Mathematics. — *Sur quelques systèmes de congruences.* Par J. G. VAN DER CORPUT.

(Communicated at the meeting of March 25, 1939.)

Les recherches modernes de la théorie additive des nombres conduisent à l'étude suivante. Considérons une congruence de la forme

$$\psi(y) \equiv 0 \qquad (mod.\ p^{\beta}),$$

où $\psi(y)$ est un polynôme à coefficients entiers, p un nombre premier et β un nombre naturel. Désignons par Q_β le nombre des solutions de cette congruence. Il y a des polynômes pour lesquels Q_β croît indéfiniment avec β, par exemple la congruence

$$y^2 \equiv 0 \qquad (mod.\ p^{\beta})$$

possède $p^{\frac{1}{2}\beta}$ ou $p^{\frac{1}{2}(\beta-1)}$ solutions, selon que β est pair ou impair. D'autre part il existe des polynômes $\psi(y)$ pour lesquels Q_β est borné. Il y a même des polynômes pour lesquels Q_β possède une même valeur pour tous les β supérieurs à une certaine borne. Ceci est le cas, comme M. LOO—KENG HUA [1]) l'a démontré, pour chaque polynôme $\psi(y)$ à coefficients entiers tel que le plus grand commun diviseur D de $\psi(y)$ et de sa dérivée $\psi'(y)$ soit indépendant de y. Dans ce cas M. HUA a démontré que Q_β possède la même valeur pour les $\beta \geqq 2\gamma+1$, où p^γ désigne la puissance la plus élevée de p qui divise D. Considérons maintenant un polynôme $\psi(y_1,\ldots,y_s)$ à coefficients entiers et désignons $\frac{\partial\psi}{\partial y_\sigma}$ par $\psi_\sigma(y_1,\ldots,y_s)$ $(\sigma=1,\ldots,s)$. Supposons qu'il existe un nombre $\gamma \geqq 0$ tel que le système des s congruences

$$\psi(y_1,\ldots,y_s) \equiv 0\ (mod.\ p^{2\gamma+1});\ \psi_\sigma(y_1,\ldots,y_s) \equiv 0\ (mod.\ p^{\gamma+1}) \qquad (1)$$

$(\sigma=1,\ldots,s)$ n'ait aucune solution. Si nous désignons par $p^{(s-1)\beta}Q_\beta$ le nombre des solutions de la congruence

$$\psi(y_1,\ldots,y_s) \equiv 0 \qquad (mod.\ p^{\beta}),$$

le nombre Q_β possède, comme nous le démontrerons, la même valeur pour tous les $\beta \geqq 2\gamma+1$.

La condition imposée est certainement remplie, si nous pouvons trouver $s+1$ polynômes à coefficients entiers $u(y_1,\ldots,y_s)$ et $u_\sigma(y_1,\ldots,y_s)$ tels que

$$u(y_1,\ldots,y_s)\,\psi(y_1,\ldots,y_s) + \sum_{\sigma=1}^{s} u_\sigma(y_1,\ldots,y_s)\,\psi_\sigma(y_1,\ldots,y_s)$$

[1]) Journal of the London Mathematical Society, **13**, 54—61 (1938).

soit égal à un nombre $D \neq 0$ indépendant de $y_1,\ldots,y_s$. En effet, on peut alors choisir pour p^γ la puissance la plus élevée de p qui divise D. Ce fait, appliqué avec $s=1$, donne le résultat cité plus haut de M. HUA.

Si $\psi(y_1,\ldots,y_s)$ est égal à $\Psi(y_1,\ldots,y_s)-t$, où $t\neq 0$ est indépendant de $y_1,\ldots,y_s$ et où $\Psi(y_1,\ldots,y_s)$ désigne une forme en $y_1,\ldots,y_s$ de degré $k \geqq 1$, on a

$$-k\psi(y_1,\ldots,y_s) + \sum_{\sigma=1}^{s} y_\sigma \psi_\sigma(y_1,\ldots,y_s) = kt;$$

dans ce cas la condition imposée est valable, si l'on choisit pour p^γ la puissance la plus élevée de p qui divise kt.

Généralisons le résultat précédent en considérant au lieu d'une congruence un système de congruences

$$\psi_\mu(y_1,\ldots,y_s) \equiv 0\ (mod.\ p^{\beta}) \quad (\mu=1,\ldots,m),$$

où s est $\geqq m$ et où $\psi_\mu(y_1,\ldots,y_s)$ désigne un polynôme à coefficients entiers. Comme nous le verrons, il est utile de considérer la matrice

$$M = \begin{pmatrix} \psi_{11} & \ldots & \psi_{1s} \\ \ldots & \ldots & \ldots \\ \psi_{m1} & \ldots & \psi_{ms} \end{pmatrix},$$

où $\psi_{\mu\sigma} = \frac{\partial\psi_\mu}{\partial y_\sigma}$. Je supposerai que M possède le rang m. Les puissances $p^{\alpha_1}, p^{\alpha_2},\ldots,p^{\alpha_m}$ s'appellent les diviseurs élémentaires modulo p de M, si $p^{\alpha_1+\ldots+\alpha_\mu}$ est pour $\mu=1,\ldots,m$ la puissance la plus élevée de p qui divise chaque déterminant d'ordre μ de M.

Ces diviseurs élémentaires modulo p ne changent pas par les transformations suivantes de M, qui s'appellent des transformations élémentaires [1]):

1. Echanger deux lignes entre elles ou deux colonnes entre elles.
2. Multiplier tous les éléments d'une ligne (colonne) par un même entier qui n'est pas divisible par p.
3. Ajouter aux éléments d'une ligne (colonne) les éléments correspondants d'une autre ligne (colonne) multipliés par un même entier.
4. Remplacer un élément par un entier qui lui est congru modulo $p^{\alpha_1+\ldots+\alpha_m+1}$.

Si une matrice M peut être transformée en une matrice M' par un nombre fini de transformations élémentaires, les matrices M et M' sont dites équivalentes.

Comme M renferme au moins un élément qui n'est pas divisible par p^{α_1+1}, il existe une matrice équivalente à M dont le premier élément n'est pas divisible par p^{α_1+1} (opération 1). Il existe donc une matrice équivalente à M dont le premier élément est égal à p^{α_1} (opérations 2 et 4).

[1]) Comparez par exemple: M. BÔCHER, Introduction to Higher Algebra, 1924, Chapter XX, ou Einführung in die Höhere Algebra, 1910, Kapitel XX.

Comme tous les éléments de cette matrice sont divisibles par p^{α_1}, il existe une matrice équivalente à M, dont le premier élément est égal à p^{α_1} et dont les autres éléments figurant dans la première ligne ou première colonne s'annulent (opération 3). La répétition de ce raisonnement nous apprend que la matrice

$$M' = \begin{pmatrix} p^{\alpha_1} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & p^{\alpha_2} & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & p^{\alpha_m} & 0 & \dots & 0 \end{pmatrix}$$

est équivalente à M. Comme chaque élément de M' est divisible par p^{α_1}, on a $\alpha_1 \leqq \alpha_2$ et de la même manière on trouve $\alpha_1 \leqq \alpha_2 \leqq \dots \leqq \alpha_m$.

Si nous remplaçons dans M un élément par un entier qui lui est congru modulo p^{α_m+1}, les diviseurs élémentaires modulo p ne changent pas. En effet, un déterminant quelconque d'ordre μ de M est remplacé par un déterminant qui lui est congru modulo $p^{\alpha_1+\dots+\alpha_{\mu-1}+\alpha_m+1}$, donc modulo $p^{\alpha_1+\dots+\alpha_\mu+1}$.

Considérons maintenant le système de congruences

$$\sum_{\sigma=1}^{s} \psi_{\mu\sigma}(y_1, \dots, y_s)\, h_\sigma \equiv b_\mu\, p^{\alpha_m} \,(mod.\ p^\tau), \quad . \quad . \quad . \quad . \quad (3)$$

$(\mu = 1, , , , m)$, où $b_1, \dots, b_m$ sont entiers et $\tau \geqq \alpha_m$. Les transformations 1, 2 et 3 de M transforment ce système de congruences en un système possédant le même nombre de solutions; au lieu des membres de droite on obtient les mêmes ou d'autres multiples de p^{α_m}. Le nombre des solutions de (3) ne change non plus, si $\psi_{\mu\sigma}(y_1, \dots, y_s)$ est remplacé par un entier qui lui est congru à $p^{\tau+1}$. Par cette opération et les opérations 1, 2 et 3 on peut transformer (3) en

$$p^{\alpha_\mu}\, h'_\mu \equiv b'_\mu\, p^{\alpha_m} \,(mod.\ p^\tau) \qquad (\mu = 1, \dots, m), \quad . \quad . \quad . \quad . \quad (4)$$

de façon que le nombre des solutions $(h_1, \dots, h_s)$ de (3) est égal au nombre des solutions $(h'_1, \dots, h'_s)$ de (4), donc égal à $p^{(s-m)\tau+\alpha_1+\dots+\alpha_m}$.

Passons après ces remarques préliminaires à la proposition 1.

Proposition 1: *Supposons qu'il existe un entier $\gamma \geqq 0$ tel que pour toute solution du système de congruences*

$$\psi_\mu(y_1, \dots, y_s) \equiv 0 \,(mod.\ p^{2\gamma+1}) \qquad (\mu = 1, \dots, m). \quad . \quad . \quad (5)$$

le rang de M soit m et que le dernier diviseur élémentaire modulo p de M soit $\leqq p^\gamma$. Si nous désignons par $p^{(s-m)\beta} Q_\beta$ le nombre des solutions de (2), le nombre Q_β possède la même valeur pour chaque $\beta \geqq 2\gamma + 1$.

On peut ajouter à cette proposition une autre proposition plus générale. Soit ν un entier $\geqq 0$. Je dis qu'une solution $y = (y_1, \dots, y_n)$ de (2) possède la propriété $P(\alpha_1, \dots, \alpha_m)$, si le rang de la matrice M est égal à m et

si $p^{\alpha_1}, \dots, p^{\alpha_m}$ sont les diviseurs élémentaires modulo p de M. Comme nous le démontrerons, la proposition 1 découle immédiatement de la suivante.

Proposition 2: *Introduisons les entiers $s, m, \beta, w_1, \dots, w_s$ tels que nous ayons $s \geqq m \geqq 1$ et $\beta \geqq 1$; introduisons en outre m polynômes $\psi_\mu(y_1, \dots, y_s)$ à coefficients entiers et m entiers non-négatifs $\alpha_1 \leqq \alpha_2 \leqq \dots \leqq \alpha_m$. Posons $\alpha_m = \nu$ et $\beta \geqq 2\nu + 1$. Le nombre de solutions du système*

$$\psi_\mu(y_1, \dots, y_s) \equiv 0 \,(mod.\ p^{\beta+1});\ y_\sigma \equiv w_\sigma \,(mod.\ p^{\beta-\nu}). \quad . \quad . \quad (6)$$

$(\mu = 1, \dots, m;\ \sigma = 1, \dots, s)$ possédant la propriété $P(\alpha_1, \dots, \alpha_m)$, est exactement p^{s-m} multiplié par le nombre de solutions du système

$$\psi_\mu(y_1, \dots, y_s) \equiv 0 \,(mod.\ p^\beta);\ y_\sigma \equiv w_\sigma \,(mod.\ p^{\beta-\nu}) \quad . \quad . \quad . \quad (7)$$

avec cette même propriété.

Il découle de cette proposition que le système

$$\psi_\mu(y_1, \dots, y_s) \equiv 0 \,(mod.\ p^{\beta+1}) \qquad (\mu = 1, \dots, m) \quad . \quad . \quad . \quad (8)$$

possède exactement p^{s-m} fois autant de solutions avec la propriété $P(\alpha_1, \dots, \alpha_m)$ que le système (2).

Il est facile de déduire la proposition 1 de la précédente. Il résulte des conditions de la proposition 1 que le système (2) ne possède aucune solution avec la propriété $P(\alpha_1, \dots, \alpha_m)$, si $\beta \geqq 2\gamma + 1$ et $\alpha_m \geqq \gamma + 1$. On a par conséquent

$$Q_\beta = \sum_{\alpha_1, \dots \alpha_m} Q_\beta(\alpha_1, \dots, \alpha_m) \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (9)$$

où $p^{(s-m)\beta} Q_\beta(\alpha_1, \dots, \alpha_m)$ désigne le nombre des solutions de (2) avec la propriété $P(\alpha_1, \dots, \alpha_m)$. On obtient de la même manière

$$Q_{\beta+1} = \sum_{\alpha_1, \dots \alpha_m} Q_{\beta+1}(\alpha_1, \dots, \alpha_m),$$

où $p^{(s-m)(\beta+1)} Q_{\beta+1}(\alpha_1, \dots, \alpha_m)$ désigne le nombre des solutions de (8) avec la propriété $P(\alpha_1, \dots, \alpha_m)$. La proposition 2 nous apprend $Q_{\beta+1}(\alpha_1, \dots, \alpha_m) = Q_\beta(\alpha_1, \dots, \alpha_m)$, par conséquent $Q_{\beta+1} = Q_\beta$, si β est $\geqq 2\gamma + 1$.

Démonstration de la proposition 2.

Soit $y = (y_1, \dots, y_s)$ une solution quelconque de (2) possédant la propriété $P(\alpha_1, \dots, \alpha_m)$. Pour une solution $z = (z_1, \dots, z_s)$ de (2) telle que

$$z_\sigma \equiv y_\sigma \,(mod.\ p^{\beta-\nu}) \qquad (\sigma = 1, \dots, s), \quad . \quad . \quad . \quad . \quad . \quad (10)$$

la différence

$$\psi_{\mu\sigma}(z_1, \dots, z_s) - \psi_{\mu\sigma}(y_1, \dots, y_s)$$

est congrue à zéro, modulo $p^{\beta-\nu}$, donc aussi modulo $p^{\nu+1}$ (en vertu de $\beta - \nu \geqq \nu + 1$), de sorte que, d'après une remarque précédente, les diviseurs élémentaires modulo p de M ne changent pas, si l'on remplace y par z. La

solution z possède donc aussi la propriété $P(\alpha_1, \ldots, \alpha^m)$. Si j'appelle y et z deux solutions équivalentes, cette notion d'équivalence possède par conséquent les propriétés réflexive, symétrique et transitive.

Si y désigne une solution de (2), ayant la propriété $P(\alpha_1, \ldots, \alpha_m)$ et si l'on pose

$$z_\sigma = y_\sigma + g_\sigma\, p^{\beta-\nu} \qquad (\sigma = 1, \ldots, s),$$

où g_σ est entier, on a

$$\psi_\mu(z_1, \ldots, z_s) \equiv \psi_\mu(y_1, \ldots, y_s) + \sum_{\sigma=1}^{s} g_\sigma\, p^{\beta-\nu}\, \psi_{\mu\sigma}(y_1, \ldots, y_s)$$

modulo $p^{2\beta-2\nu}$, donc aussi modulo p^β. On obtient par conséquent

$$\psi_\mu(z_1, \ldots, z_s) \equiv \sum_{\sigma=1}^{s} g_\sigma\, p^{\beta-\nu}\, \psi_{\mu\sigma}(y_1, \ldots, y_s) \,(mod.\ p^\beta).$$

Une condition nécessaire et suffisante pour que z soit une solution de (2) est donc

$$\sum_{\sigma=1}^{s} g_\sigma\, \psi_{\mu\sigma}(y_1, \ldots, y_s) \equiv 0 \ (mod.\ p^\nu).$$

D'après le raisonnement précédent (appliqué avec $\tau = \nu$) le nombre des solutions $g = (g_1, \ldots, g_s)$ de ce système est égal à $p^{(s-m+1)\nu+\omega}$, où $\omega = \alpha_1 + \ldots + \alpha_{m-1}$, de sorte qu'à chaque solution y de (2) avec la propriété $P(\alpha_1, \ldots, \alpha_m)$ correspondent exactement $p^{(s-m+1)\nu+\omega}$ solutions équivalentes, et ces solutions équivalentes possèdent toutes cette même propriété $P(\alpha_1, \ldots, \alpha_m)$. Une classe K de solutions de (7), équivalentes à une solution donnée qui possède la propriété $P(\alpha_1, \ldots, \alpha_m)$, est donc formée par $p^{(s-m+1)\nu+\omega}$ solutions de (7).

Si $u = (u_1, \ldots, u_s)$ est une solution de (8) avec la propriété $P(\alpha_1, \ldots, \alpha_m)$, toute solution $v = (v_1, \ldots, v_s)$ de (8) avec

$$v_\sigma \equiv u_\sigma \ (mod.\ p^{\beta+1-\nu}) \qquad (\sigma = 1, \ldots, s)$$

est dite équivalente à la solution u. Une classe K' de solutions de (6), équivalentes à une solution donnée qui possède la propriété $P(\alpha_1, \ldots, \alpha_m)$, est formée par $p^{(s-m+1)\nu+\omega}$ solutions de (6), d'après le résultat précédent, appliqué avec $\beta + 1$ au lieu de β. Toutes ces solutions de (6) possèdent la propriété $P(\alpha_1, \ldots, \alpha_m)$.

Soit r le nombre des classes différentes K des solutions de (7) qui possèdent la propriété $P(\alpha_1, \ldots, \alpha_m)$ et désignons par t le nombre des classes différentes K' de solutions de (6) qui possèdent cette propriété $P(\alpha_1, \ldots, \alpha_m)$. Comme chacune des classes K contient autant de solutions que chacune des classes K', il suffit de démontrer que t est égal à $p^{s-m}\, r$. Pour obtenir ce résultat je démontrerai qu'à chacune des classes K correspond bi-univoquement un système formé par p^{s-m} classes K'.

Soit K l'une quelconque des classes citées. Un élément arbitraire

$y = (y_1, \ldots, y_s)$ de K est une solution de (7) avec la propriété $P(\alpha_1, \ldots, \alpha_m)$. Si nous posons

$$u_\sigma = y_\sigma + h_\sigma\, p^{\beta-\nu} \qquad (\sigma = 1, \ldots, s), \quad . \quad . \quad . \quad . \quad . \quad (11)$$

nous avons pour $\mu = 1, \ldots, m$

$$\psi_\mu(u_1, \ldots, u_s) \equiv \psi_\mu(y_1, \ldots, y_s) + \sum_{\sigma=1}^{s} h_\sigma\, p^{\beta-\nu}\, \psi_{\mu\sigma}(y_1, \ldots, y_s)$$

modulo $p^{2\beta-2\nu}$, par conséquent aussi modulo $p^{\beta+1}$ en vertu de $\beta \geqq 2\nu + 1$. Une condition nécessaire et suffisante pour que $u = (u_1, \ldots, u_s)$ soit une solution de (6) est donc

$$\sum_{\sigma=1}^{s} h_\sigma\, \psi_{\mu\sigma}(y_1, \ldots, y_s) \equiv -\, p^\nu \cdot \frac{\psi_\mu(y_1, \ldots, y_s)}{p^\beta} \,(mod.\ p^{\nu+1})$$

$(\mu = 1, \ldots, m)$ et, d'après le raisonnement précédent, ce système de congruences possède $p^{(s-m)(\nu+1)+\nu+\omega}$ solutions. De cette manière chaque solution $y = (y_1, \ldots, y_s)$ de K fournit $p^{(s-m)(\nu+1)+\nu+\omega}$ solutions différentes u de (6), et chacune de ces solutions u possède la propriété $P(\alpha_1, \ldots, \alpha_m)$, car $\psi_{\mu\sigma}(u_1, \ldots, u_s) - \psi_{\mu\sigma}(y_1, \ldots, y_s)$ est divisible par $p^{\beta-\nu}$, donc par $p^{\nu+1}$. Deux solutions différentes y et z de (7) appartenant à la même classe K donnent les mêmes solutions de (6), parce que y et z sont équivalents et vérifient donc les congruences (10). La classe K fournit ainsi exactement $p^{(s-m)(\nu+1)+\nu+\omega}$ solutions différentes de (6) qui toutes possèdent la propriété $P(\alpha_1, \ldots, \alpha_m)$.

Si l'on trouve de cette manière une solution u de (6), on obtient aussi chaque solution de (6) qui est équivalente à u, de sorte qu'à la classe K correspondent

$$p^{(s-m)(\nu+1)+\nu+\omega} : p^{(s-m+1)\nu+\omega} = p^{s-m}$$

classes K'. Réciproquement, si une de ces classes K' est donnée, la classe correspondante K est définie univoquement; en effet, une solution quelconque u de (6) appartenant à K', est une solution de (7) ayant la propriété $P(\alpha_1, \ldots, \alpha_m)$ et appartient à une classe K qui est ainsi fixée univoquement. La proposition 2 est donc démontrée.

Le corollaire suivant de cette proposition est utile dans la théorie additive des nombres. Considérons le système de congruences

$$\left.\begin{aligned} &\chi_\mu(h_1, \ldots, h_s) \equiv 0 \,(mod.\ p^\beta) \qquad (\mu = 1, \ldots, m) \\ &h_\sigma \equiv u_\sigma \qquad\qquad (mod.\ U_\sigma) \qquad (\sigma = 1, \ldots, s), \end{aligned}\right\} \quad . \quad . \quad (12)$$

où $\chi_1, \ldots, \chi_m$ désignent des polynômes à coefficients entiers, u_σ et U_σ des entiers donnés; U_σ est supposé positif. Je partagerai les nombres naturels $\sigma \leqq s$ en deux familles (l'une d'elles pouvant être vide) et je supposerai pour tout σ de la première famille que u_σ soit premier avec U_σ.

Désignons par $p^{(s-m)\beta} Q_\beta^*$ le nombre des systèmes $h = (h_1, \ldots, h_s)$ formés par s nombres naturels $h_\sigma \leqq U_\sigma p^\beta$ $(\sigma = 1, \ldots, s)$, qui vérifient le système (12) et remplissent en même temps la condition

$$\prod_\sigma{}' h_\sigma \not\equiv 0 \qquad (mod.\ p), \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (13)$$

où $\prod_\sigma{}'$ est étendu aux σ de la première famille; si la première famille est vide, la dernière condition est automatiquement remplie. Pour étudier ce nombre Q_β^* on peut, comme on le verra dans la proposition suivante, considérer la matrice

$$M^* = \begin{pmatrix} U_1 \chi_{11} & \ldots & U_s \chi_{1s} \\ \ldots & \ldots & \ldots \\ U_1 \chi_{m1} & \ldots & U_s \chi_{ms} \end{pmatrix},$$

où $\chi_{\mu\sigma} = \dfrac{\partial \chi_\mu}{\partial h_\sigma}$.

Proposition 3: *Supposons qu'il existe un entier $\gamma \geqq 0$ tel que le système*

$$\left.\begin{aligned} \chi_\mu (h_1, \ldots, h_s) &\equiv 0 \ (mod.\ p^{2\gamma+1}) \qquad (\mu = 1, \ldots, m) \\ h_\sigma &\equiv u_\sigma \ (mod.\ U_\sigma) \qquad (\sigma = 1, \ldots, s) \end{aligned}\right\} \quad . \quad . \quad (14$$

ne possède aucune solution $h = (h_1, \ldots, h_s)$ avec (13) et avec la propriété que le dernier diviseur élémentaire modulo p de la matrice M^* soit supérieur à p^γ.

Dans ces conditions Q_β^* possède la même valeur pour tout $\beta \geqq 2\gamma + 1$.

Démonstration: Si nous posons

$$\chi_\mu (u_1 + U_1 y_1, \ldots, u_s + U_s y_s) = \psi_\mu (y_1, \ldots, y_s),$$

$p^{(s-m)\beta} Q_\beta^*$ désigne le nombre des solutions du système

$$\psi_\mu (y_1, \ldots, y_s) \equiv 0 \ (mod.\ p^\beta) \qquad (\mu = 1, \ldots, m), \quad . \quad . \quad . \quad (15)$$

telles qu'on ait pour tout σ de la première famille

$$u_\sigma + U_\sigma y_\sigma \not\equiv 0 \qquad (mod.\ p). \quad . \quad . \quad . \quad . \quad . \quad . \quad (16)$$

Pour un σ de la première famille pour lequel U_σ est divisible par p, le nombre u_σ est premier avec U_σ, donc n'est pas divisible par p; pour un tel σ la congruence (16) est vérifiée d'elle même. Pour un σ de la première famille tel que U_σ ne soit pas divisible par p, il existe un seul nombre naturel $z_\sigma \leqq p$ avec la propriété que $u_\sigma + U_\sigma z_\sigma$ est divisible

par p. Par conséquent $p^{(s-m)\beta} Q_\beta^*$ est le nombre des solutions de (15) telles qu'on ait

$$y_\sigma \not\equiv z_\sigma \qquad (mod.\ p). \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (17)$$

pour tout σ de la première famille avec $U_\sigma \not\equiv 0$ $(mod.\ p)$.

Supposons maintenant $\beta \geqq 2\gamma + 1$. Si une solution quelconque de (15) et (17) possède la propriété $P(\alpha_1, \ldots, \alpha_m)$, le nombre α_m est nécessairement $\leqq \gamma$. En effet, si α_m était $\geqq \gamma + 1$, le système $h = (h_1, \ldots, h_s)$ défini par

$$h_\sigma = u_\sigma + U_\sigma y_\sigma \qquad (\sigma = 1, \ldots, s)$$

serait une solution de (14) avec (13), telle que le dernier diviseur élémentaire modulo p de la matrice M^* serait supérieur à p^γ. On a donc

$$Q_\beta^* = \sum_{\alpha_1, \ldots, \alpha_m} Q_\beta (\alpha_1, \ldots, \alpha_m),$$

où $p^{(s-m)\beta} Q_\beta (\alpha_1, \ldots, \alpha_m)$ désigne le nombre des solutions de (15) et (17) possédant la propriété $P(\alpha_1, \ldots, \alpha_m)$. De la même manière on obtient

$$Q_{\beta+1}^* = \sum_{\alpha_1, \ldots \alpha_m} Q_{\beta+1} (\alpha_1, \ldots, \alpha_m)$$

où $p^{(s-m)(\beta+1)} Q_{\beta+1} (\alpha_1, \ldots, \alpha_m)$ désigne le nombre des solutions de (17) et

$$\psi_\mu (y_1, \ldots, y_m) \equiv 0 \ (mod.\ p^{\beta+1})$$

qui possèdent la propriété $P(\alpha_1, \ldots, \alpha_m)$. La proposition 2 nous apprend que $Q_\beta (\alpha_1, \ldots, \alpha_n)$ et $Q_{\beta+1} (\alpha_1, \ldots, \alpha_m)$, donc aussi Q_β^* et $Q_{\beta+1}^*$ possèdent les mêmes valeurs, si β est $\geqq 2\gamma + 1$.