bien connue.

XXIV. Sur les nombres $(10a \pm b)^2 + (10b \mp a)^2$.

Comme application des règles générales que nous venons de développer, dans l'article précédent, j'ai examiné les 23 nombres de la forme

$$101(a^2 + b^2) = (10a \pm b)^2 + (10b \mp a)^2$$

qui sont inférieurs à 10000, et j'ai trouvé que dix-sept de ces nombres sont des bases de première espèce, savoir

101 202 1010 1313 2626 2929 3434 4141 5050
5353 5858 6161 6565 7373 7474 8282 8989,

tandis que six seulement sont de seconde espèce, savoir

505 1717 2525 3737 8585 9797.

Remarquons tout d'abord qu'il existe sept résidus quadratiques de 101 parmi les nombres premiers $4k+1$, inférieurs à 100, savoir

5 13 17 37 97,

il est évident que

202 2929 4141 5353 6161 7373 8989

sont des bases de première espèce.

De plus, les valeurs suivantes du symbole de LEGENDRE

$$\left(\frac{2}{101}\right) = -1, \ \left(\frac{2}{5}\right) = \left(\frac{2}{13}\right) = \left(\frac{2}{29}\right) = \left(\frac{2}{37}\right) = -1$$

montrent immédiatement que les nombres

$$1010 \quad 2626 \quad 5858 \quad 7474$$

sont des bases de première espèce.

Enfin, on aura

$$101 = 10^2 + 1, \quad 6565 = 81^2 + 4, \quad 8282 = 91^2 + 1,$$

nombres qui sont certainement des bases de première espèce.

Restent encore les trois bases

$$1313 \quad 3434 \quad 5050,$$

et nous aurons pour

$$\begin{aligned} 1313:& \quad 36^2 - 1313 \cdot 1^2 = -17, \quad 32^2 - 1313 \cdot 1^2 = -17^2 \\ 3434:& \quad 59^2 - 3434 \cdot 1^2 = 47, \quad 35^2 - 3434 \cdot 1^2 = -47^2; \end{aligned}$$

c'est-à-dire que ces deux nombres sont des bases de première espèce.

Quant à la dernière des bases susdites, savoir

$$5050 = 202 \cdot 5^2,$$

ou aura, pour la base 202,

$$A_1 = 3131, \quad B_1 = 221, \quad B_3 = 3 A_1^2 B_1 + 202 B_1^3 = 5 \beta_3,$$

ce qui donnera

$$A_3^2 - 5050 \beta_3^2 = -1,$$

donc 5050 est une base de première espèce.

Étudions maintenant les six bases de seconde espèce, nous aurons tout d'abord

$$2525 = 5^2 (10^2 + 1), \quad 9797 = 99^2 - 4,$$

de sorte que ces deux bases sont certainement de seconde espèce.

De plus, on aura, pour les quatres nombres qui restent encore:

$$505:\quad 5\cdot 9^2 - 101\cdot 2^2 = 1 \qquad 1717:\; 17\cdot 39^2 - 101\cdot 16^2 = 1$$
$$3737:\quad 37\cdot 38^2 - 101\cdot 23^2 = -1$$
$$8585:\quad 85\cdot 1^2 - 101\cdot 1^2 = -2^4, \quad 67^2 - 8585\cdot 1^2 = -2^{12},$$

et l'opération itérative du cinquième ordre conduira de la première de ces équations à cette autre

$$85\,\sigma^2 - 101\,\tau^2 = -2^{12},$$

donc 8585 est une base de seconde espèce.

TABLES NUMÉRIQUES

Table Première. La base 41 (32,5).

$$u^2 - 41 v^2 = \pm \omega.$$

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
—5	6	1	8	7	1	—16	5	1
23	8	1	—25	4	1	31	20	3
32	3	1	—37	2	1	-40_1	1	1
40_2	9	1	—43	11	2	59	10	1
61	15	2	—64	31	5	73	27	4
80_1	11	1	-80_2	17	3	—83	9	2
103	12	1	—107	37	6	—113	16	3
-115_1	7	2	115_2	22	3	125	17	2
—127	23	4	128	13	1	131	34	5
—139	5	2	-155_1	3	2	155_2	14	1
160_1	23	3	-160_2	43	7	—163	1	2
—173	14	3	184_1	15	1	-184_2	29	5
185_1	29	4	185_2	53	8	197	19	2
-200_1	13	3	200_2	47	7	215_1	16	1
-215_2	21	4	—223	49	8	—241	28	5
248_1	17	1	-248_2	11	3	—251	35	6
256	25	3	—269	10	3	271	36	5
277	21	2	283	18	1	-295_1	19	4
295_2	48	7	-296_1	27	5	-296_2	55	9
305_1	31	4	-305_2	8	3	307	26	3
320_1	19	1	-320_2	7	3	—337	68	11

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
344_1	5	3	344_2	37	5	—349	26	5
—353	4	3	359	20	1	$—365_1$	2	3
365_2	23	2	—367	17	4	$—368_1$	1	3
368_2	73	11	373	43	6	—379	61	10
389	67	10	400_1	21	1	400_2	61	9
401	55	8	—409	40	7	415_1	28	3
$—415_2$	47	8	419	38	5	—431	15	4
433	31	4	443	22	1	—449	24	5
461	25	2	467	86	13	472_1	29	3
$—472_2$	67	11	—487	13	4	488_1	23	1
$—488_2$	39	7	491	50	7	$—496_1$	23	5
496_2	39	5	—512	53	9	$—515_1$	31	6
515_2	74	11	523	62	9	—529	80	13
535_1	24	1	$—535_2$	11	4	—541	22	5
565_1	27	2	$—565_2$	38	7	569	35	4
$—575_1$	9	4	$—575_2$	73	12	584_1	25	1
$—584_2$	21	5	592_1	31	3	592_2	51	7
—599	45	8	—607	7	4	613	93	14
—617	52	9	—619	59	10	625	57	8
—631	5	4	635_1	26	1	$—635_2$	29	6
$—640_1$	37	7	640_2	87	13	—647	3	4
655_1	1	4	655_2	32	3	661	69	10
$—664_1$	19	5	664_2	75	11	677	29	2
688_1	27	1	$—688_2$	79	13	695_1	52	7
$—695_2$	99	16	—701	18	5	713_1	37	4
$—713_2$	36	7	733	47	6	$—736_1$	17	5
$—736_2$	65	11	739	42	5	743	28	1
—761	92	15	—769	16	5	$—775_1$	43	8
775_2	64	9	787	34	3	797	31	2
800_1	29	1	800_2	53	7	—811	85	14
815_1	76	11	815_2	88	13	—821	50	9

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
824_1	43	5	-824_2	105	17	-829	14	5
-851_1	25	6	-851_2	57	10	-853	34	7
856_1	35	3	-856_2	13	5	857	59	8
859	30	1	-863	71	12	865_1	39	4
-865_2	64	11	877	119	18	-881	12	5
-904_1	11	5	904_2	65	9	907	54	7
911	44	5	-920_1	33	7	-920_2	49	9
920_3	31	1	920_4	113	17	925_1	33	2
925_2	49	6	941	71	10	-944_1	9	5
-944_2	91	15	-947	23	6	953	107	16
-961	8	5	-976_1	7	5	-976_2	101	15
983	32	1	-985_1	32	7	985_2	83	12
989_1	6	5	989_2	95	14	-992_1	63	11
992_2	89	13	1000_1	37	3	-1000_2	77	13

Table II. La base **30** (11,2).

$$u^2 - 30\,v^2 = (-1)^{\delta}\,\omega.$$

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
19	7	1	-29	1	1	49	13	2
-71	7	2	91_1	19	3	91_2	11	1
-101	13	3	-119_1	1	2	-119_2	19	4
139	13	1	-149	11	3	169	17	2
-191	17	4	211	31	5	-221_1	7	3
-221_2	23	5	-239	29	6	241	19	2
259_1	17	1	259_2	23	3	-269	1	3
289	37	6	-311	13	4	331	19	1
-359	11	4	361	29	4	379	43	7
-389	19	5	409	23	2	-431	7	4
-461	17	5	-479	1	4	481_1	31	4

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
481_2	49	8	499	23	1	-509	31	7
-551_1	23	6	-551_2	37	8	571	29	3
-581_1	13	5	-581_2	43	9	-599	49	10
601	41	6	619	37	5	-629_1	11	5
-629_2	29	7	691	31	3	-701	7	5
-719	19	6	721_1	29	2	721_2	61	10
739	47	7	-749_1	1	5	-749_2	41	9
769	43	6	-791_1	17	6	-791_2	47	10
811	29	1	-821	53	11	-839	59	12
841	31	2	859	67	11	889_1	37	4
889_2	53	8	-911	13	6	931_1	31	1
931_2	41	5	-941	23	7	-959_1	11	6
-959_2	31	8						

Les équations principales $5\alpha^2 - 6\beta^2 = (-1)^\delta \omega$.

$\pm\omega$	α	β	$\pm\omega$	α	β	$\pm\omega$	α	β
-1	1	1	-19	1	2	29	5	4
-49	1	3	71	5	3	-91_1	1	4
-91_2	5	6	101	5	2	119_1	11	9
119_2	5	1	-139	7	8	149	7	4
-169	5	7	191	7	3	-211	1	6
221_1	11	8	221_2	7	2	239	7	1
-241	7	9	-259_1	11	12	-259_2	5	8
269	17	14	-289	1	7	311	11	7
-331	13	14	359	13	9	-361	5	9
-379	1	8	389	11	6	-409	11	13
431	17	13	461	13	8	479	23	19
-481_1	7	11	-481_2	1	9	-499	17	18
509	11	4	551_1	13	7	551_2	11	3
-571	11	14	581_1	17	12	581_2	11	2
599	11	1	-601	5	11	-619	7	12

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
629_1	19	14	629_2	13	6	-691	13	16
701	23	18	719	17	11	-721_1	17	19
-721_2	1	11	-739	5	12	749_1	29	24
749_2	13	4	-769	7	13	791_1	19	13
791_2	13	3	-811	23	24	821	13	2
839	13	1	-841	19	21	-859	1	12
-889_1	13	17	-889_2	5	13	911	23	17
-931_1	25	26	-931_2	11	16	941	19	12
959_1	25	19	959_2	17	9			

Les équations simultanées

$$2s^2 - 15t^2 = 3\sigma^2 - 10\tau^2 = (-1)^\delta \omega.$$

$\pm\omega$	s	t	σ	τ	$\pm\omega$	s	t	σ	τ	$\pm\omega$	s	t	σ	τ
-7	2	1	1	1	-13	1	1	3	2	17	4	1	3	1
-37	7	3	1	2	83	7	1	9	4	-103	4	3	7	5
107	11	3	7	2	113	8	1	11	5	-127	2	3	11	7
-133_1	1	3	13	8	-133_2	11	5	17	10	137	16	5	7	1
-157	8	5	1	4	203_1	13	3	9	2	203_2	17	5	11	4
-223	16	7	3	5	227	11	1	17	8	233	22	7	9	1
-247_1	8	5	1	5	-247_2	17	9	9	7	257	14	3	13	5
-277	7	5	11	8	323_1	13	1	11	2	323_2	23	7	21	10
-343	4	5	17	11	347	19	5	13	4	353	28	9	11	1
-367	2	5	21	13	-373	1	5	23	14	377_1	14	1	17	7
377_2	16	3	23	11	-397	13	7	9	8	443	17	3	19	8
-463	26	11	3	7	467	29	9	13	2	-487	32	13	1	7
-493_1	11	7	7	8	-493_2	19	9	13	10	497_1	16	1	13	1
497_2	44	15	27	13	563	17	1	29	14	587	19	3	23	10
593	22	5	19	7	-607	8	7	19	13	-613	31	13	3	8
617	26	7	17	5	-637_1	17	9	11	10	-637_2	43	17	1	8
683	23	5	21	8	-703_1	4	7	27	17	-703_2	16	9	13	11

$\pm\omega$	s	t	σ	τ	$\pm\omega$	s	t	σ	τ	$\pm\omega$	s	t	σ	τ
707_1	19	1	33	16	707_2	31	9	17	4	—727	2	7	31	19
—757	23	11	9	10	—823	14	9	17	13	827	41	13	17	2
833_1	22	3	29	13	833_2	32	9	19	5	—853	29	13	7	10
857	46	15	17	1	—877	13	9	19	13	923_1	37	11	19	4
923_2	23	3	31	14	947	29	7	23	8	953	22	1	39	19
—967	28	13	9	11	—973_1	11	9	3	10	—973_2	41	17	23	16
977	26	5	27	11	—997	47	19	1	10					

Table III. La base 51 (50,7).

$$u^2 - 51\,v^2 = (-1)^\delta \omega.$$

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
—2	7	1	13	8	1	25	22	3
—26	5	1	—35_1	4	1	—35_2	13	2
—47	2	1	49	10	1	—50	1	1
—59	20	3	70_1	11	1	70_2	23	3
—83	11	2	94	37	5	—98	19	3
118	13	1	145_1	14	1	145_2	31	4
—155_1	7	2	—155_2	41	6	157	19	2
166	25	3	169	38	5	—179	5	2
—191	25	4	—203_1	1	2	—203_2	16	3
205_1	16	1	205_2	52	7	217_1	26	3
217_2	59	8	229	73	10	—239	55	8
—251	32	5	—263	14	3	—287_1	23	4
—287_2	62	9	—290_1	13	3	—290_2	47	7
310_1	19	1	310_2	53	7	—314	31	5
325_1	23	2	325_2	28	3	—338	11	3
349	20	1	358	67	9	—359	10	3
373	47	6	382	29	3	—383	46	7

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
-395_1	8	3	-395_2	76	11	406_1	41	5
406_2	95	13	409	35	4	-410_1	7	3
-410_2	61	9	421	25	2	433	22	1
-434_1	5	3	-434_2	29	5	-443	4	3
-455_1	2	3	-455_2	19	4	-455_3	83	12
-455_4	134	19	457	61	8	-458	1	3
-467	37	6	478	13	1	-491	28	5
502	31	3	526	55	7	553_1	37	4
553_2	82	11	-563	44	7	565_1	32	3
565_2	49	6	574_1	25	1	574_2	43	5
577	89	12	-587	97	14	-599	26	5
-611_1	35	6	-611_2	67	10	613	103	14
625	26	1	637_1	29	2	637_2	124	17
-647	13	4	-650_1	43	7	-650_2	59	9
-659	104	15	661	44	5	-695_1	11	4
-695_2	74	11	-698	89	13	718	83	11
733	28	1	-746	23	5	757	31	2
766	35	3	-767	7	4	769	70	9
790_1	29	1	790_2	97	13	-791_1	5	4
-791_2	22	5	-815_1	1	4	-815_2	118	17
-818	41	7	829	77	10	841	46	5
-842	73	11	-863	49	8	865_1	58	7
865_2	41	4	-866	103	15	-875_1	31	6
-875_2	88	13	886	125	17	-899_1	40	7
-899_2	125	18	910_1	37	3	910_2	31	1
-914	19	5	934	47	5	937	91	12
961	65	8	-971	95	14	973_1	32	1
973_2	53	6	982	59	7	985_1	38	3
985_2	98	13	-995_1	29	6	-995_2	56	9

Les équations simultanées

$$3s^2 - 17t^2 = \pm\omega\,,\quad 3\sigma^2 - 17\tau^2 = \mp 2\omega.$$

$\pm\omega$	s	t	σ	τ	$\pm\omega$	s	t	σ	τ	$\pm\omega$	s	t	σ	τ
-5	2	1	3	1	7	5	2	1	1	-29	9	4	5	1
31	4	1	11	5	-41	3	2	13	5	-65_1	1	2	27	11
-65_2	16	7	7	1	79	7	2	15	7	91_1	6	1	25	11
91_2	11	4	9	5	-113	23	10	9	1	-125	7	4	19	7
139	18	7	7	5	163	14	5	13	7	-173	30	13	11	1
175_1	8	1	39	17	175_2	9	2	29	13	-197	5	4	33	13
199	32	13	3	5	211	39	16	1	5	-233	8	5	29	11
235_1	13	4	23	11	235_2	21	8	11	7	-245_1	3	4	47	19
-245_2	37	16	13	1	-269	1	4	61	25	283	10	1	53	23
295_1	11	2	43	19	295_2	28	11	9	7	-317	6	5	43	17
-329_1	24	11	19	5	-329_2	44	19	15	1	343	16	5	27	13
367	20	7	21	11	-377_1	4	5	57	23	-377_2	21	10	23	7
379	42	17	5	7	-401	12	7	35	13	403	15	4	37	17
-413_1	2	5	71	29	-413_2	15	8	31	11	415_1	12	1	67	29
415_2	56	23	1	7	439	13	2	57	25	-449	31	14	21	5
487	27	10	19	11	499	23	8	25	13	-521	28	13	25	7
-533_1	10	7	49	19	-533_2	58	25	19	1	547	18	5	41	19
571	14	1	81	35	-581_1	13	8	45	17	-581_2	38	17	23	5
607	15	2	71	31	-617	19	10	37	13	619	22	7	35	17
-641	8	7	63	25	643	30	11	23	13	-653	65	28	21	1
-677	35	16	27	7	691	41	16	15	11	-725_1	6	7	77	31
-725_2	11	8	59	23	751	16	1	95	41	775_1	37	14	21	13
775_2	48	19	13	11	-785_1	4	7	91	37	-785_2	72	31	23	1
787	25	8	39	19	-809	29	14	35	11	811	19	4	65	29
-821	2	7	105	43	823	29	10	33	17	-845_1	9	8	73	29
-845_2	42	19	29	7	-857	20	11	47	17	-881	52	23	27	5
895	24	7	49	23	895_2	44	17	19	13	907	62	25	9	11
-921	79	34	25	1	-941	7	8	87	35	955_1	18	1	109	47
955_2	69	28	7	11	991	76	31	5	11					

Table IV. La base **130** (57,5).

$$u^2 - 130v^2 = \pm\omega.$$

$\pm\omega$	u	v	$\pm\omega$	u	v	$\pm\omega$	u	v
-9	11	1	-49	9	1	-79	21	2
-81	7	1	-121	3	1	-129_1	1	1
-129_2	47	4	159_1	17	1	-159_2	19	2
-191	67	6	199	37	3	209_1	27	2
-209_2	31	3	-231_1	17	2	231_2	59	5
-231_3	43	4	231_4	19	1	311	21	1
-321_1	19	2	321_2	49	4	361	71	6
-329_1	29	3	329_2	93	8	399_1	23	1
-399_2	11	2	-399_3	41	4	-399_4	89	8
-439	9	2	441	31	2	-441_2	53	5
-471_1	7	2	471_2	61	5	-511_1	3	2
511_2	41	3	-519_1	1	2	519_2	83	7
521	51	4	569	33	2	599	27	1
-601	123	11	-641	23	8	-649_1	51	5
649_2	73	6	679_1	43	3	-679_2	111	10
711_1	29	1	-711_2	33	4	719	63	5
729	53	4	-751	87	8	-809	19	3
831_1	31	1	831_2	151	13	-849_1	49	5
849_2	37	2	-881	17	3	911	129	11
919	107	9	959_1	33	1	-959_2	61	6
-991	33	4						

$$2\sigma^2 - 65\tau^2 = \pm\omega.$$

$\pm\omega$	σ	τ	$\pm\omega$	σ	τ	$\pm\omega$	σ	τ
7	6	1	-33_1	4	1	33_2	7	1
-47	3	1	-57_1	2	1	-57_2	28	5
-63_1	1	1	63_2	8	1	-73	16	3
97	9	1	137	19	3	-167	27	5
177_1	11	1	177_2	41	7	-193	14	3

$\pm\omega$	σ	τ	$\pm\omega$	σ	τ	$\pm\omega$	σ	τ
223	12	1	297_1	31	5	-297_2	38	7
327_1	14	1	327_2	64	11	-343	11	3
-353	53	9	383	22	3	423_1	32	5
-423_2	61	11	447_1	16	1	-447_2	37	7
-457	8	3	-463	49	9	473_1	23	3
-473_2	24	5	-487	7	3	513_1	17	1
513_2	43	7	-553_1	4	3	553_2	33	5
-567_1	23	5	567_2	76	13	-577	2	3
-583_1	1	3	-583_2	18	1	-593	36	7
-617	72	13	657_1	19	1	-657_2	22	5
687_1	34	5	687_2	44	7	-743	21	5
-847_1	47	9	-847_2	83	15	863	88	15
873_1	34	7	873_2	77	13	-903_1	19	5
-903_2	59	11	-903_3	71	13	903_4	22	1
967	36	5	977	18	5	983	28	3
993_1	23	1	-993_2	106	19			

$$5\sigma^2 - 26\tau^2 = \pm\omega.$$

$\pm\omega$	σ	τ	$\pm\omega$	σ	τ	$\pm\omega$	σ	τ
11	7	3	19	3	1	-21_1	1	1
21_2	5	2	-59	3	2	-99_1	1	2
99_2	5	1	-109	5	3	141_1	7	2
141_2	19	8	-149	15	7	-171_1	7	4
171_2	17	7	189_1	11	4	-189_2	23	13
219_1	7	1	-219_2	17	8	-229	1	3
-291_1	5	4	-291_2	31	14	301_1	9	2
-301_2	19	9	-331	11	6	349	33	14
-371_1	3	4	371_2	11	3	379	9	1
-411_1	1	4	411_2	31	13	-421	47	21
461	29	12	499	27	11	501_1	11	2

$\pm\omega$	σ	τ	$\pm\omega$	σ	τ	$\pm\omega$	σ	τ
-501_2	23	11	509	17	6	531_1	19	7
-531_2	35	16	-539_1	17	8	539_2	23	9
541	21	8	579_1	11	1	-579_2	49	22
-619	23	12	-661	17	9	-669_1	11	7
-669_2	13	17	-691	7	6	709	15	4
739	45	19	-749_1	27	13	-749_2	51	23
-811	5	6	821	43	18	-869_1	9	7
869_2	19	6	-931_1	1	6	-931_2	53	24
981_1	23	8	-981_2	41	19			

$$10\sigma^2 - 13\tau^2 = \pm\omega.$$

$\pm\omega$	σ	τ	$\pm\omega$	σ	τ	$\pm\omega$	σ	τ
-3	1	1	27	2	1	43	4	3
-53	10	9	77_1	3	1	-77_2	2	3
-107	1	3	133_1	5	3	-133_2	12	11
147_1	4	1	147_2	22	19	157	11	9
173	9	7	237_1	5	1	-237_2	14	13
243	20	17	-277	6	7	283	38	33
347	6	1	363_1	10	7	-363_2	16	13
373	7	3	-387_1	5	7	387_2	14	11
-413_1	8	9	413_2	27	23	-443	23	21
-467	37	33	477_1	7	1	-477_2	4	7
-517_1	18	17	517_2	25	21	523	8	3
-547	3	7	-563	7	9	-573_1	10	11
573_2	11	7	-597_1	2	7	597_2	23	19
627_1	8	1	-627_2	25	23	-627_3	1	7
-627_4	34	29	653	21	17	677	15	11
-693_1	20	19	-693_2	23	29	693_3	17	13
693_4	43	37	-757	12	13	-763_1	9	11
763_2	32	27	797	9	1	803_1	12	7

CHAPITRE V

Sur l'opération du troisième ordre.

CHAPITRE VI

Sur les sommes de deux carrés.

TABLES NUMÉRIQUES

Forelagt paa Mødet den 14. December 1923.
Færdig fra Trykkeriet den 12. Juni 1924.