ANNALES SCIENTIFIQUES DE L'É.N.S.

GUSTAVE RADOS

Sur une théorie des congruences à plusieurs variables

Annales scientifiques de l'É.N.S. 3^e série, tome 27 (1910), p. 217-231

<http://www.numdam.org/item?id=ASENS_1910_3_27__217_0>

SUR UNE

THÉORIE DES CONGRUENCES

A

PLUSIEURS VARIABLES,

PAR M. GUSTAVE RADOS.

Dans ce travail, je me propose d'établir une série de théorèmes relatifs aux congruences de degré supérieur à 1 et ayant pour module un nombre premier. Ces théorèmes contribueront à poser les fondements de la théorie des congruences à plusieurs variables, congruences très peu étudiées jusqu'ici. Leur importance a été caractérisée par M. Poincaré, dans sa conférence sur l'*Avenir des Mathématiques* (1), en ces termes : « Quand les problèmes relatifs aux congruences à plusieurs variables seront résolus, ce sera un premier pas vers la solution de beaucoup de questions d'analyse indéterminée ». Ce sont ces paroles de M. Poincaré qui m'ont décidé à publier mes recherches à ce sujet.

Pour simplifier, je me bornerai à ne considérer que des congruences à deux inconnues. L'étude des congruences à plus de deux inconnues peut se faire par la même voie, quoique naturellement non sans quelque longueur.

Les congruences à deux variables, ayant pour module le nombre premier p, s'écrivent sous la forme

$$F(x,y)\equiv\sum_{i=0}^{m}\sum_{k=0}^{n}A_i^{(k)}x^{m-i}y^{n-k}\equiv 0 \qquad (\mathrm{mod}\,p).$$

(1) *Atti del IV° Congresso internazionale dei Matematici*, p. 175.

Le problème consiste à déterminer tous les systèmes de valeurs

$$x_\alpha, \quad y_\beta$$

pour lesquels

$$F(x_\alpha, y_\beta) \equiv 0 \pmod{p}.$$

La première question qui se pose, c'est celle de l'existence des solutions; la seconde, c'est la détermination de leur nombre au cas où elles existent. Peut-on former des critères qui permettent de répondre à ces questions?

En suivant la voie qui s'offre immédiatement, calculons toutes les valeurs

$$F(x_\alpha, y_\beta)$$
$$(x_\alpha, y_\beta = 0, 1, 2, \ldots, p-1),$$

pour chacune desquelles nous essayerons la division par p. Si aucune d'entre elles n'est divisible par p, notre congruence n'a pas de solution réelle; si, au contraire, nous pouvons en trouver r divisibles par p, la congruence aura exactement r solutions différentes. On voit que, par ce procédé primitif, le nombre des essais sera en général égal à p^2.

Tous les problèmes de la théorie des nombres ont le trait caractéristique qu'un certain élément expérimental entre dans leurs solutions et que cet élément ne s'élimine jamais complètement. On s'efforce de développer des méthodes propres à réduire les essais au nombre minimum.

Les théorèmes démontrés dans ce travail vont servir à ce but. En effet, grâce à ces théorèmes, on verra que, *pour décider de l'existence des solutions de la congruence*

$$F(x, y) \equiv 0 \pmod{p},$$

il n'y a à faire qu'un seul essai, c'est-à-dire que les essais, au nombre de p^2, dont nous avons parlé plus haut, peuvent se réduire à un seul qu'il faut effectuer sur une expression formée uniquement des coefficients de la congruence.

I. — Formes normales de la congruence et énoncé des théorèmes.

Parmi toutes les solutions de la congruence

$$F(x, y) \equiv 0 \pmod{p},$$

considérons d'abord celles dans lesquelles ni x, ni y n'est divisible par p. Nous les appellerons les *solutions non nulles*. S'il s'agit d'une telle solution, nous pouvons dans le polynome $F(x,y)$ éliminer les puissances de x et y de degré supérieur à $p-2$ moyennant les congruences (conséquences du théorème de Fermat)

$$x^{g(p-1)+h} \equiv x^h, \qquad y^{g(p-1)+h} \equiv y^h \qquad (\mathrm{mod}\, p)$$
$$(h < p-1).$$

Cela étant, notre congruence prend la forme normale

$$(1^*) \quad F^*(x,y) \equiv \sum_{k=0}^{p-2} (a_0^{(k)} x^{p-2} + a_1^{(k)} x^{p-3} + \ldots + a_{p-2}^{(k)}) y^{p-k-2} \equiv 0 \qquad (\mathrm{mod}\, p).$$

Formons maintenant des coefficients $a_i^{(k)}$ les matrices

$$A_k = \begin{pmatrix} a_0^{(k)} & a_1^{(k)} & \ldots & a_{p-3}^{(k)} & a_{p-2}^{(k)} \\ a_1^{(k)} & a_2^{(k)} & \ldots & a_{p-2}^{(k)} & a_0^{(k)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{p-2}^{(k)} & a_0^{(k)} & \ldots & a_{p-4}^{(k)} & a_{p-3}^{(k)} \end{pmatrix};$$

nous pouvons alors, relativement aux solutions non nulles, énoncer les théorèmes suivants :

THÉORÈME I. — *La condition nécessaire et suffisante pour que la congruence*

$$F^*(x, y) \equiv 0 \qquad (\mathrm{mod}\, p)$$

admette une solution non nulle, est que le déterminant de degré $(p-1)^2$

$$C_{F^*} = \begin{vmatrix} A_0 & A_1 & \ldots & A_{p-3} & A_{p-2} \\ A_1 & A_2 & \ldots & A_{p-2} & A_0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ A_{p-2} & A_0 & \ldots & A_{p-4} & A_{p-3} \end{vmatrix},$$

soit congru à zéro par rapport au module p.

THÉORÈME II. — *Pour que la congruence ait exactement r solutions non nulles différentes, il est nécessaire et suffisant que le déterminant* C_F. *soit*

de rang $(p-1)^2-r$. [Nous entendons par cela que, parmi les mineurs de degré $(p-1)^2-r$, il y en a un au moins différent de zéro, tous les mineurs de degré supérieur étant nuls.]

Pour plus de clarté, nous écrirons explicitement, au cas de $p=5$, le déterminant C_{F^*} de degré 16.

$$\begin{vmatrix}
a_0^{(0)} & a_1^{(0)} & a_2^{(0)} & a_3^{(0)} & a_0^{(1)} & a_1^{(1)} & a_2^{(1)} & a_3^{(1)} & a_0^{(2)} & a_1^{(2)} & a_2^{(2)} & a_3^{(2)} & a_0^{(3)} & a_1^{(3)} & a_2^{(3)} & a_3^{(3)} \\
a_1^{(0)} & a_2^{(0)} & a_3^{(0)} & a_0^{(0)} & a_1^{(1)} & a_2^{(1)} & a_3^{(1)} & a_0^{(1)} & a_1^{(2)} & a_2^{(2)} & a_3^{(2)} & a_0^{(2)} & a_1^{(3)} & a_2^{(3)} & a_3^{(3)} & a_0^{(3)} \\
a_2^{(0)} & a_3^{(0)} & a_0^{(0)} & a_1^{(0)} & a_2^{(1)} & a_3^{(1)} & a_0^{(1)} & a_1^{(1)} & a_2^{(2)} & a_3^{(2)} & a_0^{(2)} & a_1^{(2)} & a_2^{(3)} & a_3^{(3)} & a_0^{(3)} & a_1^{(3)} \\
a_3^{(0)} & a_0^{(0)} & a_1^{(0)} & a_2^{(0)} & a_3^{(1)} & a_0^{(1)} & a_1^{(1)} & a_2^{(1)} & a_3^{(2)} & a_0^{(2)} & a_1^{(2)} & a_2^{(2)} & a_3^{(3)} & a_0^{(3)} & a_1^{(3)} & a_2^{(3)} \\
a_0^{(1)} & a_1^{(1)} & a_2^{(1)} & a_3^{(1)} & a_0^{(2)} & a_1^{(2)} & a_2^{(2)} & a_3^{(2)} & a_0^{(3)} & a_1^{(3)} & a_2^{(3)} & a_3^{(3)} & a_0^{(0)} & a_1^{(0)} & a_2^{(0)} & a_3^{(0)} \\
a_1^{(1)} & a_2^{(1)} & a_3^{(1)} & a_0^{(1)} & a_1^{(2)} & a_2^{(2)} & a_3^{(2)} & a_0^{(2)} & a_1^{(3)} & a_2^{(3)} & a_3^{(3)} & a_0^{(3)} & a_1^{(0)} & a_2^{(0)} & a_3^{(0)} & a_0^{(0)} \\
a_2^{(1)} & a_3^{(1)} & a_0^{(1)} & a_1^{(1)} & a_2^{(2)} & a_3^{(2)} & a_0^{(2)} & a_1^{(2)} & a_2^{(3)} & a_3^{(3)} & a_0^{(3)} & a_1^{(3)} & a_2^{(0)} & a_3^{(0)} & a_0^{(0)} & a_1^{(0)} \\
a_3^{(1)} & a_0^{(1)} & a_1^{(1)} & a_2^{(1)} & a_3^{(2)} & a_0^{(2)} & a_1^{(2)} & a_2^{(2)} & a_3^{(3)} & a_0^{(3)} & a_1^{(3)} & a_2^{(3)} & a_3^{(0)} & a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\
a_0^{(2)} & a_1^{(2)} & a_2^{(2)} & a_3^{(2)} & a_0^{(3)} & a_1^{(3)} & a_2^{(3)} & a^{(3)} & a^{(0)} & a^{(0)} & a^{(0)} & a^{(0)} & a^{(1)} & a^{(1)} & a_2^{(1)} & a_3^{(1)} \\
a_1^{(2)} & a_2^{(2)} & a_3^{(2)} & a_0^{(2)} & a_1^{(3)} & a_2^{(3)} & a_3^{(3)} & a_0^{(3)} & a_1^{(0)} & a_2^{(0)} & a_3^{(0)} & a_0^{(0)} & a_1^{(1)} & a_2^{(1)} & a_3^{(1)} & a_0^{(1)} \\
a_2^{(2)} & a_3^{(2)} & a_0^{(2)} & a_1^{(2)} & a_2^{(3)} & a_3^{(3)} & a_0^{(3)} & a_1^{(3)} & a_2^{(0)} & a_3^{(0)} & a_0^{(0)} & a_1^{(0)} & a_2^{(1)} & a_3^{(1)} & a_0^{(1)} & a_1^{(1)} \\
a_3^{(2)} & a_0^{(2)} & a_1^{(2)} & a_2^{(2)} & a_3^{(3)} & a_0^{(3)} & a_1^{(3)} & a_2^{(3)} & a_3^{(0)} & a_0^{(0)} & a_1^{(0)} & a_2^{(0)} & a_3^{(1)} & a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\
a_0^{(3)} & a_1^{(3)} & a_2^{(3)} & a_3^{(3)} & a_0^{(0)} & a_1^{(0)} & a_2^{(0)} & a_3^{(0)} & a_0^{(1)} & a_1^{(1)} & a_2^{(1)} & a_3^{(1)} & a_0^{(2)} & a_1^{(2)} & a_2^{(2)} & a_3^{(2)} \\
a_1^{(3)} & a_2^{(3)} & a_3^{(3)} & a_0^{(3)} & a_1^{(0)} & a_2^{(0)} & a_3^{(0)} & a_0^{(0)} & a_1^{(1)} & a_2^{(1)} & a_3^{(1)} & a_0^{(1)} & a_1^{(2)} & a_2^{(2)} & a_3^{(2)} & a_0^{(2)} \\
a_2^{(3)} & a_3^{(3)} & a_0^{(3)} & a_1^{(3)} & a_2^{(0)} & a_3^{(0)} & a_0^{(0)} & a_1^{(0)} & a_2^{(1)} & a_3^{(1)} & a_0^{(1)} & a_1^{(1)} & a_2^{(2)} & a_3^{(2)} & a_0^{(2)} & a_1^{(2)} \\
a_3^{(3)} & a_0^{(3)} & a_1^{(3)} & a_2^{(3)} & a_3^{(0)} & a_0^{(0)} & a_1^{(0)} & a_2^{(0)} & a_3^{(1)} & a_0^{(1)} & a_1^{(1)} & a_2^{(1)} & a_3^{(2)} & a_0^{(2)} & a_1^{(2)} & a_2^{(2)}
\end{vmatrix}$$

Si nous considérons toutes les solutions nulles ou non de la congruence, il faut remplacer les théorèmes I et II par deux théorèmes nouveaux. Dans ce cas, la forme normale elle-même est différente. Cela tient à ce qu'il faut appliquer cette fois le théorème de Fermat sous la forme générale

$$x^{gp+h}\equiv x^h, \qquad y^{gp+h}\equiv y^h \qquad (\mathrm{mod}\,p).$$

En éliminant maintenant les puissances de x et de y de degré supérieur à $p-1$, la congruence s'écrit finalement sous la forme normale

$$(1^{**}) \quad F^{**}(x,y)\equiv\sum_{k=0}^{p-1}(a_0^{(k)}x^{p-1}+a_1^{(k)}x^{p-2}+\ldots+a_{p-1}^{(k)})y^{p-k-1}\equiv 0 \qquad (\mathrm{mod}\,p).$$

Formons les matrices

$$A_k = \begin{pmatrix} a_0^{(k)} & a_1^{(k)} & \dots & a_{p-3}^{(k)} & a_{p-2}^{(k)} & a_{p-1}^{(k)} \\ a_1^{(k)} & a_2^{(k)} & \dots & a_{p-2}^{(k)} & a_{p-1}^{(k)} + a_0^{(k)} & 0 \\ a_2^{(k)} & a_3^{(k)} & \dots & a_{p-1}^{(k)} + a_0^{(k)} & a_1^{(k)} & 0 \\ \dots & \dots & \dots & \dots\dots\dots & \dots & . \\ a_{p-1}^{(k)} + a_0^{(k)} & a_1^{(k)} & \dots & a_{p-3}^{(k)} & a_{p-2}^{(k)} & 0 \end{pmatrix}$$

$$(k = 0, 1, 2, \dots, p-1)$$

et de ces matrices le déterminant de degré p^2

$$\Gamma_{F^{**}} = \begin{vmatrix} A_0 & A_1 & \dots & A_{p-3} & A_{p-2} & A_{p-1} \\ A_1 & A_2 & \dots & A_{p-2} & A_{p-1} + A_0 & (0) \\ A_3 & A_4 & \dots & A_{p-1} + A_0 & A_1 & (0) \\ .. & .. & \dots & \dots\dots\dots & .. & \dots \\ A_{p-1} + A_0 & A_1 & \dots & A_{p-3} & A_{p-2} & (0) \end{vmatrix},$$

où la notation symbolique $A_{p-1} + A_0$ désigne la matrice

$$= \begin{pmatrix} a_0^{(p-1)} + a_0^{(0)} & a_1^{(p-1)} + a_1^{(0)} & \dots & a_{p-2}^{(p-1)} + a_{p-2}^{(0)} & a_{p-1}^{(p-1)} \\ a_1^{(p-1)} + a_1^{(0)} & a_2^{(p-1)} + a_2^{(0)} & \dots & a_{p-1}^{(p-1)} + a_{p-1}^{(0)} + a_0^{(p-1)} + a_0^{(0)} & \\ \dots\dots\dots & \dots\dots\dots & \dots & \dots\dots\dots\dots\dots & \\ a_{p-1}^{(p-1)} + a_{p-1}^{(0)} + a_0^{(p-1)} + a_0^{(0)} & a_1^{(p-1)} + a_1^{(0)} & \dots & a_{p-2}^{(p-1)} + a_{p-2}^{(0)} & \end{pmatrix}$$

et (o) la matrice à p lignes et p colonnes

$$(0) = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ . & . & \dots & . \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Cela posé, nous pouvons énoncer deux théorèmes qui se rapportent à la totalité des solutions de la congruence 1^{**}.

THÉORÈME III. — *La condition nécessaire et suffisante pour que la congruence* (1^{**}) *ait au moins une solution réelle est que le déterminant* $\Gamma_{F^{**}}$ *soit congru à zéro* (mod p).

THÉORÈME IV. — *Pour que la congruence ait r solutions différentes, il faut et il suffit que le déterminant* $\Gamma_{F^{**}}$ *soit de rang* $p^2 - r$.

II. — Calcul du déterminant $\Delta^{(k)}_{(x,y)}$.

Dans ce qui va suivre, nous aurons l'occasion à plusieurs reprises d'utiliser un déterminant compliqué ; commençons par le calculer afin de ne pas interrompre plus tard les raisonnements. Ce déterminant, que nous désignerons par $\Delta^{(k)}_{x,y}$ s'écrit

$$\begin{vmatrix}
x_0^{k-1}y_0^{k-1} & x_0^{k-2}y_0^{k-1} & \dots & y_0^{k-1} & x_0^{k-1}y_0^{k-2} & x_0^{k-2}y_0^{k-2} & \dots & y_0^{k-2} & \dots & x_0^{k-1} & x_0^{k-2} & \dots \\
x_0^{k-1}y_1^{k-1} & x_0^{k-2}y_1^{k-1} & \dots & y_1^{k-1} & x_0^{k-1}y_0^{k-2} & x_0^{k-2}y_1^{k-2} & \dots & y_1^{k-2} & \dots & x_0^{k-1} & x_0^{k-2} & \dots \\
\dots\dots & \dots\dots & \dots & \dots & \dots\dots & \dots\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
x_0^{k-1}y_{k-1}^{k-1} & x_0^{k-2}y_{k-1}^{k-1} & \dots & y_{k-1}^{k-1} & x_0^{k-1}y_{k-1}^{k-2} & x_0^{k-2}y_{k-1}^{k-2} & \dots & y_{k-1}^{k-2} & \dots & x_0^{k-1} & x_0^{k-2} & \dots \\
x_1^{k-1}y_0^{k-1} & x_1^{k-2}y_0^{k-1} & \dots & y_0^{k-1} & x_1^{k-1}y_0^{k-2} & x_1^{k-2}y_0^{k-2} & \dots & y_0^{k-2} & \dots & x_1^{k-1} & x_1^{k-2} & \dots \\
x_1^{k-1}y_1^{k-1} & x_1^{k-2}y_1^{k-1} & \dots & y_1^{k-1} & x_1^{k-1}y_1^{k-2} & x_1^{k-2}y_1^{k-2} & \dots & y_1^{k-2} & \dots & x_1^{k-1} & x_1^{k-2} & \dots \\
\dots\dots & \dots\dots & \dots & \dots & \dots\dots & \dots\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
x_1^{k-1}y_{k-1}^{k-1} & x_1^{k-2}y_{k-1}^{k-1} & \dots & y_{k-1}^{k-1} & x_1^{k-1}y_{k-1}^{k-2} & x_1^{k-2}y_{k-1}^{k-2} & \dots & y_{k-1}^{k-2} & \dots & x_1^{k-1} & x_1^{k-2} & \dots \\
\dots\dots & \dots\dots & \dots & \dots & \dots\dots & \dots\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
x_{k-1}^{k-1}y_0^{k-1} & x_{k-1}^{k-2}y_0^{k-1} & \dots & y_0^{k-1} & x_{k-1}^{k-1}y_0^{k-2} & x_{k-1}^{k-2}y_0^{k-2} & \dots & y_0^{k-2} & \dots & x_{k-1}^{k-1} & x_{k-1}^{k-2} & \dots \\
x_{k-1}^{k-1}y_1^{k-1} & x_{k-1}^{k-2}y_1^{k-1} & \dots & y_1^{k-1} & x_{k-1}^{k-1}y_1^{k-2} & x_{k-1}^{k-2}y_1^{k-2} & \dots & y_1^{k-2} & \dots & x_{k-1}^{k-1} & x_{k-1}^{k-2} & \dots \\
\dots\dots & \dots\dots & \dots & \dots & \dots\dots & \dots\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
x_{k-1}^{k-1}y_{k-1}^{k-1} & x_{k-1}^{k-2}y_{k-1}^{k-1} & \dots & y_{k-1}^{k-1} & x_{k-1}^{k-1}y_{k-1}^{k-2} & x_{k-1}^{k-2}y_{k-1}^{k-2} & \dots & y_{k-1}^{k-2} & \dots & x_{k-1}^{k-1} & x_{k-1}^{k-2} & \dots
\end{vmatrix}$$

On obtient ce déterminant (¹) de degré k^2 en partant des deux déterminants

$$\Delta^{(k)}_x = \begin{vmatrix}
x_0^{k-1} & x_0^{k-2} & \dots & 1 \\
x_1^{k-1} & x_1^{k-2} & \dots & 1 \\
\dots\dots & \dots\dots & \dots & \cdot \\
x_{k-1}^{k-1} & x_{k-1}^{k-2} & \dots & 1
\end{vmatrix}$$

(¹) Remarquons qu'on peut mettre la loi de formation des éléments du déterminant $\Delta^{(k)}_{x,y}$ sous la forme suivante

$$\Delta^{(k)}_{x,y} = |\, t_{\alpha\beta} \,|$$

$$(\alpha, \beta = 0, 1, 2, \dots, k^2 - 1),$$

où

$$t_{\alpha\beta} = x_{\alpha'}^{k-1-\beta''} y_{\alpha''}^{k-1-\beta'},$$

en désignant par α' et β' les quotients et par α'', β'' les restes des divisions de α et β par k. On a donc

$$\alpha = k\alpha' + \alpha'' \qquad (\alpha'' < k),$$

$$\beta = k\beta' + \beta'' \qquad (\beta'' < k).$$

et

$$\Delta_y^{(k)} = \begin{vmatrix} y_0^{k-1} & y_0^{k-2} & \dots & 1 \\ y_1^{k-1} & y_1^{k-2} & \dots & 1 \\ \dots & \dots & \dots & \cdot \\ y_{k-1}^{k-1} & y_{k-1}^{k-2} & \dots & 1 \end{vmatrix},$$

par un certain procédé de composition que j'ai étudié dans mon travail *Sur la Théorie des déterminants* (paru en hongrois sous le titre : *A determinànsok elméletéhez*) (1). En appliquant au cas qui nous occupe le théorème démontré en cet endroit, nous voyons que

$$\Delta_{x,y}^{(k)} = (\Delta_x^{(k)})^k (\Delta_y^{(k)})^k = \prod (x_i - x_j)^k (y_i - y_j)^k$$
$$(i < j;\ i, j = 0, 1, 2, \dots, k-1).$$

Ceci nous montre que $\Delta_{x,y}^{(k)}$ ne peut être égal à zéro ou congru à zéro mod p que s'il existe dans la suite

$$x_0,\ x_1,\ \dots,\ x_{k-1}$$

ou dans la suite

$$y_0,\ y_1,\ \dots,\ y_{k-1}$$

deux valeurs égales ou deux valeurs congrues (mod p).

III. — Démonstration des théorèmes I et II.

Revenons maintenant à la recherche des conditions nécessaires et suffisantes pour que la congruence (1*) admette une solution non nulle.

Supposons qu'une solution non nulle existe. Dans ce cas, aucune des deux inconnues n'étant congrue à zéro (mod p), on peut, par l'application répétée des relations

$$x^{g(p-1)+h} \equiv x^h, \qquad y^{g(p-1)+h} \equiv y^h \qquad (\text{mod } p)$$

(conséquences directes du théorème de Fermat), déduire, de la con-

(1) *Math. es Term. Ertesitö*, t. IV, 1886, p. 268; *voir* aussi HENSEL, *Ueber die Darstellung der Determinante eines Systems, welches aus zwei anderen komponirt ist* (*Acta mathematica*, t. XV, 1889, p. 317).

gruence (1*), les $(p-1)^2$ congruences simultanées

$$F^\star \equiv \sum_{k=0}^{p-2} (a_0^{(k)} x^{p-2} + a_1^{(k)} x^{p-3} + \ldots + a_{p-3}^{(k)} x + a_{p-2}^{(k)}) y^{p-k-2} \equiv 0,$$

$$xF^\star \equiv \sum_{k=0}^{p-2} (a_1^{(k)} x^{p-2} + a_2^{(k)} x^{p-3} + \ldots + a_{p-2}^{(k)} x + a_0^{(k)}) y^{p-k-2} \equiv 0,$$

. . . .

$$x^{p-2}F^\star \equiv \sum_{k=0}^{p-2} (a_{p-2}^{(k)} x^{p-2} + a_0^{(k)} x^{p-3} + \ldots + a_{p-4}^{(k)} x + a_{p-3}^{(k)}) y^{p-k-2} \equiv 0,$$

$$yF^\star \equiv \sum_{k=0}^{p-2} (a_0^{(k+1)} x^{p-2} + a_1^{(k+1)} x^{p-3} + \ldots + a_{p-3}^{(k+1)} x + a_{p-2}^{(k+1)}) y^{p-k-2} \equiv 0,$$

$$xyF^\star \equiv \sum_{k=0}^{p-2} (a_1^{(k+1)} x^{p-2} + a_2^{(k+1)} x^{p-3} + \ldots + a_{p-2}^{(k+1)} x + a_0^{(k+1)}) y^{p-k-2} \equiv 0,$$

. . . .

$$x^{p-2}yF^\star \equiv \sum_{k=0}^{p-2} (a_{p-2}^{(k+1)} x^{p-2} + a_0^{(k+1)} x^{p-3} + \ldots + a_{p-4}^{(k-1)} x + a_{p+3}^{(k+1)}) y^{p-k-2} \equiv 0,$$

. . . .

$$y^{p-2}F^\star \equiv \sum_{k=0}^{p-2} (a_0^{(k+p-2)} x^{p-2} + a_1^{(k+p-2)} x^{p-3} + \ldots + a_{p-3}^{(k+p-2)} x + a_{p-2}^{(k+p-2)}) y^{p-k-2} \equiv 0,$$

$$xy^{p-2}F^\star \equiv \sum_{k=0}^{p-2} (a_1^{(k+p-2)} x^{p-3} + x_2^{(k+p-2)} x^{p-3} + \ldots + a_{p-2}^{(k+p-2)} x + a_0^{(k+p-2)}) y^{p-k-2} \equiv 0,$$

. . . .

$$x^{p-2}y^{p-2}F^\star \equiv \sum_{k=0}^{p-2} (a_{p-2}^{(k+p-2)} x^{p-2} + a_0^{(k+p-2)} x^{p-3} + \ldots + a_{p-4}^{(k+p-2)} x + a_{p-3}^{(k+p-2)}) y^{p-k-2} \equiv 0$$

$$(\operatorname{mod} p)$$

où chaque fois que

$$s > p-2$$

il faut remplacer les coefficients

$$a_0^{(s)},\quad a_1^{(s)},\quad \ldots,\quad a_{p-2}^{(s)}$$

par

$$a_0^{(s-p+1)},\quad a_1^{(s-p+1)},\quad \ldots,\quad a_{p-2}^{(s-p+1)}.$$

Les congruences (K) forment un système de $(p-1)^2$ congruences linéaires et homogènes par rapport aux produits

$$x^\alpha y^\beta$$
$$(\alpha, \beta = 0, 1, 2, \ldots, p-2)$$

qui sont également au nombre de $(p-1)^2$. Ce système admet une solution dans laquelle toutes les inconnues ne sont pas congrues à zéro $(\mathrm{mod}\, p)$; donc son déterminant, qui n'est autre que le déterminant C_{F^*} considéré au n° 1, est nul $(\mathrm{mod}\, p)$.

En résumé, si la congruence

$$(1^*) \qquad F^*(x, y) \equiv 0 \qquad (\mathrm{mod}\, p)$$

est vérifiée par deux valeurs x et y différentes de zéro $(\mathrm{mod}\, p)$, nous avons

$$C_{F^*} \equiv 0 \qquad (\mathrm{mod}\, p).$$

En d'autres termes, la divisibilité par p de la valeur de C_{F^*} *est une condition nécessaire de l'existence d'une solution non nulle.*

Le caractère suffisant de la condition précédente sera établi par les considérations suivantes. La congruence (1^*) n'est résoluble que si une au moins des valeurs

$$F^*(g, h)$$
$$(g, h = 1, 2, \ldots, p-1)$$

est congrue à zéro ou bien, puisque le module p est un nombre premier, si

$$P = \prod_{g=1}^{p-1} \prod_{h=1}^{p-1} F^*(g, h) \equiv 0 \qquad (\mathrm{mod}\, p).$$

Nous aurons démontré que la condition nécessaire trouvée est en même temps suffisante si nous faisons voir que la congruence

$$P \equiv C_{F^*} \qquad (\mathrm{mod}\, p)$$

a lieu. C'est ce que nous allons faire. Soient

$$(M_1) \qquad x_0, \quad x_1, \quad \ldots, \quad x_{p-1}$$

et

$$(M_2) \qquad y_0, \quad y_1, \quad \ldots, \quad y_{p-1},$$

deux permutations quelconques du système des restes

$$1, \quad 2, \quad \ldots, \quad p-1,$$

et formons le déterminant

$$\Delta_{x,y}^{(p-1)} = |t_{\alpha\beta}| \qquad [\alpha, \beta = 0, 1, \ldots, (p-1)^2 - 1],$$

où

$$t_{\alpha\beta} = x_{\alpha'}^{p-2-\beta''} y_{\alpha''}^{p-2-\beta'},$$

en désignant par α', β' les quotients et par α'', β'' les restes des divisions de α et β par $p-1$. Puisqu'on ne peut trouver dans aucune des permutations (M_1) et (M_2) des valeurs congrues, nous pouvons affirmer, en vertu de la remarque faite à la fin du numéro précédent, que $\Delta_{x,y}^{(p-1)}$ n'est pas divisible par p ou en d'autres termes que

$$\Delta_{x,y}^{(p-1)} \not\equiv 0 \pmod{p}.$$

Calculons maintenant le produit des déterminants C_{F^*} et $\Delta_{x,y}^{(p-1)}$ en les composant ligne par ligne et faisons usage des congruences

$$\sum_{k=0}^{p-2} (a_i^{(k+j)} x_\rho^{p-2} + a_{i+1}^{(k+j)} x_\rho^{p-3} + \ldots + a_{i+p-2}^{(k+j)}) y_\sigma^{p-k-2} \equiv x_\rho^i y_\sigma^j F(x_\rho, y_\sigma) \pmod{p}$$

$$(i, j, \rho, \sigma = 0, 1, 2, \ldots, p-2),$$

où il faut substituer

$$a_{u-(p-2)}^{v-(p-2)} \quad \text{à} \quad a_u^v$$

chaque fois que

$$u > p-2, \qquad v > p-2.$$

Notre produit s'écrit alors

$$\equiv \begin{vmatrix} F^*(x_0, y_0) & \ldots & x_0^{p-2} F^*(x_0, y_0) & \ldots & y_0^{p-2} F^*(x_0, y_0) & \ldots & x_0^{p-2} y_0^{p-2} F^*(x_0, y_0) \\ F^*(x_0, y_1) & \ldots & x_0^{p-2} F^*(x_0, y_1) & \ldots & y_1^{p-2} F^*(x_0, y_1) & \ldots & x_0^{p-2} y_1^{p-2} F^*(x_0, y_1) \\ \ldots\ldots\ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots & \ldots\ldots\ldots\ldots\ldots \\ F^*(x_{p-2}, y_{p-2}) & \ldots & x_{p-2}^{p-2} F^*(x_{p-2}, y_{p-2}) & \ldots & y_{p-1}^{p-2} F^*(x_{p-2}, y_{p-2}) & \ldots & x_{p-2}^{p-2} y_{p-2}^{p-2} F^*(x_{p-2}, y_{p-2}) \end{vmatrix}$$

$$\pmod{p},$$

ou sous une forme abrégée

$$C_{F^*}\,\Delta_{x,y}^{(p-1)} \equiv (-1)^{\frac{(p-1)^2[(p-1)^2-1]}{2}}\,\Delta_{x,y}^{(p-1)}\prod_{i=0}^{p-2}\prod_{k=0}^{p-2}F^*(x_i, y_k) \qquad (\mathrm{mod}\,p);$$

or

$$\Delta_{x,y}^{(p-1)} \not\equiv 0 \qquad (\mathrm{mod}\,p)$$

et

$$\frac{(p-1)^2[(p-1)-1]}{2}$$

est un nombre toujours pair; donc

$$\prod_{i=0}^{p-2}\prod_{k=0}^{p-2}F^*(x_i, y_k) \equiv C_{F^*} \qquad (\mathrm{mod}\,p),$$

ou, ce qui revient au même,

$$P \equiv \prod_{g=1}^{p-1}\prod_{h=1}^{p-1}F^*(g, h) \equiv C_{F^*} \qquad (\mathrm{mod}\,p),$$

ce qui prouve que *la divisibilité du déterminant* C_{F^*} *par* p *est une condition suffisante pour que la congruence admette au moins une solution non nulle.*

Nous aurions maintenant à nous occuper de la relation entre le nombre des solutions non nulles et le rang (par rapport au module p) du déterminant C_{F^*}. C'est cette relation que nous donne en effet le théorème II; la démonstration peut se faire, *mutatis mutandis*, par la même voie que j'ai suivie dans mon travail (1) : *Sur la théorie des congruences non linéaires* (*A felsöbbrendü kongruenczìàk elméletéhez*, en hongrois) pour démontrer le théorème analogue relatif aux congruences à une variable. Qu'il me soit permis de renvoyer le lecteur aux endroits cités.

---

(1) *Math. ès Term. Ertesitö*, t. I, p. 296, et *Journal für die reine und angewandte Mathematik*, t. 99, p. 258; *voir* aussi KRONECKER, *Ueber einige Anwendungen der Modulsysteme auf elementare algebraische Fragen* (le même journal, t. 99, p. 329), et Léopold KRONECKER, *Vorlesungen über Mathematik*, t. II, p. 389-415.

IV. — Démonstration des théorèmes III et IV.

Si nous considérons sans distinction toutes les solutions de la congruence, les conclusions du numéro précédent ne sont plus applicables puisque nous avons exclu les solutions dans lesquelles une ou deux des inconnues avaient la valeur nulle $(\mathrm{mod}\, p)$.

Cette fois, comme nous ne faisons aucune hypothèse sur les valeurs x et y, la congruence se mettra sous la forme normale

$$(1^{**}) \quad F^{**}(x,y) \equiv \sum_{k=0}^{p-1} (a_0^{(k)} x^{p-1} + a_1^{(k)} x^{p-2} + \ldots + a_{p-2}^{(k)} x + a_{p-1}^{(k)}) y^{p-k-1} \equiv 0 \pmod p.$$

Admettons que la congruence ait une solution et appliquons le théorème de Fermat

$$(F) \qquad x^{gp+h} \equiv x^h, \qquad y^{gp+h} \equiv y^h \qquad (\mathrm{mod}\, p)$$

pour éliminer les puissances de x et y de degré supérieur à $(p-1)$ dans les congruences

$$\begin{array}{llll} F^{**}(x,y) \equiv 0, & xF^{**}(x,y) \equiv 0, & \ldots, & x^{p-1}F^{**}(x,y) \equiv 0, \\ yF^{**}(x,y) \equiv 0, & xyF^{**}(x,y) \equiv 0, & \ldots, & x^{p-1}yF^{**}(x,y) \equiv 0, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ y^{p-1}F^{**}(x,y) \equiv 0, & xy^{p-1}F^{**}(x,y) \equiv 0, & \ldots, & x^{p-1}y^{p-1}F^{**}(x,y) \equiv 0 \end{array} \pmod p.$$

Nous arriverons à p^2 congruences nouvelles, linéaires et homogènes par rapport aux p^2 produits

$$x^\alpha y^\beta \qquad (\alpha, \beta = 0, 1, 2, \ldots, p-1)$$

et le déterminant de ces congruences sera, en vertu des hypothèses faites, congru à zéro. Or ce déterminant est identique au déterminant $\Gamma_{F^{**}}$ étudié au n° 1, nous avons donc établi que *la condition*

$$\Gamma_{F^{**}} \equiv 0 \pmod p$$

est nécessaire pour que la congruence (1^{**}) *soit résoluble.*

Pour démontrer que cette même condition est suffisante, on peut procéder comme au paragraphe III dans la démonstration du théorème correspondant I. On n'a qu'à recourir au théorème relatif à la multiplication des déterminants et l'on trouve

$$\text{(I)} \qquad \Gamma_{F^{**}}\,\Delta^{(p)}_{x,y} \equiv \Delta^{(p)}_{x,y} \prod_{i=0}^{p-1}\prod_{k=0}^{p-1} F^{**}(x_i, y_k) \qquad (\text{mod.}\, p)$$

où les quantités

$$x_0, y_1, \ldots, x_{p-1}$$

et

$$y_0, y_1, \ldots, y_{p-1}$$

figurant dans $\Delta^{(p)}_{x,y}$ sont deux permutations quelconques du système complet des restes

$$0, 1, \ldots, p-1.$$

Mais alors

$$\Delta^{(p)}_{x,y} \not\equiv 0 \qquad (\text{mod}\, p)$$

et l'on peut supprimer le facteur $\Delta^{(p)}_{x,y}$ dans les deux membres de la congruence (I), donc

$$\prod_{i=0}^{p-1}\prod_{k=0}^{p-1} F^{**}(x_i, y_k) \equiv \Gamma_{F^{**}} \qquad (\text{mod}\, p)$$

ou, ce qui revient au même,

$$P \equiv \prod_{g=0}^{p-1}\prod_{h=0}^{p-1} F^{**}(g, h) \equiv \Gamma_{F^{**}} \qquad (\text{mod}\, p).$$

De là nous pouvons conclure que, *si* $\Gamma_{F^{**}}$ *est divisible par* p, un au moins des facteurs de P est congru à zéro, ce qui signifie que dans ce cas *la congruence* (1^{**}) *a nécessairement une solution réelle.*

Quant au théorème IV, nous aurions à répéter ce que nous avons dit à propos du théorème II.

V. — Liaison des théorèmes I et II.

Si nous rangeons les colonnes du déterminant $\Gamma_{F^{**}}$ (de degré p^2) dans un ordre convenable et si nous appliquons deux fois le théo-

rème de Laplace sur le développement d'un déterminant suivant les produits des mineurs, nous trouvons que $\Gamma_{F^{**}}$ se réduit au produit des trois déterminants suivants :

$$L \equiv \begin{vmatrix} a_{p-1}^{(0)} & a_{p-1}^{(1)} & \dots & a_{p-1}^{(p-2)} & a_{p-1}^{(p-1)} \\ a_{p-1}^{(1)} & a_{p-1}^{(2)} & \dots & a_{p-1}^{(p-1)} + a_{p-1}^{(0)} & 0 \\ \dots\dots & \dots\dots & \dots & \dots\dots\dots & \dots\dots \\ a_{p-1}^{(p-1)} + a_{p-1}^{(0)} & a_{p-1}^{(1)} & \dots & a_{p-1}^{(p-2)} & 0 \end{vmatrix}$$

$$M \equiv \begin{vmatrix} a_0^{(p-1)} & a_1^{(p-1)} & \dots & a_{p-2}^{(p-1)} \\ a_1^{(p-1)} & a_2^{(p-1)} & \dots & a_{p-1}^{(p-1)} + a_0^{(p-1)} \\ \dots\dots & \dots\dots & \dots & \dots\dots\dots \\ a_{p-1}^{(p-1)} + a_0^{(p-1)} & a_1^{(p-1)} & \dots & a_{p-2}^{(p-1)} \end{vmatrix}$$

$$N \equiv C_{\Phi}^{[(p-1)^2]}$$

où $\Phi(x, y)$ est ce que devient $F^{**}(x, y)$, si nous remplaçons x^{p-1} et y^{p-1} par 1.

La congruence

$$\Gamma_{F^{**}} \equiv \pm LMN \pmod{p}$$

met en lumière le fait que la congruence (1**) n'a de solution réelle que si l'un des facteurs L, M, N est congru à zéro $(\mathrm{mod}\, p)$.

De plus, nous voyons immédiatement que

$$L \equiv 0 \pmod{p}$$

est la condition nécessaire et suffisante pour la résolubilité de la congruence à une inconnue

$$F(0, y) \equiv 0 \pmod{p};$$

que la condition

$$M \equiv 0 \pmod{p}$$

est nécessaire et suffisante pour que la congruence à une inconnue

$$F(x, 0) \equiv 0 \pmod{p}$$

ait une solution non nulle et enfin que

$$N \equiv C_{\Phi}^{[(p-1)^2]} \pmod{p}$$

exprime la condition pour que la congruence

$$F^{**}(x, y) \equiv 0 \pmod{p}$$

admette une solution, dans laquelle ni x, ni y n'est congru à zéro.

Il est donc établi, même au point de vue formel (ce qui est, du reste, évident *a priori*), que la congruence

$$F^{**}(x, y) \equiv 0 \pmod{p}$$

n'a de solution réelle que si l'une au moins des congruences

$$\left.\begin{aligned} F(x, 0) &\equiv 0 \\ F(0, y) &\equiv 0 \\ \Phi(x, y) &\equiv 0 \end{aligned}\right\} \pmod{p}$$

est résoluble.