Det Kgl. Danske Videnskabernes Selskab.
Mathematisk-fysiske Meddelelser. **V**, 7.

NOTES SUPPLÉMENTAIRES

SUR LES

ÉQUATIONS DE LAGRANGE

ÉTUDE DE NIELS NIELSEN ET GEORG RASCH

PUBLIÉE PAR

NIELS NIELSEN

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

I.

Sur le rang d'un nombre premier.

Soit la base a résidu quadratique du nombre premier impair p, nous avons récemment démontré, M. RASCH et moi[1], que le rang de p par rapport à la base a est diviseur de $p-1$.

Plus tard nous avons poussé un peu plus loin nos recherches sur le rang des nombres premiers, et M. RASCH a démontré le théorème intéressant:

I. Soit r le rang du nombre premier impair p, par rapport à la base a, qui n'est pas multiple de p, on aura, quels que soient du reste a et p,

$$p-\left(\frac{a}{p}\right) \equiv 0 \pmod{r}, \tag{1}$$

où $\left(\frac{a}{p}\right)$ désigne, comme ordinairement, le symbole de LEGENDRE.

En appliquant, avec certaines modifications, la démonstration de M. RASCH, nous partons des formules de LAGRANGE

$$A_p = \sum_{s=0}^{s=\frac{p}{2}} \binom{p}{2s} a^s B_1^{2s} A_1^{p-2s}$$

$$B_p = \sum_{s=0}^{s=\frac{p-1}{2}} \binom{p}{2s+1} a^s B_1^{2s+1} A_1^{p-2s-1},$$

[1] Voir l'article XV de mon Mémoire: Recherches sur les équations de LAGRANGE.

et en déduisons les congruences

$$A_p \equiv A_1^p \equiv A_1 \pmod{p} \tag{2}$$

$$B_p \equiv a^{\frac{p-1}{2}} B_1^p \equiv \left(\frac{a}{p}\right) B_1 \pmod{p}. \tag{3}$$

Posons ensuite, dans l'équation de FERMAT ayant la base a,

$$A_1^2 - aB_1^2 = (-1)^\varepsilon, \tag{4}$$

les formules d'addition de LAGRANGE

$$A_{p-1} = (-1)^\varepsilon (A_1 A_p - a B_1 B_p), \quad B_{p-1} = (-1)^\varepsilon (A_1 B_p - B_1 A_p)$$
$$A_{p+1} = A_1 A_p + a B_1 B_p, \qquad B_{p+1} = A_1 B_p + B_1 A_p$$

donnent immédiatement, en vertu de (2) et (3),

$$A_{p-1} \equiv (-1)^\varepsilon \left(A_1^2 - \left(\frac{a}{p}\right) a B_1^2\right) \pmod{p} \tag{5}$$

$$B_{p-1} \equiv (-1)^\varepsilon \left(1 - \left(\frac{a}{p}\right)\right) A_1 B_1 \pmod{p} \tag{6}$$

$$A_{p+1} \equiv A_1^2 + \left(\frac{a}{p}\right) a B_1^2 \pmod{p} \tag{7}$$

$$B_{p+1} \equiv \left(1 + \left(\frac{a}{q}\right)\right) A_1 B_1 \pmod{p}. \tag{8}$$

Soit maintenant a résidu de p, savoir

$$\left(\frac{a}{p}\right) = 1,$$

il résulte, en vertu de (5) et (6),

$$A_{p-1} \equiv 1 \pmod{p} \tag{9}$$

$$B_{p-1} \equiv 0 \pmod{p}, \tag{10}$$

et la dernière de ces deux congruences donnera immédiatement

$$p - 1 \equiv 0 \pmod{r}. \tag{11}$$

Soit, au contraire, a non-résidu de p, savoir

$$\left(\frac{a}{p}\right) = -1,$$

les congruences (7) et (8) donnent de même

$$A_{p+1} \equiv (-1)^{\varepsilon} \pmod{p} \tag{12}$$

$$B_{p+1} \equiv 0 \pmod{p}, \tag{13}$$

de sorte que l'on aura ici

$$p+1 \equiv 0 \pmod{r}. \tag{14}$$

Et il est évident que les deux congruences (11) et (14) donnent immédiatement le théorème I.

Or, il est possible de compléter les résultats ainsi obtenus.

A cet effet, partons de la formule

$$2aB_{\mu}^{2} = A_{2\mu} - (-1)^{\mu\varepsilon},$$

où μ est un positif entier quelconque, tandis que ε est l'exposant défini par la formule (4), nous aurons immédiatement, en vertu de (9) et (12), et en posant respectivement $2\mu = p-1$, $2\mu = p+1$,

$$2aB_{\frac{p-1}{2}}^{2} \equiv 1 - (-1)^{\frac{p-1}{2}\varepsilon} \pmod{p} \tag{15}$$

$$2aB_{\frac{p+1}{2}}^{2} = (-1)^{\varepsilon} - (-1)^{\frac{p+1}{2}\varepsilon} \pmod{p}, \tag{16}$$

et la congruence (15) donnera immédiatement la proposition:

II. Soit a une base de seconde espèce, ou soit p de la forme $4k+1$, on aura toujours

$$\frac{p-1}{2} \equiv 0 \pmod{r}, \tag{17}$$

de sorte que le rang de p est une aliquote de $p-1$.

Quant à la congruence (16), elle se présente aussi sous la forme

$$(18) \qquad 2aB^2_{\frac{p+1}{2}} \equiv (-1)^{\varepsilon}\left(1-(-1)^{\frac{p-1}{2}\varepsilon}\right) \pmod{r},$$

ce qui donnera cette autre proposition, analogue à la précédente:

III. Soit a une base de seconde espèce, ou soit p de la forme $4k+1$, on aura toujours

$$(19) \qquad \frac{p+1}{2} \equiv 0 \pmod{r},$$

de sorte que le rang de p est une aliquote de $p+1$.

Cela posé, il est évident que la valeur maximum $p-1$ ou $p+1$ du nombre premier p est toujours exclue, à moin que la base ne soit de première espèce et le nombre premier p soit de la forme $4k+3$.

On voit immédiatement que le théorème III, p. 65 de mon Mémoire susdit, n'est pas démontré, parce que la remarque jointe à ce théorème est erronée, et il est facile de voir que le théorème susdit est faux, car le nombre premier

$$239 = 4 \cdot 59 + 3$$

est, par rapport à la base 2, du rang 14, et l'on aura

$$238 = 14 \cdot 17.$$

Mais quoi qu'il en soit, il existe des nombres premiers p du rang $p \pm 1$.

Soit par exemple $a = 2$, 7 est du rang 6, 11 du rang 12.

Dans l'article qui suit, nous avons à démontrer des propriétés interessantes des nombres premiers du rang maximum.

II.

Sur les nombres premiers du rang maximum.

Les nombres premiers du rang maximum, par rapport à un certaine base a, jouent un rôle assez important pour les équations de Lagrange ayant la base a, ce qui est mis en pleine lumière par les théorèmes suivants:

I. Supposons que le nombre premier p, du rang $p-1$ par rapport à la base a, ne divise pas le paramètre ω, les deux équations de LAGRANGE

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

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

En effet, soit

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

une suite quelconque, formée des solutions de la première des équations (1), il s'agit de démontrer une congruence de la forme

$$(3) \qquad v_\mu \equiv 0 \pmod{p}, \quad 1 \leq \mu \leq p-1,$$

pourvu que le paramètre ω ne soit pas multiple de p.

A cet effet, considérons tout d'abord l'hypothèse $\mu = 1$, savoir

$$(4) \qquad v_1 \equiv 0 \pmod{p},$$

le nombre premier p est, par rapport à la suite (2), de l'ordre 1.

Appliquons ensuite la congruence

$$A_{2\nu+1} \equiv 0 \pmod{p}, \quad p = 4\nu+3, \tag{5}$$

démontrée par M. RASCH, dans mon Mémoire susdit, il résulte, en vertu de la formule récursive générale

$$v_{r+1} = u_1 B_r + v_1 A_r, \tag{6}$$

que la congruence

$$v_{2\nu+2} \equiv 0 \pmod{p} \tag{7}$$

entraîne cette autre

$$u_1 \equiv 0 \pmod{p}. \tag{7 bis}$$

Abstraction faite de ces deux cas spéciaux, nous avons donc à étudier les congruences

$$u_1 B_r + v_1 A_r \equiv 0 \pmod{p}, \tag{8}$$

où ni u_1 ni v_1 n'est multiple de p.

A cet effet, supposons ou

$$1 \leqq r \leqq 2\nu \tag{9}$$

ou

$$2\nu+2 \leqq r \leqq 4\nu+1, \tag{9 bis}$$

puis posons

$$u_1 = \alpha + pk, \quad v_1 = \beta + pk_1, \tag{10}$$

où k et k_1 sont des entiers non négatifs, tandis que

$$1 \leqq \alpha \leqq p-1, \quad 1 \leqq \beta \leqq p-1, \tag{10 bis}$$

nous désignons par le symbole (α, β) les deux équations (10), suppléées par les conditions (10 bis), et la congruence (8) se transforme en celle-ci

$$A_r \beta + B_r \alpha \equiv 0 \pmod{p}. \tag{11}$$

Supposons ensuite tout d'abord que r soit un indice fixe, puis introduisons, dans (11), successivement

$$\alpha = 1, 2, 3, \ldots, p-1, \tag{12}$$

nous aurons, pour β, les valeurs inégales

$$\beta = s_1^{(r)}, s_2^{(r)}, \ldots . s_{p-1}^{(r)}, \tag{12 bis}$$

de sorte que ces valeurs de β ne sont autre chose que les nombres (12), pris dans un ordre inconnu.

Cela posé, nous avons tout d'abord à démontrer l'impossibilité d'une équation de la forme

$$s_\mu^{(r)} = s_\mu^{(q)},$$

où r et q sont des indices inégaux.

A cet effet, supposons que les deux congruences

$$A_r\beta + B_r\alpha \equiv 0 \pmod{p}$$
$$A_q\beta + B_q\alpha \equiv 0 \pmod{p}$$

soient satisfaites par les mêmes valeurs du couple (α, β), nous aurons, en éliminant β, puis supposant $q > r$,

$$B_{q-r}\alpha \equiv 0 \pmod{p},$$

ce qui est impossible parce que ni α ni B_{q-r} ne peut être multiple de p, car on aura évidemment

$$q - r < p - 1,$$

et B_{p-1} est le premier des nombres B_μ qui soit divisible par p.

Ces remarques faites, il est évident que les

$$4\nu(p-1) = (p-1)(p-3)$$

valeurs du couple (α, β), ainsi déterminées à l'aide des nombres (12) et (12 bis), sont inégales, de sorte qu'il ne nous reste que d'étudier la congruence

$$u^2 - av^2 \equiv 0 \pmod{p}, \tag{14}$$

toujours résoluble, parce que a est résidu quadratique de p.

A cet effet, désignons par

$$r_1, r_2, \ldots, r_{2\nu+1}, \quad 1 \leqq r_\varkappa \leqq p-1 \tag{15}$$

les résidus quadratiques de p, de sorte que

$$r_\sigma \equiv a \pmod{p}, \tag{15 bis}$$

la congruence (14) n'est autre chose que celle-ci

$$r_\gamma \equiv r_\sigma r_\varkappa \pmod{p}, \tag{16}$$

et cette congruence est certainement résoluble, parce que p et r_σ sont premiers entre eux.

Quant aux valeurs de u et v, tirées de la congruence (14), posons

$$r_\mu \equiv \alpha_\mu^2 \equiv (p-\alpha_\mu)^2 \pmod{p},$$

où nous avons constamment

$$1 \leqq \alpha_\mu \leqq p-1$$

pour toutes les valeurs de l'indice μ, savoir

$$1 \leqq \mu \leqq 2\nu+1.$$

Remarquons ensuite que la congruence (16) exclut cette autre

$$r_\lambda \equiv r_\sigma r_\mu \pmod{p}, \quad \varkappa \neq \mu,$$

il est évident que la congruence (16) donnera précisément

$$2p-2$$

valeurs inégales du couple (α, β), savoir, pour α les valeurs

$$\alpha = \alpha_\lambda, \quad \alpha = p-\alpha_\lambda, \tag{17}$$

et, pour β les valeurs correspondantes

$$\beta = \alpha_\varkappa, \quad \beta = p-\alpha_\varkappa \tag{18}$$

ou

(18 bis) $$\beta = p - \alpha_z, \quad \beta = \alpha_z.$$

Cela posé, nous avons encore à démontrer que les $2p-2$ valeurs du couple (α, β) ainsi déterminées, par les formules (17) et (18), sont différentes des $(p-1)(p-3)$ valeurs du couple (α, β), déterminées par les congruences (11).

Or, supposons que les deux congruences

$$A_r\beta + B_r\alpha \equiv 0 \pmod{p}$$
$$\alpha^2 - a\beta^2 \equiv 0 \pmod{p}$$

soient simultanément résolubles, nous aurons, en éliminant α,

$$(A_r^2 - aB_r^2)\beta^2 \equiv (-1)^r\beta^2 \equiv 0 \pmod{p},$$

ce qui est inadmissible, parce que β n'est pas divisible par p.

Les valeurs du couple (α, β), déterminées par les formules (12), (17) et (18), épuisent donc toutes les $(p-1)^2$ valeurs possibles de ce couple, de sorte que, ω n'étant pas multiple de p, les deux équations (1) sont simultanément résolubles ou non, et, en cas de résolubilité, ces deux équations sont du même genre parce que (2) est une suite quelconque, formée des solutions de la première de ces deux équations.

Quant au calcul des solutions de la dernière des équations susdites, savoir

(19) $$u^2 - (ap^2)v^2 = (-1)^\delta\omega,$$

à l'aide de celles de la première de ces deux équations, appliquons les formules récursives de LAGRANGE

$$A_{k+r} = A_kA_r + aB_kB_r, \qquad B_{k+r} = A_kB_r + B_kA_r$$
$$(-1)^kA_{k-r} = A_kA_r - aB_kB_r, \quad (-1)^kB_{k-r} = B_kA_r - A_kB_r,$$

où il faut admettre, dans les deux dernières, $k > r$, puis posons

$$k = \frac{p-1}{2} = 2\nu + 1,$$

il résulte, en vertu de (5)

$$(20)\quad \begin{cases} A_{k+r} \equiv A_{k-r} \pmod{p} \\ B_{k+r} \equiv -B_{k-r} \pmod{p}, \end{cases}$$

ce qui donnera la proposition:

II. Supposons remplies les conditions indiquées dans le théorème I, une des congruences

$$(21)\quad A_r v_1 \pm B_r u_1 \equiv 0 \pmod{p}, \quad 1 \leqq r \leqq \frac{p-3}{2},$$

est toujours résoluble.

Quant à la solution primitive d'une suite formée de solutions de l'équation (19), supposons applicable, dans la congruence (21), le signe positif, p est de l'ordre $r+1$, et la solution primitive de la suite susdite appartenant à l'équation (19) deviendra

$$(22)\quad \left(u_1 A_r + a v_1 B_r, \quad \frac{1}{p}(v_1 A_r + u_1 B_r)\right).$$

Soit, au contraire, valable la congruence (21) pour le signe négatif, le nombre premier p divise

$$v_{2k-r+1} = v_{p-r}$$

et par conséquent aussi le nombre

$$v'_r,$$

où (u'_n, v'_n) est l'élément général de la suite coordonnée à celle qui contient (u_n, v_n), et la solution primitive deviendra, dans ce cas,

$$(23)\quad \left(u'_1 A_{r-1} + a v'_1 B_{r-1}, \quad \frac{1}{p}(u'_1 B_{r-1} + v'_1 A_{r-1})\right),$$

où il faut admettre, comme ordinairement,

$$A_0 = 1, \quad B_0 = 0.$$

Or, les formules fondamentales de la théorie des suites coordonnées donnent, en vertu de (23), pour la solution primitive du couple susdit, cette autre expression

$$\text{(23 bis)} \qquad \left(| u_r A_r - a v_1 B_r |, \quad \frac{1}{p} | u_1 B_r - v_1 A_r | \right),$$

de sorte que le calcul de la solution (u'_1, v'_1) réciproque de (u_1, v_1) n'est pas nécessaire pour la détermination de l'élément primitif des deux suites coordonnées appartenant à l'équation (19).

Quant aux cas spéciaux qui correspondent à une des congruences (4) et (7 bis), on aura, comme élément primitif des suites coordonnées appartenant à l'équation (19)

$$\text{(24)} \qquad \left(u_1, \frac{1}{p} v_1 \right)$$

respectivement

$$\text{(24 bis)} \qquad \left(u_1 A_k + a v_1 B_k, \quad \frac{1}{p} (u_1 B_k + v_1 A_k) \right),$$

où il faut admettre

$$k = 2\nu + 1 = \frac{p-1}{2}.$$

Supposons maintenant que la base a de première espèce soit résidu quadratique du nombre premier

$$p = 4\nu + 1,$$

nous savons que le rang ϱ de p, par rapport à la base a est diviseur du nombre

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

de sorte qu'il n'est pas sûr que les deux équations (1) soient simultanément résolubles, et, en cas de résolubilité simultanée, ces deux équations ne sont pas généralement du même genre.

Dans le cas, où le rang ϱ est un nombre pair, savoir

$$\varrho = 2k,$$

nous aurons toujours

$$A_k \equiv 0 \pmod{p},$$

de sorte que la résolubilité de la seconde des équations (1) exige, abstraction faite des deux cas évidents

$$v_1 \equiv 0 \pmod{p}, \quad u_1 \equiv 0 \pmod{p},$$

l'existence d'une des congruences (21), où l'indice r satisfait aux conditions

$$1 \leqq r \leqq k-1.$$

Étudions par exemple la base la plus simple de première espèce, savoir

$$a = 2,$$

nous aurons, pour les premières solutions de l'équation de Fermat correspondante, les expressions

$$(25) \quad \begin{cases} (1,1)\ (3,2)\ (7,5)\ (17,12)\ (41,29)\ (99,70) \\ \qquad\qquad (239,169). \end{cases}$$

Cela posé, il est évident que le nombre premier 7 est du rang 6, par rapport à la base 2, supposons donc que le paramètre ω ne soit pas multiple de 7, les deux équations

$$(26) \qquad u^2 - 2v^2 = \pm\omega, \quad u^2 - 98v^2 = (-1)^{\vartheta}\omega$$

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

De plus, il résulte, en vertu de la suite (25), que le nombre premier 17 est, par rapport à la base 2, du rang 8, de sorte que la résolubilité de l'équation

$$u^2 - 378\,v^2 = (-1)^\vartheta \omega\,,$$

où tous les facteurs premiers de ω sont nécessairement, comme dans les équations (26), de la forme $8\nu \pm 1$, exige l'existence d'une des six congruences

$$\begin{aligned} v_1 \pm u_1 &\equiv 0 \pmod{17} \\ 3v_1 \pm 2u_1 &\equiv 0 \pmod{17} \\ 7v_1 \pm 5u_1 &\equiv 0 \pmod{17}. \end{aligned}$$

Quant à la seconde valeur maximum $p+1$ du nombre premier p, nous avons à démontrer le théorème:

III. Supposons que le nombre premier impair p soit, par rapport à la base a, du rang $p+1$, les deux équations de Lagrange

$$(27) \qquad u^2 - a\,v^2 = \pm\omega\,, \quad u^2 - (ap^2)\,v^2 = (-1)^\vartheta \omega$$

sont, quels que soient du reste a et p, simultanément résolubles ou non, et, en cas de résolubilité, ces deux équations sont du même genre.

En effet, posons

$$p = 2\nu + 1\,,$$

nous aurons

$$A_\nu \equiv 0 \pmod{p};$$

remarquons ensuite que les congruences (8) épuisent, pour

$$1 \leqq r \leqq \nu - 1\,, \quad \nu + 1 \leqq r \leqq 2\nu - 1\,,$$

toutes les $(p-1)^2$ valeurs possibles du couple (α, β), la démonstration du théorème III est évidente.

De plus, la solution primitive de la dernière des équa-

tions (27) se détermine à l'aide des expressions (23) et (23 bis), où il faut admettre

$$1 \leqq r \leqq \nu - 1.$$

Remarquons, en passant, que la méthode appliquée, dans la démonstration des théorèmes I et III, montrera clairement que le rang du nombre premier impair p, par rapport à une base quelconque a, ne peut jamais dépasser $p+1$, ce qui est, au contraire, possible pour le rang du nombre composé p.

Revenons maintenant à la base $a = 2$, il résulte, en vertu de la suite (25), que les nombres premiers

$$3 \quad 11 \quad 19$$

sont, par rapport à la base $a = 2$, respectivement du rang

$$4 \quad 12 \quad 20,$$

de sorte que les équations

$$(28) \quad \begin{cases} u^2 - 18v^2 = (-1)^{\delta}\omega, \quad u^2 - 242v^2 = (-1)^{\delta_1}\omega, \\ u^2 - 722v^2 = (-1)^{\delta_2}\omega \end{cases}$$

sont toujours résolubles et du genre maximum, pourvu que tous les facteurs premiers du paramètre ω soient de la forme $8\nu \pm 1$, sinon les équations (28) sont irrésolubles toutes les trois.

En terminant cette Note, nous avons encore à regarder l'hypothèse

$$a = 2, \quad p = 13;$$

remarquons que 13 est, par rapport à la base 2, du rang 7, la résolubilité de l'équation

$$(29) \qquad u^2 - 338v^2 = \pm\omega$$

exige que tous les facteurs premiers de ω soient de la forme $8\nu \pm 1$, et que 13 divise un des nombres

$$v_1, \quad v_1 + u_1, \quad 3v_1 + 2u_1, \quad 6v_1 - 5u_1,$$
$$2v_1 - u_1, \quad 2v_1 + 3u_1, \quad v_1 - u_1.$$

Or, remarquons que 13 est, par rapport à la base 2, de la hauteur 2, parce que $B_7 = 169$, il n'est pas sûr que l'équation (29), supposée résoluble, soit du genre maximum, ce qui a toujours lieu pour les équations (26) et (28).

III.

Sur la multiplication des équations de Lagrange.

Dans un Mémoire récent[1], j'ai souvent appliqué la multiplication de deux équations de Lagrange qui correspondent ou au même paramètre ou à des paramètres premiers entre eux.

M. Rasch a poussé plus loin ces recherches, en étudiant la multiplication de deux équations de Lagrange aux paramètres quelconques.

En suivant le développement de M. Rasch, nous remarquons tout d'abord que l'équation de Lagrange

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

n'est jamais résoluble, à moins que a ne soit résidu quadratique de ω; c'est-à-dire qu'il existe un positif entier b, tel que

$$a \equiv b^2 \pmod{\omega}, \tag{2}$$

ce qui donnera, en vertu de (1),

$$(u + bv)(u - bv) \equiv 0 \pmod{\omega}. \tag{3}$$

Remarquons ensuite que le nombre 2 est le seul diviseur commun des deux facteurs

$$u + bv, \quad u - bv \tag{4}$$

qui divise aussi ω, car un diviseur commun des deux nombres (4) est aussi diviseur de leur somme $2u$, et u et

[1] Recherches sur les équations de Lagrange.

ω sont premiers entre eux; c'est-à-dire qu'il existe une décomposition de la forme

$$\omega = \omega_1 \omega_2 \tag{5}$$

ou de la forme

$$\frac{\omega}{2} = \omega_1 \omega_2 , \tag{5 bis}$$

selon que ω est impair ou pair, et où ω_1 et ω_2 sont premiers entre eux, de sorte que l'on aura simultanément

$$u + bv \equiv 0 \pmod{\omega_1}, \quad u - bv \equiv 0 \pmod{\omega_2}. \tag{6}$$

En effet, ces deux congruences sont évidentes, pourvu que ω soit un nombre impair; soit, au contraire, ω un nombre pair, un des premiers membres des congruences (6) est un nombre de la forme $4k+2$, parce que leur somme $2u$ est précisément de cette forme.

Ces remarques faites, il est facile de démontrer le lemme fondamental:

I. A chaque couple de suites coordonnées, formées des solutions de l'équation (1), correspond une décomposition de la forme (5) ou (5 bis), où ω_1 et ω_2 sont premiers entre eux.

En premier lieu, il est évident qu'une solution quelconque de l'équation (1), exige une décomposition de la forme susdite, de sorte que les congruences (6) soient remplies.

Soient, en second lieu, (u_1, v_1) et (u_2, v_2) deux solutions de l'équation (1) qui correspondent à la même décomposition (5) ou (5 bis), il existe des exposants m et n, tels que

$$\begin{cases} u_1 + (-1)^m b v_1 \equiv 0 \pmod{\omega_1}, \\ u_1 - (-1)^m b v_1 \equiv 0 \pmod{\omega_2}. \end{cases} \tag{7}$$

$$\text{(7 bis)} \quad \begin{cases} u_2 + (-1)^n b v_2 \equiv 0 \pmod{\omega_1}, \\ u_2 - (-1)^n b v_2 \equiv 0 \pmod{\omega_2}, \end{cases}$$

Multiplions ensuite les deux premières, respectivement les deux dernières, des congruences (7) et (7 bis), nous aurons, en posant

$$m + n = p,$$

puis tenant compte de la congruence (2), les deux autres congruences

$$u_1 u_2 + (-1)^p a v_1 v_2 \pm b (u_2 v_1 + (-1)^p u_1 v_2) \equiv 0 \pmod{\omega},$$

ce qui donnera

$$\begin{aligned} u_1 u_2 + (-1)^p a v_1 v_2 &\equiv 0 \pmod{\omega} \\ u_2 v_1 + (-1)^p u_1 v_2 &\equiv 0 \pmod{\omega}, \end{aligned}$$

car ω et b sont premiers entre eux. Et ces deux dernières congruences ne sont possibles à moins que les deux solutions (u_1, v_1) et (u_2, v_2) n'appartiennent au même couple de suites coordonnées.

Nous remarquons expressément qu'il existe généralement des décompositions de la forme (5) ou (5 bis), auxquelles ne correspond aucune solution de l'équation (1), ce qui a toujours lieu, pourvu que cette équation ne soit pas du genre maximum.

Supposons ensuite que le paramètre ω de l'équation (1) contienne r facteurs premiers inégaux, il existe précisément 2^r décompositions de la forme (5) ou (5 bis), pourvu que ω ne soit pas de la forme $4k+2$; dans ce cas, le nombre des décompositions susdites se réduit à 2^{r-1}.

Cela posé, nous avons de nouveau démontré le théorème, essentiel dans la théorie des équations de LAGRANGE:

II. Supposons que le paramètre ω contienne r facteurs premiers inégaux, le genre de l'équation

(1) est au plus égal à 2^{r-1} ou à 2^r, selon que ω est de la forme $4k+2$ ou non.

Étudions maintenant la multiplication des deux équations de LAGRANGE

$$(8) \qquad u^2 - a v^2 = (-1)^{\delta_1}\omega_1, \quad u^2 - a v^2 = (-1)^{\delta_2}\omega_2,$$

dont les paramètres ω_1 et ω_2 ont ou le plus grand commun diviseur impair ϱ ou le plus grand commun diviseur pair 2ϱ, puis posons

$$(9) \qquad \omega_1 = \varrho\sigma, \quad \omega_2 = \varrho\tau$$

respectivement

$$(9\text{ bis}) \qquad \omega_1 = 2\varrho\sigma, \quad \omega_2 = 2\varrho\tau,$$

les nombres σ et τ sont toujours premiers entre eux.

Posons ensuite

$$(10) \qquad \varrho = \varrho_1\varrho_2\varrho'_1\varrho'_2,$$

où les quatre facteurs qui figurent au second membre sont deux à deux premiers entre eux, puis choisissons ces quatre facteurs, de sorte qu'il existe une solution (u_1, v_1) et (u_2, v_2) de chacune des équations (8) qui satisfont, en vertu de (2) et (6), aux congruences

$$(11) \qquad u_1 + b v_1 \equiv 0 \pmod{\varrho_1\varrho_2}, \quad u_1 - b v_1 \equiv 0 \pmod{\varrho'_1\varrho'_2}$$
$$(11\text{ bis}) \qquad u_2 + b v_2 \equiv 0 \pmod{\varrho_1\varrho'_1}, \quad u_2 - b v_2 \equiv 0 \pmod{\varrho_2\varrho'_2}.$$

nous aurons, par le même procédé que dans le cas précédent,

$$(12) \qquad u_1 u_2 + a v_1 v_2 \equiv u_1 v_2 + u_2 v_1 \equiv 0 \pmod{\varrho'_1\varrho_2}$$
$$(12\text{ bis}) \qquad u_1 u_2 - a v_1 v_2 \equiv u_1 v_2 - u_2 v_1 \equiv 0 \pmod{\varrho_1\varrho'_2}.$$

Cela posé, je dis que les deux nombres entiers

$$(13) \qquad \alpha = \frac{u u_1 + a v_1 v_2}{\varrho'_1\varrho_2}, \quad \beta = \frac{u_1 v_2 + u_2 v_1}{\varrho'_1\varrho_2}$$

ne peuvent jamais avoir d'autres facteurs communs que les nombres 1 et 2, et que c'est la même chose pour ces deux autres nombres entiers

$$(13\text{ bis}) \quad \varkappa = \frac{u_1 u_2 - a v_1 v_2}{\varrho_1 \varrho_2'}, \quad \lambda = \frac{u_1 v_2 - u_2 v_1}{\varrho_1 \varrho_2'}.$$

Quant à la démonstration de ce postulat, nous pouvons évidemment nous borner à l'étude des nombres α et β.

Soit donc k le plus grand commun diviseur de α et β, de sorte que

$$\begin{aligned} u_1 u_2 + a v_1 v_2 &\equiv 0 \pmod{k \varrho_1' \varrho_2} \\ u_1 v_2 + u_2 v_1 &\equiv 0 \pmod{k \varrho_1' \varrho_2}, \end{aligned}$$

nous aurons

$$\begin{aligned} (u_1^2 - a v_1^2) u_2 v_2 &\equiv 0 \pmod{k \varrho_1' \varrho_2} \\ (u_2^2 - a v_2^2) u_1 v_1 &\equiv 0 \pmod{k \varrho_1' \varrho_2}, \end{aligned}$$

ce qui donnera

$$2 \varrho_1 \varrho_2' \sigma \equiv 2 \varrho_1 \varrho_2' \tau \pmod{k};$$

c'est-à-dire que nous aurons nécessairement

$$2 \varrho_1 \varrho_2' \equiv 0 \pmod{k},$$

car σ et τ sont premiers entre eux. Et cette dernière congruence entraîne, en vertu de (13 bis), ces deux autres

$$u_1 u_2 - a v_1 v_2 \equiv u_1 v_2 - u_2 v_1 \equiv 0 \pmod{k},$$

ce qui donnera finalement

$$2 u_1 u_2 \equiv 2 a v_1 v_2 \equiv 2 u_1 v_2 \equiv 2 u_2 v_1 \equiv 0 \pmod{k},$$

congruences qui ne sont possibles que pour

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

et il est évident que les hypothèses (9 bis) donnent toujours

$$k = 2.$$

Dans ce cas, les deux nombres entiers

$$(14) \qquad \alpha_1 = \frac{u_1 u_2 + a v_1 v_2}{2\varrho'_1 \varrho_2}, \quad \beta_1 = \frac{u_1 v_2 + u_2 v_1}{2\varrho'_1 \varrho_2}$$

sont premiers entre eux, et c'est la même chose pour

$$(14\text{ bis}) \qquad \varkappa_1 = \frac{u_1 u_2 - a v_1 v_2}{2\varrho_1 \varrho'_2}, \quad \lambda_1 = \frac{u_1 v_2 - u_2 v_1}{2\varrho_1 \varrho'_2}.$$

Cela posé, nous avons démontré la proposition:

III. Choisissons, comme nous venons de l'indiquer, les quatre facteurs ϱ_1, ϱ'_1, ϱ_2, ϱ'_2, la multiplication des deux équations (8) conduira à ces deux autres équations résolubles

$$(15) \qquad u^2 - a v^2 = (-1)^{\delta_1+\delta_2}(\varrho_1 \varrho'_2)^2 \sigma\tau$$

$$(16) \qquad u^2 - a v^2 = (-1)^{\delta_1+\delta_2}(\varrho'_1 \varrho_2)^2 \sigma\tau.$$

En effet, on voit que ces équations admettent ou la solution (α, β) respectivement $(\varkappa, \lambda)$ ou la solution (α_1, β_1) respectivement $(\varkappa_1, \lambda_1)$, selon que les deux paramètres ω_1 et ω_2 ont leur plus grand commun diviseur impair ou pair.

Quant aux solutions des équations (15) et (16), supposons que les solutions (u_1, v_1) et (u_2, v_2) correspondent respectivement aux décompositions

$$\sigma = \sigma_1 \cdot \sigma_2, \quad \tau = \tau_1 \cdot \tau_2,$$

je dis que les solutions susdites correspondent aux décompositions

$$\varrho_1^2 \sigma_1 \tau_1 \cdot \varrho_1'^2 \sigma_2 \tau_2, \quad \varrho_2^2 \sigma_1 \tau_2 \cdot \varrho_2'^2 \sigma_2 \tau_1.$$

En effet, les congruences (11) et (11 bis) deviennent ici

$$(17) \qquad \begin{cases} u_1 + b v_1 \equiv 0 \pmod{\varrho_1 \varrho_2 \sigma_1} \\ u_1 - b v_1 \equiv 0 \pmod{\varrho'_1 \varrho'_2 \sigma_2} \end{cases}$$

respectivement

$$(17\text{ bis})\quad \begin{cases} u_2 + bv_2 \equiv 0 \pmod{\varrho_1 \varrho_1' \tau_1} \\ u_2 - bv_2 \equiv 0 \pmod{\varrho_2 \varrho_2' \tau_2}, \end{cases}$$

et nous aurons immédiatement le résultat susdit, en multipliant les congruences (17) et (17 bis).

Forelagt paa Mødet den 9. Februar 1923.
Færdig fra Trykkeriet den 8. September 1923.