JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

CAMILLE JORDAN

Sur la forme canonique des congruences du second degré et le nombre de leurs solutions

Journal de mathématiques pures et appliquées 2^e série, tome 17 (1872), p. 368-402.
<http://www.numdam.org/item?id=JMPA_1872_2_17__368_0>

Sur la forme canonique des congruences du second degré et le nombre de leurs solutions;

PAR M. CAMILLE JORDAN.

Nous nous proposons de donner ici la solution de la question suivante, dont nous avons examiné ailleurs quelques cas particuliers (*Comptes rendus*, 19 mars 1866; *Traité des Substitutions*, nos 197-200 et 259-260) :

Déterminer le nombre des solutions de la congruence du second degré à m inconnues

$$(1) \qquad a_1 x_1^2 + \ldots + a_m x_m^2 + b_{12} x_1 x_2 + \ldots \equiv c \pmod{M}.$$

1. La question se ramène immédiatement au cas où le module M est une puissance d'un nombre premier.

Soit, en effet, $M = P^\lambda P_1^{\lambda_1}, \ldots$, P, P_1 étant des facteurs premiers différents. Soient $x_1, \ldots, x_m$ un système de solutions de la congruence (1); $\xi_1, \ldots, \xi_m$ les restes de la division de $x_1, \ldots, x_m$ par P^λ; $\eta_1, \ldots, \eta_m$ les restes de leur division par $P_1^{\lambda_1}, \ldots$; on aura évidemment

$$(2) \qquad a_1 \xi_1^2 + \ldots + a_m \xi_m^2 + b_{12} \xi_1 \xi_2 + \ldots \equiv c \pmod{P^\lambda},$$

$$(3) \qquad a_1 \eta_1^2 + \ldots + a_m \eta_m^2 + b_{12} \eta_1 \eta_2 + \ldots \equiv c \pmod{P_1^{\lambda_1}},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Réciproquement, soient $\xi_1, \ldots, \xi_m$ un système quelconque de solutions de la congruence (2); $\eta_1, \ldots, \eta_m$ un système de solutions de la congruence (3), etc. On sait qu'on pourra déterminer d'une seule ma-

nière un système d'entiers $x_1, \ldots, x_m$ inférieurs à M et satisfaisant aux conditions

$$x_\rho \equiv \xi_\rho \pmod{P^\lambda} \equiv \eta_\rho \pmod{P_1^{\lambda_1}} \equiv \ldots,$$

et ces entiers satisferont évidemment à la congruence (1); d'où cette première conclusion :

Le nombre des solutions de la congruence (1) *est égal au produit des nombres de solutions des congruences* (2), (3), *etc.*

Nous supposerons donc à l'avenir que M se réduise à P^λ, P étant premier. Deux cas seront à distinguer, suivant que P sera impair ou égal à 2.

PREMIER CAS : P PREMIER IMPAIR.

2. Soit P^α la plus haute puissance de P qui divise à la fois tous les coefficients du premier membre de la congruence considérée. En la mettant en évidence, la congruence prendra la forme

$$(4)\quad f(x_1, \ldots, x_m) = P^\alpha [a_1 x_1^2 + \ldots + a_m x_m^2 + b_{12} x_1 x_2 + \ldots] \equiv c \pmod{P^\lambda},$$

et l'un au moins des coefficients $a_1, \ldots, a_m, b_{12}, \ldots$ sera premier à P. Il est permis de supposer que l'un des coefficients $a_1, \ldots, a_m$ des carrés des variables est premier à P. En effet, si l'on avait

$$a_1 \equiv \ldots \equiv a_m \equiv 0 \pmod{P},$$

mais $b_{12} \not\equiv 0 \pmod{P}$, par exemple, on pourrait poser $x_2 \equiv x'_2 + x_1$, et l'on aurait, pour déterminer les nouvelles variables $x_1, x'_2, x_3, \ldots$, une congruence analogue à (4), mais où le coefficient du terme en x_1^2 serait $a_1 + b_{12} + a_2$, nombre premier à P.

Soit donc $a_1 \not\equiv 0 \pmod{P}$. On pourra déterminer des entiers $k_2, \ldots, k_m$ satisfaisant aux congruences

$$2 a_1 k_\rho \equiv b_{1\rho} \pmod{P^\lambda} \quad (\rho = 2, 3, \ldots, m),$$

et prenant pour nouvelle inconnue la quantité

$$X_1 \equiv x_1 + k_2 x_2 + \ldots + k_m x_m,$$

la congruence prendra la forme

$$P^{\alpha} a_1 X_1^2 + P^{\alpha} f_1(x_2,\ldots,x_m) \equiv c \pmod{P^{\lambda}}.$$

Si la fonction $f_1(x_2,\ldots,x_m)$ n'est pas identiquement congrue à zéro, on pourra opérer sur elle comme sur f, de manière à faire disparaître les rectangles d'une seconde variable.

Poursuivant ainsi, on voit qu'on pourra faire disparaître les rectangles de toutes les variables. Mettant alors en évidence les puissances de P qui peuvent diviser chaque coefficient, on pourra mettre la congruence sous la forme

$$(5)\quad \begin{cases} \Phi = P^{\alpha}(A_1 X_1^2 + \ldots + A_p X_p^2) + P^{\beta}(B_1 Y_1^2 + \ldots + B_q Y_q^2) + \ldots \\ \qquad\qquad \equiv c \pmod{P^{\lambda}}. \end{cases}$$

3. Le nombre n des variables qui figurent explicitement dans cette congruence peut être inférieur à m. Dans ce cas, chacune des $m-n$ variables restantes prenant les valeurs de zéro à $P^{\lambda}-1$, cette variation n'influera pas sur la valeur de la fonction Φ. Donc le nombre des solutions cherchées sera égal à $P^{\lambda(m-n)} Q$, Q étant le nombre des solutions de la congruence (5), où l'on ne considère plus d'autres variables que celles qui y figurent explicitement.

On peut supposer que les exposants α, β,... soient rangés par ordre de grandeur croissante. Mais alors la congruence (5), à n variables, ne peut avoir de solution que si c est divisible par P^{α}. Soit $c = P^{\alpha} d$ et $\lambda - \alpha = \mu$. On pourra poser

$$(6)\qquad X_1 \equiv x_1 + P^{\mu} x'_1,\ldots,\quad Y_1 \equiv y_1 + P^{\mu} y'_1,\ldots,$$

$x_1,\ldots, y_1,\ldots$ étant des entiers moindres que P^{μ}, et $x'_1,\ldots, y'_1,\ldots$ des entiers moindres que P^{α}.

Chaque système de solutions de la congruence (5) donnera évidemment un système de solutions de la congruence

$$(7)\quad A_1 x_1^2 + \ldots + A_p x_p^2 + P^{\beta-\alpha}(B_1 y_1^2 + \ldots + B_q y_q^2) + \ldots \equiv d \pmod{P^{\mu}},$$

et réciproquement, à chaque système de solutions de cette congruence correspondront $P^{\alpha n}$ systèmes de solutions de la congruence (5), qui

s'obtiendront par les relations (6) en y donnant à $x'_1,\ldots, y'_1,\ldots$ tous les systèmes de valeurs possibles moindres que P^α. On aura donc

$$Q = P^{\alpha n} R,$$

R étant le nombre des solutions de la congruence (7).

4. Examinons donc cette dernière congruence. Ses solutions pourront être partagées en deux classes : 1° celles où l'un au moins des entiers $x_1,\ldots, x_p$ est premier à P ; 2° celles où $x_1 \equiv \ldots \equiv x_p \equiv 0 \pmod{P}$. Soient respectivement S_μ, T_μ les nombres de systèmes de solutions de chaque classe. On aura

$$R = S_\mu + T_\mu.$$

Solutions de la première classe. — Soit $x_1,\ldots, x_p, y_1,\ldots, y_q,\ldots$ un système de solutions de la première classe; et soient

$$(8)\qquad \begin{cases} x_\rho = x'_\rho + P^{\mu-1}\xi_\rho, & (\rho = 1, 2, \ldots, p); \\ y_\sigma = y'_\sigma + P^{\mu-1}\eta_\sigma, & (\sigma = 1, 2, \ldots, q); \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \end{cases}$$

$x'_\rho, y'_\sigma,\ldots$ étant $< P^{\mu-1}$, et $\xi_\rho, \eta_\sigma,\ldots < P$; on aura évidemment

$$(9)\quad A_1 x'^2_1 + \ldots + A_p x'^2_1 + P^\beta (B_1 y'^2_1 + \ldots + B_q y'^2_1) + \ldots \equiv d \pmod{P^{\mu-1}}.$$

D'ailleurs $x'_1,\ldots, x'_p$ ne sont pas tous nuls par hypothèse. Donc $x'_1,\ldots, x'_p, y'_1,\ldots, y'_q,\ldots$ est l'un des $S_{\mu-1}$ systèmes de solutions de première classe de la congruence (9).

Réciproquement, soit $x'_1,\ldots, x'_p, y'_1,\ldots, y'_q,\ldots$ l'un quelconque de ces $S_{\mu-1}$ systèmes de solutions; on aura une relation de la forme

$$A_1 x'^2_1 + \ldots + A_p x'^2_1 + P^\beta (B_1 y'^2_1 + \ldots + B_q y'^2_1) + \ldots \equiv d + e P^{\mu-1} \pmod{P^\mu},$$

et $x_1,\ldots, x_p, y_1,\ldots, y_q,\ldots$ satisferont à la congruence (7), si l'on détermine les entiers $\xi_1,\ldots, \xi_p, \eta_1,\ldots, \eta_q,\ldots$, de telle sorte que l'on ait

$$(10)\qquad 2A_1 x'_1 \xi_1 + \ldots + 2A_p x'_p \xi_p \equiv e \pmod{P}.$$

Or, par hypothèse, l'un au moins des entiers $x'_1, \ldots, x'_p$, par exemple x'_1, est premier à P. La congruence (10) détermine ξ_1, après qu'on aura choisi arbitrairement les $n-1$ autres quantités $\xi_2, \ldots, \xi_p, \eta_1, \ldots, \eta_q, \ldots$, ce qui pourra se faire de P^{n-1} manières différentes.

On aura donc

$$S_\mu = P^{n-1} S_{\mu-1} = P^{2(n-1)} S_{\mu-2} = \ldots = P^{(\mu-1)(n-1)} S_1.$$

Il reste à déterminer S_1, c'est-à-dire le nombre des solutions de première classe de la congruence

$$(11) \quad A_1 x_1^2 + \ldots + A_p x_p^2 + P^{\beta-\alpha}(B_1 y_1^2 + \ldots + B_q y_q^2) + \ldots \equiv d \pmod{P}.$$

Or on peut donner à chacune des $n-p$ variables $y_1, \ldots, y_q, \ldots$ une valeur quelconque sans altérer la valeur (mod. P) du premier membre de cette congruence; on aura donc

$$S_1 = P^{n-p} U,$$

U étant le nombre des solutions de première classe de la congruence

$$(12) \qquad A_1 x_1^2 + \ldots + A_p x_p^2 \equiv d \pmod{P}.$$

Or nous avons déterminé (*Comptes rendus*, 19 mars 1866, ou *Traité de Substitutions*, nos 197-200) le nombre total des solutions de la congruence (12). Ce nombre sera égal à U si $d \gtrless 0 \pmod{P}$; à $U+1$ dans le cas où $d \equiv 0 \pmod{P}$; car dans ce cas on a une solution de seconde classe $x_1 = \ldots = x_p = 0$.

Posant, pour abréger, suivant la notation de Legendre,

$$\left[\frac{(-1)^l A_1 \ldots A_{2l}}{P}\right] = \nu, \quad \left[\frac{(-1)^l A_1 \ldots A_{2l+1} d}{P}\right] = \nu',$$

on aura, d'après les formules de l'endroit cité :

1° Si $p = 2l$ et $d \gtrless 0 \pmod{P}$,

$$U = P^{2l-1} - P^{l-1}\nu;$$

2° Si $p = 2l+1$ et $d \gtrless 0 \pmod{P}$,

$$U = P^{2l} + P^l \nu';$$

3° Si $p = 2l$ et $d \equiv 0 \pmod{P}$,

$$U + 1 = P^{2l-1} + (P^l - P^{l-1})\nu ;$$

4° Si $p = 2l + 1$ et $d \equiv 0 \pmod{P}$,

$$U + 1 = P^{2l}.$$

5. *Solutions de la seconde classe.* — Posons $x_\rho = Px'_\rho$. On aura à déterminer le nombre T_μ de solutions de la congruence

$$(13)\quad P^2(A_1 x_1'^2 + \ldots + A_p x_p'^2) + P^{\beta-\alpha}(B_1 y_1^2 + \ldots + B_q y_q^2) + \ldots \equiv d \pmod{P^\mu},$$

où $y_1, \ldots y_q$ varient de 0 à $P^\mu - 1$, et $x'_1, \ldots, x'_p$ de 0 à $P^{\mu-1} - 1$ seulement. Si l'on faisait varier les p quantités $x'_1, \ldots, x'_p$, non plus de 0 à $P^{\mu-1} - 1$, mais de 0 à $P^\mu - 1$, il est clair que le nombre des solutions de la congruence (13) deviendrait P^p fois plus considérable; on aura donc

$$T_\mu = P^{-p} V,$$

V étant le nombre des solutions de la congruence (13), où toutes les variables varient de 0 à $P^\mu - 1$.

Soit δ le plus petit des exposants $2, \beta - \alpha, \ldots$. La congruence (13) n'aura de solutions que si d est divisible par P^δ. Soit d'ailleurs $d = P^\delta d_1$. On aura, comme on l'a vu plus haut,

$$V = P^{\delta n} W,$$

W étant le nombre de solutions de la congruence

$$(14)\quad \left\{ \begin{array}{l} P^{2-\delta}(A_1 x_1'^2 + \ldots + A_p x_p'^2) + P^{\beta-\alpha-\delta}(B_1 y_1^2 + \ldots + B_q y_q^2) + \ldots \\ \qquad\qquad \equiv d_1 \pmod{P^{\mu-\delta}}. \end{array} \right.$$

Cette congruence contient dans son premier membre un groupe de variables dont les coefficients sont premiers à P. Elle est donc analogue à la congruence (7), et ses solutions pourront être partagées en deux classes; le nombre des solutions de première classe s'obtenant directement; les solutions de seconde classe se ramenant à celles d'une

nouvelle congruence par rapport à un module $P^{\mu-\delta-\varepsilon}$ moindre que $P^{\mu-\delta}$. On poursuivra cette réduction jusqu'à ce qu'on arrive à une congruence ayant pour module P ou l'unité, auquel cas le nombre des solutions s'obtiendra immédiatement.

Nous laisserons au lecteur le soin d'écrire la formule définitive qui résulte de cette méthode.

6. L'analyse qui précède repose essentiellement, comme on a pu le voir, sur la propriété des congruences du second degré mod. P^λ (P premier impair) de pouvoir se réduire par un changement de variables à la forme canonique (5). Mais les diverses expressions que donne cette formule en y faisant varier α, β,... p, q,... A_1,..., A_p, B_1,..., B_q,... sont elles-mêmes réductibles à un moindre nombre. On peut, en effet, faire en sorte que les coefficients dans chacune des suites A_1,..., A_p, B_1,..., B_q,... se réduisent tous à l'unité, sauf l'un d'eux, qui pourra, suivant le cas, se réduire à l'unité ou à un nombre N choisi arbitrairement parmi les non-résidus quadratiques de P.

Pour le démontrer, considérons l'expression

$$A_1X_1^2+\ldots+A_pX_p^2. \tag{15}$$

Supposons que, parmi les coefficients A_1,..., A_p, il y en ait ρ qui soient non-résidus de P; si ce nombre ρ est >1, on pourra l'abaisser de deux unités par un changement de variables.

Soient en effet A_1 et A_2 non-résidus; et soient R un résidu quelconque; a, c un système de solutions de la congruence

$$A_1a^2+A_2c^2\equiv R \pmod{P}, \tag{16}$$

on aura $a\gtrless 0$, $c\gtrless 0$ (mod. P), car si a était congru à zéro, on aurait $A_2c^2\equiv R$, ce qui est absurde, A_2 étant non-résidu.

Posons maintenant

$$X_1\equiv ax_1+bx_2,\quad X_2\equiv cx_1+dx_2, \tag{17}$$

l'expression (15) deviendra

$$\begin{cases}(A_1a^2+A_2c^2)x_1^2+2(A_1ab+A_2cd)x_1x_2\\ \qquad\qquad +(A_1b^2+A_2d^2)x_2^2+\ldots+A_pX_p^2.\end{cases} \tag{18}$$

On peut, sans annuler le déterminant de la substitution (17), poser

$$A_1 ab + A_2 cd \equiv 0 \pmod{P}. \tag{19}$$

En effet, ce déterminant sera égal à

$$ad - bc \equiv ad + \frac{A_2 c^2 d}{A_1 a} \equiv \frac{(A_1 a^2 + A_2 c^2) d}{A_1 a} \equiv \frac{R d}{A_1 a} \gtrless 0 \pmod{p}.$$

Supposons donc la condition (19) remplie. L'expression (18) transformée de l'expression (15) sera, comme cette dernière, une somme de carrés; mais les coefficients des deux nouvelles variables x_1, x_2 seront devenus des résidus. En effet, le coefficient de x_1 est égal à R, et celui de x_2 à

$$A_1 b^2 + A_2 d^2 \equiv A_1 \frac{A_2^2 c^2 d^2}{A_1^2 a^2} + A_2 d^2 \equiv \frac{A_1 A_2 R d^2}{A_1^2 a^2},$$

qui est évidemment un résidu.

On pourra donc préparer l'expression

$$A_1 X^2 + A_2 X_2^2 + \ldots + A_p X_p^2$$

de telle sorte que tous ses coefficients soient des résidus, sauf l'un d'entre eux A_1, pour lequel il y aura indécision. Cela posé, on saura déterminer des entiers $k_2, \ldots, k_p$ satisfaisant aux relations

$$A_2 k_2^2 \equiv 1, \ldots, \quad A_p k_p^2 \equiv 1.$$

On pourra de même satisfaire à la relation

$$A_1 k_1^2 \equiv \theta,$$

θ étant égal à 1 ou à N, suivant que A_1 est résidu ou non.

Posant maintenant

$$X_1 = k_1 x_1, \ldots, \quad X_p = k_p x_p,$$

l'expression considérée prend la forme

$$\theta x_1^2 + x_2^2 + \ldots + x_p^2,$$

ce qu'il fallait démontrer.

SECOND CAS : $P = 2$.

7. Soit 2^α la plus haute puissance de 2 qui divise tous les coefficients de la congruence considérée. Mettant ce facteur commun en évidence, la congruence prendra la forme

$$f(x_1,\ldots,x_m) = 2^\alpha[a_1x_1^2+\ldots+a_mx_m+b_{12}x_1x_2+\ldots] = c \pmod{2^\lambda}.$$

On peut supposer que les coefficients $a_1,\ldots,a_m$ des carrés des variables sont tous pairs, sauf deux d'entre eux tout au plus.

Supposons, en effet, qu'on ait a_1, a_2, a_3 impairs. Si l'un des coefficients b_{12}, b_{13}, b_{23}, par exemple b_{13}, est pair, on pourra poser

$$x_1 = x'_1 + x_3,$$

et obtenir ainsi entre les variables $x'_1, x_2,\ldots, x_m$ une nouvelle congruence équivalente à la proposée, mais où le coefficient de x_3^2 sera le nombre pair $a_1 + b_{13} + a_3$.

Si b_{12}, b_{13}, b_{23} sont impairs, on posera

$$x_1 \equiv x'_1 + x_3, \quad x_2 \equiv x'_2 + x_3,$$

et, après cette substitution, le coefficient de x_3^2 sera le nombre pair

$$a_1 + a_2 + a_3 + b_{12} + b_{13} + b_{23}.$$

On pourra distinguer ici trois cas :

8. *Premier cas.* — Tous les a sont pairs. L'un des coefficients b, par exemple b_{12} sera impair. Soit 2^ρ la plus haute puissance de 2 qui divise a_1. Remplaçons x_2 par une nouvelle variable y_2, définie par la relation

(20) $$x_2 = y_2 + 2^\rho x_1.$$

La congruence prendra la forme

$$2^{\alpha}[a'_1 x_1^2 + b'_{12} x_1 y_2 + a_2 y_2^2 + \ldots] \equiv c \pmod{2^{\lambda}},$$

en posant

$$a'_1 = a_1 + 2^{\rho} b_{12} + 2^{2\rho} a_2,$$
$$b'_{12} = b_{12} + 2^{\rho+1} a_2.$$

On voit immédiatement que b'_{12} sera impair et que a'_1 sera divisible au moins par $2^{\rho+1}$. Par une suite de transformations analogues, on augmentera progressivement le degré de la puissance de 2 qui divise le coefficient de la première variable, jusqu'à ce que ce coefficient, étant divisible par 2^{λ}, devienne congru à zéro (mod. 2^{λ}) et puisse être supprimé. On pourra ensuite, par un procédé analogue, faire disparaître le carré de la seconde variable.

Il nous est donc permis de supposer $a_1 \equiv a_2 \equiv 0 \pmod{2^{\lambda}}$, avec $b_{12} \equiv 1 \pmod{2}$; mais alors on pourra déterminer des entiers $k_3, \ldots, k_m$ satisfaisant aux relations

$$b_{1\rho} \equiv k_{\rho} b_{12} \pmod{2^{\lambda}}.$$

Prenant alors pour variables indépendantes, au lieu de x_1, x_2, celles-ci

$$x \equiv b_{12} x_1 + b_{23} x_3 + \ldots + b_{2m} x_m,$$
$$y \equiv \quad x_2 + k_3 x_3 + \ldots + k_m x_m,$$

la congruence proposée deviendra

$$2^{\alpha} xy + 2^{\alpha} f_1(x_3, \ldots, x_m) \equiv c \pmod{2^{\lambda}},$$

et l'on aura ainsi un groupe de deux variables séparées des autres, et ne figurant plus que par leur rectangle.

9. *Deuxième cas.* — Tous les a sont pairs, sauf a_1. Chacun des coefficients $b_{12}, \ldots, b_{1m}$ sera pair. En effet, si b_{13} par exemple était impair, on n'aurait qu'à poser $x_3 = x'_3 + x_1$ pour rendre pair le coefficient de x_1^2 et retomber sur le premier cas. Cela posé, on pourra dé-

terminer des entiers $k_2,\ldots, k_m$ par les relations

$$2a_1k_\rho \equiv b_{1\rho};$$

et prenant pour variable $z = x_1 + k_2x_2 + \ldots$, la congruence prendra la forme

$$2^\alpha a_1 z^2 + 2^\alpha f_1(x_2,\ldots, x_m) \equiv c \pmod{2^\lambda},$$

où la variable z est séparée.

Troisième cas. — a_1 et a_2 impairs. Chacune des quantités $b_{13},\ldots, b_{1m}, b_{23},\ldots, b_{2m}$ est paire; car si b_{13} était impair, on pourrait rendre pair le coefficient de x_1^2 et retomber ainsi sur le deuxième cas. Au contraire, b_{12} sera impair; car, s'il était pair, il suffirait de poser $x_2 = x'_2 + x_1$ pour rendre pair le coefficient de x_1^2.

Cela posé, soient k_ρ, l_ρ des entiers déterminés par les relations

$$(21)\qquad \begin{cases} 2a_1k_\rho + b_{12}l_\rho \equiv b_{1\rho}, \\ b_{12}k_\rho + 2a_2l_\rho \equiv b_{2\rho}, \end{cases}$$

(dont le déterminant est impair). Prenons pour variables, au lieu de x_1 et x_2, les suivantes

$$u \equiv x_1 + k_3x_3 + ,\ldots, \quad v \equiv x_2 + l_3x_3 + \ldots.$$

La congruence deviendra

$$2^\alpha(a_1u^2 + b_{12}uv + a_2v^2) + 2^\alpha f_1(x_3,\ldots, x_m) \equiv c \pmod{2^\lambda}.$$

10. Nous obtenons ainsi dans chaque cas un mode de réduction de la fonction f à une forme plus simple; opérant de même sur la fonction f_1 à $n-1$ ou $n-2$ variables, on arrivera évidemment à mettre la congruence sous la forme

$$(22)\qquad 2^\alpha\Sigma_\alpha + 2^\beta\Sigma_\beta + \ldots \equiv c \pmod{2^\lambda},$$

l'une quelconque des suites $\Sigma_\alpha,\ldots$ pouvant être composée de trois parties :

1° Une somme de rectangles

$$x_1 y_1 + \ldots + x_p y_p;$$

2° Une somme de carrés, multipliés par des coefficients impairs,

$$A_1 z_1^2 + \ldots + A_q z_q^2;$$

3° Des groupes de trois termes à coefficients impairs, tels que

$$B_1 u_1^2 + C_1 u_1 v_1 + D_1 v_1^2, \ldots, \quad B_r u_r^2 + C_r u_r v_r + D_r v_r^2.$$

D'ailleurs la suite considérée pourra ne pas contenir à la fois ces trois sortes de termes; auquel cas un, ou même deux des nombres p, q, r, se réduirait à zéro. Mais si tous trois s'annulaient à la fois, la suite ne contiendrait plus aucun terme et s'évanouirait.

Si nous convenons de poser $\Sigma_\rho = 0$ toutes les fois que ρ n'est pas l'un des nombres α, β,..., il est clair que la congruence (22) pourra s'écrire

$$\sum_{\rho=0}^{\rho=\lambda-1} 2^\rho \Sigma_\rho \equiv c \pmod{2^\lambda}, \tag{23}$$

expression qui pourra être considérée comme la forme canonique des congruences du second degré (mod. 2^λ).

En faisant varier la répartition des indices entre les diverses suites Σ_1,... et entre les trois parties de chacune de ces suites, ainsi que les coefficients A_1,..., A_q, B_1, C_1, D_1,... qui les multiplient, on obtiendra beaucoup de formes diverses; mais plusieurs d'entre elles pourront se ramener les unes aux autres par un changement d'indices. Pour éliminer les formes réduites qui font ainsi double emploi, il sera nécessaire d'assujettir celles que l'on conserve à certaines conditions que nous allons indiquer.

11. 1° Aucune des suites Σ_ρ ne doit contenir à la fois des termes de deuxième espèce, $Az^2 + \ldots$, et des termes de troisième espèce, $Bu^2 + Cuv + Dv^2 + \ldots$.

Nous allons montrer, en effet, que les formes réduites où cette cir-

constance se présenterait se ramènent à d'autres qui ne contiennent plus de termes de troisième espèce.

Posons, en effet,

$$z \equiv z' + \delta u' + \varepsilon v', \quad u \equiv 2z' + u', \quad v \equiv 2z' + v',$$

substitution permise, car son déterminant $\equiv 1 \pmod 2$; l'expression

$$Az^2 + Bu^2 + Cuv + Du^2$$

sera transformée en

$$(A + 4B + 4C + 4D)z'^2 + (A\delta^2 + B)u'^2 + (A\varepsilon^2 + D)v'^2$$
$$(2A\delta + 4B + 2C)z'u' + (2A\varepsilon + 2C + 4D)z'v' + (2A\delta\varepsilon + C)u'v'.$$

Posons maintenant

$$2A\delta + 4B + 2C \equiv 0 \pmod{2^\lambda},$$
$$2A\varepsilon + 2C + 4D \equiv 0.$$

Ces congruences donneront pour δ et ε des valeurs impaires (A, B, C, D étant impairs) qui, substituées dans les coefficients de u'^2, v'^2, $u'v'$, rendront les deux premiers pairs et le dernier impair. En opérant comme au n° **8**, on pourra donc remplacer u', v' par deux nouveaux indices x, y qui ne figurent plus que par leur rectangle dans l'expression de Σ_ρ.

Si Σ_ρ renfermait d'autres groupes de termes de troisième espèce, on les ferait disparaître de la même manière, en leur substituant de simples rectangles.

12. 2° La suite Σ_ρ ne peut contenir plusieurs groupes de termes de troisième espèce.

Soit, en effet,

$$\Sigma_\rho = B_1 u_1^2 + C_1 u_1 v_1 + D_1 v_1^2 + B_2 u_2^2 + C_2 u_2 v_2 + D_2 v_2^2 + \dots.$$

Nous allons montrer que par une transformation convenable on peut remplacer les six termes ci-dessus écrits par une somme de deux rectangles.

Posons

$$u_1 = x + z + u, \quad v_1 = y + z + u,$$
$$u_2 = z + x + y, \quad v_2 = u + x + y,$$

substitution permise, car son déterminant $\equiv 1 \pmod 2$. Il viendra

$$\Sigma_\rho = \mathfrak{A} x^2 + \mathfrak{A}_1 y^2 + \mathfrak{A}_2 z^2 + \mathfrak{A}_3 u^2 + \mathfrak{B} xy + \mathfrak{C} xz + \mathfrak{C}_1 xu + \mathfrak{C}_2 yz + \mathfrak{C}_3 yu + \mathfrak{B}_1 zu,$$

en posant

$$\mathfrak{A} = B_1 + B_2 + C_2 + D_2, \quad \mathfrak{A}_1 = D_1 + B_2 + C_2 + D_2, \ldots,$$
$$\mathfrak{B} = C_1 + 2B_2 + 2C_2 + 2D_2, \quad \mathfrak{B}_1 = C_2 + 2B_1 + 2C_1 + 2D_1,$$
$$\mathfrak{C} = 2B_1 + C_1 + 2B_2 + C_2, \quad \mathfrak{C}_1 = 2B_1 + C_1 + 2D_2 + C_2, \ldots.$$

Il résulte de ces expressions que $\mathfrak{A}, \mathfrak{A}_1, \ldots, \mathfrak{C}, \mathfrak{C}_1, \ldots$ sont pairs, et $\mathfrak{B}, \mathfrak{B}_1$ impairs. On pourra donc, en opérant comme au n° 8, remplacer x, y par deux nouveaux indices x', y', choisis de telle sorte que leurs carrés disparaissent de l'expression de Σ_ρ, laquelle se réduira à la forme

$$\Sigma_\rho = \mathfrak{B}' x' y' + \mathfrak{C}' x' z + \mathfrak{C}'_1 x' u + \mathfrak{C}'_2 y' z + \mathfrak{C}'_3 y' u + \mathfrak{A}_2 z^2 + \mathfrak{A}_3 u^2 + \mathfrak{B}_1 zu,$$

$\mathfrak{C}'$, $\mathfrak{C}'_1$, $\mathfrak{C}'_2$, $\mathfrak{C}'_3$ étant des fonctions linéaires entières de $\mathfrak{C}$, $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$ et, par suite, des nombres pairs.

Posant maintenant

$$x_1 \equiv \mathfrak{B}' x' + \mathfrak{C}'_2 z + \mathfrak{C}'_3 u, \quad \mathfrak{C}' \equiv \mathfrak{B}' k,$$
$$y_1 \equiv y' + kz + lu, \quad \mathfrak{C}'_1 \equiv \mathfrak{B}' l,$$

il vient

$$\Sigma_\rho = x_1 y_1 + (\mathfrak{A}_2 - \mathfrak{C}'_2 k) z^2 + (\mathfrak{A}_3 - \mathfrak{C}'_3 l) u^2 + (\mathfrak{B}_1 - \mathfrak{C}'_2 l - \mathfrak{C}'_3 k) zu;$$

les coefficients de z^2, u^2, dans cette expression, étant pairs et celui de zu impair, on pourra, par une dernière transformation (n° 8), faire disparaître les carrés et mettre Σ_ρ sous la forme

$$x_1 y_1 + x_2 y_2.$$

13. 3° Σ_ρ ne peut contenir plus de deux termes de seconde espèce. Soit, en effet,

$$\Sigma_\rho = A_1 z_1^2 + A_2 z_2^2 + A_3 z_3^2 + \dots.$$

Nous allons montrer qu'on peut, par une transformation convenable, réduire le nombre des termes de seconde espèce.

Posons

$$z_1 = x + z, \quad z_2 = y + z, \quad z_3 = z - kx - ly,$$

où k, l sont des entiers impairs, déterminés par les relations

$$A_1 \equiv A_3 k, \quad A_2 \equiv A_3 l$$

(cette substitution est admissible, car son déterminant $1 + k + l$ est impair) : il viendra

$$\Sigma_\rho = A_1 (1 + k) x^2 + 2kl\, xy + A_2 (1 + l) y^2 + (A_1 + A_2 + A_3) z^2;$$

mais, dans cette expression, tous les coefficients sont pairs, sauf celui de z^2. On pourra donc mettre 2 en facteur commun dans les trois premiers termes de cette expression, et reporter ces termes dans la suite $\Sigma_{\rho+1}$, de telle sorte que, des trois carrés mis en évidence dans Σ_ρ, il n'en reste plus qu'un.

On remarquera que, k et l étant impairs, l'expression

$$2\left(A_1 \frac{1+k}{2} x^2 + klxy + A_2 \frac{1+'}{2} y^2\right)$$

pourra se ramener à la forme $2xy$ par un changement de variables si l'un des entiers $\frac{1+k}{2}$, $\frac{1+l}{2}$ est pair; dans le cas contraire, à la forme

$$2(Bu^2 + Cuv + Du^2).$$

14. D'après ce qui précède, on peut admettre que Σ_ρ se réduira à

l'une des quatre formes suivantes :

$$(24) \qquad S_\rho,$$

$$(25) \qquad S_\rho + Az^2,$$

$$(26) \qquad S_\rho + Az^2 + A_1 z_1^2,$$

$$(27) \qquad S_\rho + Bu^2 + Cuv + Dv^2,$$

S_ρ désignant une somme de rectangles, telle que $x_1 y_1 + \ldots + x_p y_p$ (le nombre p de ces rectangles peut d'ailleurs se réduire à zéro), et A, A_1, B, C, D étant des entiers impairs.

On peut d'ailleurs exclure le cas où $\Sigma_{\lambda-1}$ serait de la forme (26).

En effet, si l'on avait

$$\Sigma_{\lambda-1} = S_{\lambda-1} + Az^2 + A_1 z_1^2,$$

on n'aurait qu'à poser

$$z = z' + z_1', \quad z_1 = z_1',$$

pour changer l'expression $2^{\lambda-1}\Sigma_{\lambda-1}$ en

$$2^{\lambda-1}[S_{\lambda-1} + Az'^2 + 2Az'z_1' + (A + A_1)z_1'^2] \equiv 2^{\lambda-1}(S_{\lambda-1} + Az'^2) \pmod{2^\lambda},$$

expression analogue à la précédente, mais qui ne contient plus qu'un seul carré.

Nous allons maintenant passer à un second ordre de conditions, en cherchant quelles limitations on peut imposer aux valeurs des coefficients A, A_1, B, C, D.

15. *Premier cas.* — Admettons d'abord que Σ_ρ soit de la forme (27); on pourra y supposer $B = C = D = 1$. Nous allons montrer, en effet, qu'on peut atteindre ce résultat par un changement de variables.

Posons

$$(28) \qquad \begin{cases} u \equiv \alpha u' + \beta v', \\ v \equiv \gamma u' + \delta v'. \end{cases}$$

Il viendra

$$\Sigma_\rho = S_\rho + A' u'^2 + B' u' v' + C' v'^2,$$

expression qui remplira les conditions voulues si l'on a

$$(29)\qquad \left\{\begin{array}{l} A' = A\alpha^2 + B\alpha\gamma + C\gamma^2 \equiv 1 \\ B' = 2A\alpha\beta + B(\delta\alpha + \beta\gamma) + 2C\gamma\delta \equiv 1 \\ C' = A\beta^2 + B\beta\delta + C\delta^2 \equiv 1 \end{array}\right\} \pmod{2^\lambda},$$

auxquelles il faudra ajouter la suivante :

$$(30)\qquad \alpha\delta - \beta\gamma \gtrless 0 \pmod 2,$$

pour que la substitution (28) soit admissible. Mais cette condition découle des trois autres. En effet, pour qu'elle ne fût pas satisfaite, il faudrait qu'on eût

α et β pairs,	d'où	B′ pair,
α et γ id.		A′ id.
δ et β id.		B′ id.
δ et γ id.		C′ id.
$\alpha, \beta, \gamma, \delta$, impairs,		B′ id.

ce qui serait contraire aux relations (29). Il ne nous reste donc qu'à satisfaire à celles-ci.

Or ces congruences sont satisfaites si $\lambda = 1$ par les valeurs $\alpha = \delta = 1$, $\beta = \gamma = 0$, et nous allons montrer que, si l'on peut y satisfaire pour $\lambda = \mu$, on pourra y satisfaire pour $\lambda = \mu + 1$.

Soit, en effet, α, β, γ, δ un système de solutions pour lequel on ait

$$\left.\begin{array}{l} A' \equiv 1 \\ B' \equiv 1 \\ C' \equiv 1 \end{array}\right\} \pmod{2^\mu}, \qquad \left.\begin{array}{l} \equiv 1 + e2^\mu \\ \equiv 1 + f2^\mu \\ \equiv 1 + g2^\mu \end{array}\right\} \pmod{2^{\mu+1}}.$$

Remplaçons α, β, γ, δ par $\alpha + 2^\mu\alpha'$, $\beta + 2^\mu\beta'$,... ; pour que ces nouvelles valeurs donnent

$$A' \equiv B' \equiv C' \equiv 1 \pmod{2^{\mu+1}},$$

il faudra que l'on ait

$$\left.\begin{aligned} &1 + e\,2^{\mu} + 2^{\mu} B(\alpha\gamma' + \gamma\alpha') &&\equiv 1 \\ &1 + f\,2^{\mu} + 2^{\mu} B(\alpha\delta' + \delta\alpha' + \gamma\beta' + \beta\gamma') &&\equiv 1 \\ &1 + g\,2^{\mu} + 2^{\mu} B(\delta\beta' + \beta\delta') &&\equiv 1 \end{aligned}\right\} \pmod{2^{\mu+1}},$$

ou, ce qui revient au même,

$$\left.\begin{aligned} &B(\alpha\gamma' + \gamma\alpha') &&\equiv e \quad (31) \\ &B(\alpha\delta' + \delta\alpha' + \gamma\beta' + \beta\gamma') &&\equiv f \quad (32) \\ &B(\delta\beta' + \beta\delta') &&\equiv g \quad (33) \end{aligned}\right\} \pmod{2}.$$

Or α, β, γ, δ satisfaisant, comme on l'a vu, à la relation (30), β et δ ne seront pas pairs tous deux à la fois. Donc la relation (33) permettra toujours de déterminer l'une des quantités β', δ' en fonction de l'autre. Cela fait, α' et γ' seront déterminés sans difficulté par les congruences (31) et (32), dont le déterminant par rapport à ces variables est le nombre impair $\alpha\delta - \beta\gamma$.

16. *Deuxième cas.* — Supposons maintenant que Σ_ρ soit de la forme (25) : on pourra supposer $A < 8$.

Nous allons en effet donner le moyen de transformer au besoin cette expression en une autre semblable, où le coefficient A soit remplacé par a, reste de la division de A par 8.

Soit $A = a + e\,2^{\rho}$, e étant impair et ρ étant au moins égal à 3, puisque $A - a$ est divisible par 8. Posons

$$z = (1 + \alpha\,2^{\rho-1})\,z';$$

$A\,z^2$ sera changé en $A'z'^2$, et l'on aura

$$A' = (a + e\,2^{\rho})(1 + \alpha\,2^{\rho-1})^2 = a + (e + a\alpha)\,2^{\rho} + a\alpha\,2^{2\rho-2} + \dots.$$

Si donc on détermine α par la relation

$$e + a\alpha \equiv 0 \pmod{2},$$

on aura

$$A' \equiv a \pmod{2^{\rho+1}},$$

et, par suite,

$$A' = a + e' 2^{\sigma},$$

e' étant impair et $\sigma > \rho$. Renouvelant cette manière de procéder, on transformera $A' z'^2$ en $A'' z''^2$, A'' étant de la forme

$$a + e'' 2^{\tau}, \quad \tau > \sigma;$$

et, continuant ainsi, on arrive à faire en sorte que le coefficient du carré ne diffère de a que par des multiples du module 2^{λ}, lesquels peuvent être négligés.

On pourra donc supposer que A est < 8 et, par suite, se réduit à l'un des quatre nombres 1, 3, 5, 7.

17. De nouvelles limitations seront possibles si $\Sigma_{\rho+1}$ et $\Sigma_{\rho+2}$ sont eux-mêmes de la forme (25) ou de la forme (26).

1° Si $\Sigma_{\rho+1}$ est de la forme (25), on pourra supposer que le coefficient A du carré contenu dans Σ_{ρ} est congru à 1 (mod. 4).

Soit, en effet,

$$\Sigma_{\rho} = S_{\rho} + A z^2, \quad \Sigma_{\rho+1} = S_{\rho+1} + \mathfrak{b} \zeta^2,$$

et admettons que $A \equiv 3 \pmod 4$. Nous poserons

$$z = z' + 2\mathfrak{b}\zeta', \quad \zeta = \zeta' - A z',$$

substitution qui transformera

$$2^{\rho} \Sigma_{\rho} + 2^{\rho+1} \Sigma_{\rho+1} \equiv 2^{\rho} (S_{\rho} + A z^2 + 2 S_{\rho+1} + 2 \mathfrak{b} \zeta^2)$$

en

$$2^{\rho} [S_{\rho} + (A + 2\mathfrak{b} A^2) z'^2 + 2 S_{\rho+1} + 2(\mathfrak{b} + 2A) \zeta'^2),$$

expression de même forme, mais où le coefficient de z'^2 est égal à

$$A + 2\mathfrak{b} A^2 \equiv A + 2\mathfrak{b} \equiv A + 2 \equiv 1 \pmod 4.$$

2° Si $\Sigma_{\rho+1}$ est de la forme (26), auquel cas l'on aura

$$\Sigma_{\rho} = S_{\rho} + A z^2, \quad \Sigma_{\rho+1} = S_{\rho+1} + \mathfrak{b} \zeta^2 + \mathfrak{b}_1 \zeta_1^2,$$

on pourra de même supposer $A \equiv 1 \pmod 4$; mais si de plus on a

$$\mathfrak{a} + \mathfrak{a}_1 \equiv 2 \pmod 4,$$

on pourra supposer $A \equiv 1$.

En effet, le changement de variables du numéro précédent permet de transformer l'expression proposée de telle sorte que le coefficient de la nouvelle variable qui figure dans Σ_ρ devienne

$$A + 2\mathfrak{a}A^2 \equiv A + 2\mathfrak{a} \pmod 8.$$

On pourra de même changer ce coefficient en $A + 2\mathfrak{a}_1 \pmod 8$, ou par deux transformations successives en $A + 2\mathfrak{a} + 2\mathfrak{a}_1 \pmod 8$. Cela posé, parmi les quatre nombres

$$A, \quad A + 2\mathfrak{a}, \quad A + 2\mathfrak{a}_1, \quad A + 2\mathfrak{a} + 2\mathfrak{a}_1,$$

il est aisé de voir qu'il y en aura au moins un égal à $1 \pmod 8$; et l'on pourra par une transformation nouvelle, indiquée ci-dessus, le réduire à son résidu minimum 1.

3° Si $\Sigma_{\rho+2}$ est de l'une des deux formes (25) ou (26), on pourra supposer $A < 4 \pmod 8$.

Soit en effet, pour fixer ces idées,

$$\Sigma_\rho = S_\rho + Az^2, \quad \Sigma_{\rho+2} = S_{\rho+2} + \mathfrak{a}\zeta^2.$$

Si $A > 4 \pmod 8$, posons

$$z = z' + 4\mathfrak{a}\zeta', \quad \zeta = \zeta' - Az'.$$

Les termes $2^\rho (Az^2 + 4\mathfrak{a}\zeta^2)$ contenus dans la somme $\frac{1}{i}2^\rho \Sigma_\rho + 2^{\rho+2}\Sigma_{\rho+2}$ seront transformés en

$$2^\rho [(A + 4\mathfrak{a}A^2) z'^2 + 4(\mathfrak{a} + 4A\mathfrak{a}^2)\zeta'^2],$$

expression analogue à la précédente, mais où le coefficient de z'^2 est égal à

$$A + 4\mathfrak{a}A^2 \equiv A + 4\mathfrak{a} \equiv A + 4 < 4 \pmod 8.$$

18. *Troisième cas.* — Supposons que Σ_ρ soit de la forme (26). On pourra supposer

$$A \leqq A_1 \pmod 4, \quad A < 4, \quad A_1 < 8.$$

En effet, si l'on avait $A > A_1 \pmod 4$, on n'aurait qu'à changer z en z_1 et réciproquement pour renverser le sens de l'inégalité.

En second lieu, nous allons montrer qu'on peut supposer

$$A < 4 \pmod 8.$$

Soit en effet

$$A \equiv 4 + \alpha \pmod 8,$$

α étant < 4. Posons

$$z = z' + 2A_1 z'_1, \quad z_1 = z'_1 - 2Az'.$$

L'expression

$$Az^2 + A_1 z_1^2$$

sera transformée en une expression analogue

$$(A + 4A_1^2) z'^2 + (A_1 + 4A^2) z_1'^2.$$

Mais $A_1^2 \equiv 1 \pmod 8$, d'où

$$A + 4A_1^2 \equiv A + 4 \equiv \alpha \pmod 8.$$

L'expression transformée jouit donc de la propriété annoncée, que le reste de la division de son premier coefficient par 8 soit < 4.

Cela posé, la transformation du cas précédent, appliquée successivement aux deux termes Az^2, $A_1 z_1^2$, permettra de réduire leurs coefficients à leurs résidus (mod. 8), ce qu'il fallait démontrer.

19. La considération des suites $\Sigma_{\rho+1}$, $\Sigma_{\rho+2}$ permet d'introduire de nouvelles limitations.

1° Si $\Sigma_{\rho+1}$ ne se réduit pas à zéro, on pourra faire en sorte que A se réduise à l'unité.

Supposons d'abord que $\Sigma_{\rho+1}$ contienne un carré $\mathfrak{a}\zeta^2$; nous avons

vu qu'on peut supposer dans ce cas $A \equiv 1 \pmod 4$; d'ailleurs $A < 4$; donc $A = 1$.

Supposons, en second lieu, que $\Sigma_{\rho+1}$ contienne un rectangle tel que xy. La substitution

$$\begin{aligned} x &= x' - Az' - A_1 z'_1, \\ y &= y' - Az' - A_1 z'_1, \\ z &= z' + x' + y', \\ z_1 &= z'_1 + x' + y' \end{aligned}$$

de déterminant impair, opérée sur l'expression

$$2^\rho \Sigma_\rho + 2^{\rho+1} \Sigma_{\rho+1} = 2^\rho [S_\rho + Az^2 + A_1 z'_2 + 2(xy + \dots)],$$

la transforme en une expression analogue

$$\begin{aligned} 2_\rho [S_\rho &+ (A + 2A^2) z'^2 + 4AA_1 z' z'_1 + (A_1 + 2A_1^2) z'^2_1 \\ &+ (A + A_1) x'^2 + (2A + 2A_1 + 2) x'y' + (A + A_1) y'^2 + \dots]. \end{aligned}$$

Les termes en x', y', ayant leurs coefficients pairs, peuvent être joints aux autres termes de $\Sigma_{\rho+1}$. D'autre part, soit k un entier tel que l'on ait

$$(A_1 + 2A_1^2) k \equiv AA_1 \pmod{2^\lambda},$$

et faisons $z'_1 + kz' = z''_1$. Les autres termes de l'équation précédente pourront se mettre sous la forme

$$S_\rho + (A + 2A^2 - 4k^2) z'^2 + (A_1 + 2A_1^2) z''^2_1. \tag{34}$$

Or on a, A et A_1 étant impairs, ainsi que k,

$$\begin{aligned} A_1 + 2A_1^2 &\equiv A_1 + 2 \pmod 8, \\ A + 2A^2 - 4k^2 &\equiv A - 2 \pmod 8. \end{aligned}$$

On pourra donc, en appliquant les transformations indiquées plus haut, mettre l'expression (34) sous la forme

$$S_\rho + (A - 2) z^2 + A_1 - 2) z_1^2.$$

Or, par hypothèse, on avait $A < 4$; si donc il différait de l'unité, il était égal à 3; donc $A - 2 = 1$. Il est donc prouvé que l'on peut ramener à l'unité le coefficient du premier carré.

Supposons enfin que $\Sigma_{\rho+1}$ ne contienne ni rectangle ni carré isolé, mais soit de la forme $u^2 + uv + v^2$. On emploiera la substitution à déterminant impair

$$\begin{aligned} u &= u' - Az' - A_1 z'_1, \\ v &= v' - Az' - A_1 z'_1, \\ z &= 3z' + u' + v', \\ z_1 &= 3z'_1 + u' + v', \end{aligned}$$

qui transformera $2^\rho \Sigma_\rho + 2^{\rho+1} \Sigma_{\rho+1}$ en

$$\begin{aligned} 2^\rho [S_\rho + (9A + 6A^2) z'^2 - 12 AA_1 z' z'_1 + (9A_1 + 6A_1^2) z'^2_1 \\ + (A + A_1 + 2) u'^2 + (2A + 2A_1 + 2) u'v' + (A + A_1 + 2) v'^2]. \end{aligned}$$

Les termes en u', v' ont ici encore des coefficients pairs, et devront être comptés dans la suite $\Sigma_{\rho+1}$. Quant aux termes en z', z'_1, si l'on pose

$$\begin{aligned} (9A + 6A^2) k &\equiv 3AA_1 \pmod{2^\lambda}, \\ z' + kz'_1 &= z'', \end{aligned}$$

ils prendront la forme

$$(35) \qquad (9A + 6A^2) z''^2 + (9A_1 + 6A_1^2 - 4k^2) z'^2_1.$$

On a d'ailleurs

$$\begin{aligned} 9A + 6A^2 &\equiv 9A + 6 \equiv A - 2 \pmod{8}, \\ 9A_1 + 6A_1^2 - 4k^2 &\equiv 9A_1 + 2 \equiv A_1 + 2, \end{aligned}$$

et l'on pourra, par une transformation convenable, mettre l'expression (35) sous la forme

$$(A - 2) z^2 + (A_1 + 2) z_1^2,$$

ce qui démontre notre proposition.

2° Si $\Sigma_{\rho+2}$ est de la forme (25) ou de la forme (26), on pourra supposer A et $A_1 < 4$; car on les abaisserait au besoin au-dessous de cette limite, par la transformation indiquée (n° **17**).

20. Enfin, si $\Sigma_{\lambda-1}$ est de la forme (25) ou (26), on peut admettre que A et A_1 soient égaux à l'unité; car il suffirait pour les y réduire d'effacer les multiples de 2^λ dans l'expression $2^{\lambda-1}\Sigma_{\lambda-1}$.

De même, si $\Sigma_{\lambda-2}$ est de la forme (25) ou (26), on pourra supposer A et $A_1 < 4$.

21. La détermination du nombre de solutions de la congruence

$$F = a_1 x_1^2 + \ldots + a_m x_m^2 + b_{12} x_1 x_2 + \ldots \equiv c \pmod{2^\lambda}$$

peut maintenant se faire sans difficulté.

Ramenons cette congruence, par un changement de variables, à sa forme canonique

$$F = \Sigma 2^\rho \Sigma_\rho \equiv c \pmod{2^\lambda}. \tag{36}$$

Soit n le nombre des variables qui figurent explicitement dans la congruence transformée. On verra, comme au n° **3** :

1° Que le nombre des solutions cherchées est égal à $2^{\lambda(m-n)}Q$, Q étant le nombre des solutions de la congruence (36), où l'on ne considère plus que les variables qui y figurent explicitement;

2° Que si Σ_α est parmi les sommes Σ_1, Σ_2,... la première qui ne s'annule pas, on aura $Q = 0$ toutes les fois que c n'est pas divisible par 2^α. Soient, au contraire, $c = 2^\alpha d$, $\lambda - \alpha = \mu$; on aura

$$Q = 2^{\alpha n} R,$$

R étant le nombre des solutions de la congruence

$$\Sigma_\alpha + 2\Sigma_{\alpha+1} + \ldots \equiv d \pmod{2^\mu}. \tag{37}$$

Cela posé, nous allons montrer que la détermination de R peut toujours se ramener à un problème analogue, mais pour un module $< 2^\mu$

22. On aura en général

$$\Sigma_\alpha = s_\alpha + \mathfrak{E},$$

s_α étant une somme de rectangles, telle que $x_1 y_1 + \ldots + x_p y_p$ et $\mathfrak{E}$ se réduisant soit à zéro, soit à l'une des formes Az^2, $Az^2 + A_1 z_1^2$, $u^2 + uv + v^2$. Nous supposerons, pour plus de généralité, que p ne soit pas nul, et nous distinguerons deux espèces de solutions, suivant que l'une des variables $y_1, \ldots, y_p$ est impaire, ou qu'elles sont toutes paires.

Le nombre des systèmes de valeurs de $y_1, \ldots, y_p$ (mod. 2^μ) qui ne soient pas toutes paires à la fois est évidemment égal à $2^{\mu p} - 2^{(\mu-1)p}$. L'un quelconque de ces systèmes étant choisi, et y_1, par exemple, étant supposé impair, la congruence (37) déterminera sans difficulté la variable x_1 en fonction des $n - p - 1$ variables restantes, qui seront arbitraires et pourront être choisies chacune de 2^μ manières distinctes. Donc le nombre total des solutions de première espèce sera

$$(2^{\mu p} - 2^{(\mu-1)p})\, 2^{\mu(n-p-1)}.$$

Passons aux solutions de seconde espèce. Posons

$$y_1 = 2y'_1, \ldots, \quad y_p = 2y'_p, \quad \Sigma'_{\alpha+1} = \Sigma_{\alpha+1} + x_1 y'_1 + \ldots + x_p y'_p,$$

la congruence deviendra

$$\mathfrak{E} + 2\Sigma'_{\alpha+1} + \ldots \equiv d \pmod{2^\mu}. \tag{38}$$

Les nouvelles variables $y'_1, \ldots, y'_p$ ne doivent plus varier ici que de zéro à $2^{\mu-1} - 1$; mais, le premier membre de (38) ne changeant pas de valeur (mod. 2^μ) lorsqu'on augmente de $2^{\mu-1}$ une des quantités $y'_1, \ldots, y'_p$, il est clair qu'on pourra étendre leur champ d'excursion jusqu'à $2^\mu - 1$, pourvu que l'on divise par 2^p le nombre des solutions obtenues dans cette dernière hypothèse.

On est donc ramené à chercher le nombre Q′ de solutions de la congruence (38), où toutes les variables se meuvent de zéro à $2^\mu - 1$.

23. *Premier cas :* $\mathfrak{E} = 0$. — Le nombre Q′ sera nul lorsque d sera

impair. Si d est un nombre pair $2d'$, Q' sera égal (**21**) à 2^nR', R' étant le nombre des solutions de la congruence

$$\Sigma'_{\alpha+1} + \Sigma_{\alpha+2} + \ldots \equiv d' \pmod{2^{\mu-1}}, \tag{39}$$

où les variables ne se meuvent plus qu'au-dessous de $2^{\mu-1}$.

La congruence (39) est analogue à la congruence (37), mais son module est moindre. Le problème est donc réduit, comme nous l'avons annoncé (**21**); de telle sorte que nous pouvons passer à l'examen des autres cas.

24. *Second cas :* $\varepsilon = Az^2$. — Si d est pair, la congruence (38) ne pourra être satisfaite que si z est un nombre pair. Posons donc

$$z = 2z', \quad \Sigma'_{\alpha+2} = \Sigma_{\alpha+2} + Az'^2.$$

On aura à satisfaire à la congruence

$$2\Sigma'_{\alpha+1} + 4\Sigma'_{\alpha+2} + \ldots \equiv d \pmod{2^{\mu}},$$

ou, ce qui revient au même, à celle-ci

$$\Sigma'_{\alpha+1} + 2\Sigma'_{\alpha+2} + \ldots \equiv \frac{d}{2} \pmod{2^{\mu-1}}, \tag{40}$$

où la variable z' se meut au-dessous de $2^{\mu-1}$. On peut d'ailleurs faire la même supposition pour les $n-1$ autres variables, pourvu qu'on multiplie par 2^{n-1} le nombre des solutions trouvé. Cela posé, la congruence (40) ayant un module moindre que la congruence (37), le problème est encore réduit.

25. Soit, au contraire, d impair; z sera impair, et la valeur de Az^2 restera la même (mod. 2^{μ}) pour deux valeurs de z congrues entre elles suivant le module $2^{\mu-1}$. On aura donc $Q' = 2Q_{\mu}$, Q_{μ} étant le nombre des solutions que l'on aurait, en supposant que z ne variât plus qu'au-dessous de $2^{\mu-1}$, les autres variables x, y,... continuant à se mouvoir jusqu'à 2^{μ}.

Supposons maintenant $\mu > 3$, et posons

$$z = z' + \zeta 2^{\mu-2}, \quad x = x' + \xi 2^{\mu-1}, \quad y = y' = \eta 2^{\mu-1}, \quad d = d' + \delta 2^{\mu-1},$$

z' étant $< 2^{\mu-2}$, $x', y', \ldots, d' < 2^{\mu-1}$, et $\zeta, \xi, \eta, \ldots, \delta$ égaux à zéro ou à 1.

Si l'on suppose que $z, x, y, \ldots$ est un système de solutions de la congruence

$$(41) \qquad Az^2 + 2\Sigma'_{\alpha+1} + \ldots \equiv d \pmod{2^\mu},$$

il est clair que $z', x', y', \ldots$ satisferont à cette congruence pour le module $2^{\mu-1}$. Réciproquement, soient $z', x', y', \ldots$ un des $Q_{\mu-1}$ systèmes de solutions relatifs à ce dernier module;

$$D \equiv d \pmod{2^{\mu-1}} = d' + \delta' 2^{\mu-1}$$

la valeur correspondante du premier membre de (41) : on vérifie sans peine que $z, x, y, \ldots$ satisferont à la congruence pour le module 2^μ, quels que soient $\xi, \eta, \ldots$, si l'on détermine ζ par la relation

$$(A\zeta + \delta') \equiv \delta \pmod{2},$$

ce qui est toujours possible [*].

Chacune des $n-1$ quantités $\xi, \eta, \ldots$ étant susceptible de deux valeurs, on aura

$$Q_\mu = 2^{n-1} Q_{\mu-1} = \ldots = 2^{(n-1)(\mu-3)} Q_3.$$

26. Il ne reste donc plus qu'à calculer Q_3.

Effaçons dans la congruence (41) tous les multiples de 8, il viendra

$$Az^2 + 2\Sigma'_{\alpha+1} + 4\Sigma_{\alpha+2} \equiv d \pmod{8},$$

ou, plus simplement, z^2 étant congru à 1 (mod. 8),

$$(42) \qquad 2\Sigma'_{\alpha+1} + 4\Sigma_{\alpha+2} \equiv d - A \pmod{8}.$$

---

[*] Si μ n'était pas > 3, le terme $\zeta^2 2^{2\mu-4}$, que renferme le développement de Az^2, ne serait plus zéro (mod. 2^μ), ce qui troublerait le raisonnement.

Soit t le nombre des variables qui figurent explicitement dans cette équation; les autres variables prenant les diverses valeurs de o à 7, sauf z, qui varie de o à 3 seulement, il est clair que l'on aura

$$Q_3 = 2^{3(n-t)-1} R,$$

R étant le nombre des solutions de la congruence (42), en ne tenant plus compte des autres variables.

Cela posé, soient respectivement T_b, U_c les nombres de solutions des congruences

$$\Sigma'_{\alpha+1} \equiv b \pmod 4, \tag{43}$$

$$\Sigma_{\alpha+2} \equiv c \pmod 2, \tag{44}$$

il est clair que l'on aura

$$R = \sum T_b U_c,$$

la sommation s'étendant à tous les systèmes de valeurs de b, c (mod. 8), qui satisfont à la congruence

$$2b + 4c \equiv d - A \pmod 8. \tag{45}$$

Or il est aisé, pour chaque système de valeurs de b et de c, de calculer T_b, U_c.

27. Calculons d'abord T_b. Soit r le nombre des variables contenues dans $\Sigma'_{\alpha+1}$. Leur champ d'excursion est de o à 7; mais on peut évidemment ne les faire varier que de o à 3, pourvu qu'on multiplie par 2^r le nombre des solutions que nous allons trouver.

On aura, dans le cas le plus général,

$$\Sigma'_{\alpha+1} = \mathfrak{s} + \mathfrak{C},$$

$\mathfrak{s}$ étant une somme de rectangles telle que

$$x_1 y_1 + \ldots + x_q y_q,$$

et $\mathfrak{C}$ une expression de l'une des formes

$$A_1 z_1^2, \quad A_1 z_1^2 + A_2 z_2^2, \quad u^2 + uv + v^2.$$

Supposons d'abord que l'on ait simplement

$$\Sigma'_{\alpha+1} = s.$$

Les solutions de la congruence

$$x_1 y_1 + \ldots + x_q y_q \equiv b \pmod 4$$

sont de deux sortes : celles pour lesquelles $y_1, \ldots, y_q$ ne sont pas tous pairs, et dont le nombre sera égal à $(2^{2q} - 2^q)\, 2^{2(q-1)}$ (car les systèmes de valeurs non paires de $y_1, \ldots, y_q$ sont en nombre $2^{2q} - 2^q$, et, l'un d'eux étant donné, on pourra déterminer une des variables $x_1, \ldots, x_q$ en fonction des $q - 1$ autres qui resteront arbitraires), et celles pour lesquelles $y_1, \ldots, y_q$ sont pairs. Il n'y a aucune solution de cette seconde sorte si b est impair. Si b est pair, on posera

$$y_1 = 2y'_1, \ldots, \quad y_q = 2y'_q;$$

la congruence deviendra

$$x_1 y'_1 + \ldots + x_q y'_q \equiv \frac{b}{2} \pmod 2, \tag{46}$$

et le nombre de ses solutions sera évidemment égal à 2^q fois le nombre des solutions qu'elle aurait en supposant que $x_1, \ldots, x_q$, de même que $y_1, \ldots, y_q$, ne variassent que de 0 à 1.

Ce dernier nombre s'obtient aisément. Si $\frac{b}{2}$ est impair, l'un des entiers $y'_1, \ldots, y'_q$ devra être impair, et l'on aura $(2^q - 1)\, 2^{q-1}$ solutions, toutes de première espèce. Si $\frac{b}{2}$ est pair, il faudra y ajouter les 2^q solutions de seconde espèce, correspondant à $y_1 \equiv \ldots \equiv y_q \pmod 2$.

Soient, en second lieu, $s = 0$, $\varpi = A_1 z_1^2$. On aura à satisfaire à la relation

$$A_1 z_1^2 \equiv b \pmod 4,$$

laquelle sera impossible si $b \equiv 2 \pmod 4$ ou $b \equiv A_1 + 2 \pmod 4$, et admettra deux solutions si $b \equiv 0$ ou $\equiv A_1$.

Soient maintenant $s = 0$, $\varpi = A_1 z_1^2 + A_2 z_2^2$. Si b est impair et

$A_1 \gtrless A_2 \pmod 4$, on aura, en posant z_1 pair, z_2 impair, 4 solutions pour $b = A_1$; en posant z_1 impair, z_2 pair, 4 solutions pour $b = A_2$; si $A_1 \equiv A_2$, ces 8 solutions se concentreront sur cette seule valeur de b.

Si b est pair et $A_1 \gtrless A_2$, d'où $A_1 + A_2 \equiv 0$, on aura 8 solutions pour $b \equiv 0$, aucune pour $b \equiv 2$; mais si $A_1 \equiv A_2$, on aura 4 solutions pour $b \equiv 0$, 4 pour $b \equiv 2$.

Soient encore $s = 0$, $\mathfrak{S} = u^2 + uv + v^2$. On aura 4 solutions si $b \equiv 0$, 6 si b est impair, aucune si $b \equiv 2$.

Soit enfin $\Sigma'_{\alpha+1} = s + \mathfrak{S}$. La congruence

$$s + \mathfrak{S} \equiv b \pmod 4$$

aura évidemment un nombre de solutions représenté par

$$\sum T'_\beta T''_\gamma,$$

T'_β, T''_γ désignant respectivement les nombres de solutions des congruences

$$s \equiv \beta, \quad \mathfrak{S} \equiv \gamma \pmod 4,$$

et la sommation s'étendant à tous les systèmes de valeurs de β et de γ tels que l'on ait

$$\beta + \gamma \equiv b \pmod 4.$$

28. Le calcul de U_c se fait comme le précédent, mais plus simplement. On aura d'abord $U_c = 2^{2s} U'_c$, s étant le nombre des variables contenues dans $\Sigma_{\alpha+2}$, et U'_c le nombre des solutions de la congruence (46) lorsqu'on ne les fait plus varier que de 0 à 1.

Si $\Sigma_{\alpha+2}$ se réduit à la forme $x_1 y_1 + \ldots + x_t y_t$, la congruence

$$\Sigma_{\alpha+2} \equiv c \pmod 2$$

n'aura de solutions, si c est impair, qu'en supposant que $y_1, \ldots, y_q$ ne soient pas pairs à la fois. Ces solutions seront en nombre $(2^t - 1)2^{t-1}$. Si c est pair, on aura, en outre, 2^t solutions de seconde espèce à ajouter aux précédentes pour former U'_c.

Si $\Sigma_{\alpha+2} = x_1 y_1 + \ldots + x_t y_t + A z^2$ (ou $+ A z^2 + A' z'^2$), on voit,

en remarquant que $Az^2 \equiv z \pmod 2$, que la relation (44) définit z en fonction des $s-1$ autres variables restantes, qui demeurent arbitraires. Donc $U'_t = 2^{s-1}$.

Enfin, si $\Sigma_{\alpha+2} = x_1 y_1 + \ldots + x_t y_t + u^2 + uv + v^2$, on aura

$$u^2 + uv + v^2 \equiv u + uv + v \equiv (u+1)(v+1) - 1 \pmod 2;$$

d'où, en posant $u+1 = x_{t+1}$, $v+1 = y_{t+1}$,

$$x_1 y_1 + \ldots + x_{t+1} y_{t+1} \equiv c - 1 \pmod 2,$$

congruence dont le nombre de solutions est connu par ce qui précède.

29. Il resterait à examiner les cas où $\mu = 2$ ou $\mu = 1$; mais la manière de les traiter est suffisamment indiquée par ce qui précède.

30. *Troisième cas :* $\mathfrak{G} = Az^2 + A_1 z_1^2$. — Nous distinguerons plusieurs sortes de solutions, suivant que les variables z, z_1 seront paires ou impaires.

Si z_1 est pair, on posera $z_1 = 2z'_1$, z'_1 étant une nouvelle variable dont le champ d'excursion est de 0 à $2^{\mu-1} - 1$, mais peut être poussé jusqu'à $2^{\mu} - 1$, pourvu qu'on ait soin de diviser par 2 le nombre des solutions obtenues dans cette nouvelle hypothèse. Posant alors

$$\Sigma_{\alpha+2} + A_1 z_1'^2 = \Sigma'_{\alpha+2},$$

on aura à résoudre la congruence

$$Az^2 + 2\Sigma'_{\alpha+1} + 4\Sigma'_{\alpha+2} + \ldots \equiv d \pmod 2,$$

question déjà traitée (n^{os} **24** à **29**).

Si z_1 est impair, mais z pair, on posera $z = 2z'$, et l'on aura à résoudre la congruence

$$A_1 z_1^2 + 2\Sigma'_{\alpha+1} + 4(\Sigma_{\alpha+2} + Az^2) + \ldots \equiv d \pmod 2,$$

où z_1 est supposé impair; question déjà traitée (n^{os} **24** à **29**).

Soient enfin z et z_1 impairs. Si $\mu > 3$, on ramènera, comme au n° **25**, la question au cas où $\mu = 3$, et la congruence

$$Az^2 + A_1 z_1^2 + 2\Sigma'_{\alpha+1} + 4\Sigma_{\alpha+2} \equiv d \pmod 8$$

se réduit, en remarquant que $z^2 \equiv z_1^2 \equiv 1$, à

$$2\Sigma'_{\alpha+1} + 4\Sigma_{\alpha+2} \equiv d - A - A_1 \pmod 8,$$

congruence analogue à celle déjà traitée au n° **26**.

Nous passons ici encore sur les cas où $\mu < 3$, car ils sont implicitement résolus par ce qui précède.

31. *Quatrième cas* : $\varepsilon = u^2 + uv + v^2$. — Supposons d'abord d impair; l'une au moins des quantités u, v sera impaire. Soient dans ce cas u, v, x, y,... les variables contenues dans la congruence donnée

$$(47) \qquad u^2 + uv + v^2 + 2\Sigma_{\alpha+1} + \ldots \equiv d \pmod{2^\mu}.$$

Posons

$$u = u' + u_1 2^{\mu-1}, \quad v = v' + v_1 2^{\mu-1}, \quad x = x' + x_1 2^{\mu-1}, \ldots, \quad d = d' + d_1 2^{\mu-1}$$

u', v', x',..., d' étant $< 2^{\mu-1}$, et u_1, v_1, x_1,..., d_1 étant égaux à 0 ou à 1. Si u, v, x,... est un système de solutions pour la congruence (47), il est clair que u', v', x',... satisferont à la même congruence relativement au module $2^{\mu-1}$. Réciproquement, soient u', v', x',... un système de solutions pour le module $2^{\mu-1}$; on aura

$$u'^2 + u'v' + v'^2 + \ldots \equiv d \pmod{2^{\mu-1}} \equiv d + \delta 2^{\mu-1} \pmod{2^\mu},$$

et u, v, x,... sera un système de solutions de la congruence pour le module 2^μ, si l'on a

$$u'v_1 + v'u_1 \equiv \delta \pmod 2,$$

relation qui pourra toujours servir à déterminer l'un des entiers v_1 ou u_1, car u' ou v' est impair. Tous les entiers de la suite u_1, v_1, x_1,...

sauf celui dont il s'agit, pourront être pris à volonté égaux à 0 ou à 1. Donc, si l'on désigne par t le nombre des variables de la congruence (47), par Q_μ le nombre de ses solutions pour le module 2^μ, on aura

$$Q_\mu = 2^{t-1} Q_{\mu-1} = 2^{(t-1)(\mu-1)} Q_1.$$

Or, si $\mu = 1$, la congruence (47) se réduit à

$$u^2 + uv + v^2 \equiv d \pmod 2 \equiv 1 \pmod 2,$$

et l'on aura ses solutions en posant $u = 1$ et $v = 0$ ou 1, ou $u = 0$, $v = 1$, avec $x, y, \ldots$ arbitraires, soit $3 \cdot 2^{t-2}$ solutions. Donc $Q_1 = 3 \cdot 2^{t-2}$.

32. Supposons maintenant d pair; u et v devront être pairs. Posons donc

$$u = 2u', \quad v = 2v', \quad \Sigma_{\alpha+2} + u'^2 + u'v' + v'^2 = \Sigma'_{\alpha+2};$$

on aura à résoudre la congruence

$$2\Sigma_{\alpha+1} + 4\Sigma'_{\alpha+2} + \ldots \equiv d \pmod{2^\mu},$$

ou

$$\Sigma_{\alpha+1} + 2\Sigma'_{\alpha+2} + \ldots \equiv \frac{d}{2} \pmod{2^{\mu-1}}.$$

Dans cette congruence, les $t - 2$ variables autres que u', v' se meuvent de 0 à $2^\mu - 1$; mais on peut borner leur champ d'excursion à $2^{\mu-1} - 1$, pourvu qu'on multiplie par 2^{t-2} le nombre R des solutions trouvées dans cette dernière hypothèse.

Il ne reste donc plus qu'à trouver R, nombre des solutions d'une congruence prise suivant le module $2^{\mu-1}$. Donc le problème, ici encore, se trouve réduit.

33. Comme exemple numérique, cherchons le nombre des solutions de la congruence

$$23x^2 + 21xy + 2y^2 + zy + 5zx + z^2 + 2x_1y_1 + 4x_1v + 2uz + 5u^2 + 12uv + 4v^2 \equiv 12 \pmod{32}.$$

Il faut commencer par la ramener à sa forme canonique. Pour cela,

remarquons que le coefficient de xy est impair, et celui de y^2 pair. En remplaçant y par $y + \alpha x$, le coefficient de x^2 deviendra

$$A = 23 + 21\alpha + 2\alpha^2,$$

et l'on pourra le rendre congru à zéro (mod. 32). A cet effet, on se rappellera la remarque faite plus haut que si, pour une certaine valeur α_i de α, on a $A = 2^\rho i$, i étant impair, A sera pour $\alpha_0 + 2^\rho$ de la forme $2^\sigma i$, σ étant $> \rho$.

On posera donc successivement

$$\begin{aligned}
&\alpha = 0, && \text{d'où } A = i;\\
&\alpha = 1, && \text{d'où } A = 46 = 2i;\\
&\alpha = 1 + 2 = 3, && \text{d'où } A = 104 = 8i;\\
&\alpha = 3 + 8 = 11, && \text{d'où } A = 16i;\\
&\alpha = 11 + 16 = 27 \equiv -5 \pmod{32}.
\end{aligned}$$

Remplaçant donc y par $y - 5x$ dans la congruence donnée, elle deviendra

$$xy + 2y^2 + zy + z^2 + 2x_1y_1 + \ldots \equiv 12 \pmod{32},$$

ou, en remplaçant x par $x - 2y - z$,

$$xy + z^2 + 2x_1y_1 + 4x_1v + 2uz + 5u^2 + 12uv + 4v^2 \equiv 12 \pmod{32}.$$

Les variables x, y sont déjà isolées. On isolera la variable z, dont les rectangles ont des coefficients pairs et le carré un coefficient impair, en la remplaçant par $z - u$; la congruence devient

$$xy + z^2 + 2x_1y_1 + 4x_1v + 4u^2 + 12uv + 4v^2 \equiv 12 \pmod{32},$$

et, en remplaçant y_1 par $y_1 - v$, en remarquant, d'autre part, que les termes $4u^2 + 12uv + 4v^2$ peuvent être ramenés à la forme $4(u^2 + uv + v^2)$ par une transformation opérée sur les indices u et v (n° **15**), transformation dont il nous suffit d'avoir le résultat sans avoir besoin de l'effectuer, on ramènera la congruence à sa forme canonique

$$(48)\quad xy + z^2 + 2x_1y_1 + 4(u^2 + uv + v^2) \equiv 12 \pmod{32}.$$

34. Cherchons maintenant le nombre N de ses solutions.

Si y est impair, $z, x_1, \ldots$ seront arbitraires et x déterminé, ce qui donne 16.32^5 solutions de première espèce.

Pour avoir les solutions de seconde espèce, on devra changer y en $2y$, et leur nombre sera $\frac{1}{2}N_1$, N_1 étant le nombre des solutions de la congruence

$$(49)\quad z^2 + 2(x_1y_1 + xy) + 4(u^2 + uv + v^2) \equiv 12 \pmod{32}.$$

Or z est nécessairement pair; changeons-le en $2z$; on aura $N_1 = 2^6 N_2$, N_2 étant le nombre des solutions de la congruence

$$(50)\quad x_1y_1 + xy + 2(u^2 + uv + v^2 + z^2) \equiv 6 \pmod{16}.$$

Cette nouvelle congruence ne satisfait plus aux conditions imposées à nos formes canoniques; mais nous pourrons, par des transformations d'indices (qu'il est inutile d'effectuer pour notre objet actuel), transformer $u^2 + uv + v^2 + z^2$ en

$$(1 + 4 + 4 + 4)z'^2 + Au'^2 + Bu'v' + Cv'^2,$$

A et C étant pairs et B impair (n° **11**); puis remplacer ces trois derniers termes eux-mêmes par le produit de deux nouvelles variables x_2, y_2 (n° **8**); enfin supprimer les multiples de 8 dans le coefficient de z'^2 (n° **16**), ce qui réduira la congruence (50) à la forme

$$x_1y_1 + xy + 2(x_2y_2 + 5z'^2) \equiv 6 \pmod{16}.$$

Cette congruence a $(16^2 - 8^2)16^4$ solutions de première espèce (y, y_1 non pairs à la fois), et $2^5 N_3$ solutions de seconde espèce, N_3 étant le nombre des solutions de la congruence

$$xy + x_1y_1 + x_2y_2 + 5z'^2 \equiv 3 \pmod{8}.$$

Or cette congruence, n'ayant de solutions que si y, y_1, y_2 ne sont pas tous pairs, en aura en tout $(8^3 - 4^3)8^3$.

Récapitulant ces résultats, on aura

$$N = 16.32^5 + 2^5[(16^2 - 8^2)16^4 + 2^5(8^3 - 4^3)8^3] = 35.2^{25}.$$