ANNALES SCIENTIFIQUES DE L'É.N.S.

GUSTAVE RADOS

Sur la théorie des congruences de degré supérieur

Annales scientifiques de l'É.N.S. 3^e série, tome 30 (1913), p. 395-412

<http://www.numdam.org/item?id=ASENS_1913_3_30__395_0>

SUR LA THÉORIE

DES

CONGRUENCES DE DEGRÉ SUPÉRIEUR;

PAR M. GUSTAVE RADOS.

Dans le présent travail, je me propose de donner quelques théorèmes qui contiennent la réponse à certaines questions — non sans intérêt, à mon avis — se présentant dans la théorie des congruences de degré supérieur.

On peut toujours décider si deux équations algébriques ont une racine commune ou non. Pour cela, on n'a qu'à former le résultant et examiner sa valeur. Il n'en est plus de même lorsqu'il s'agit de la racine commune de deux congruences. Pour que les congruences

$$\begin{aligned} f(x) &\equiv a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m \equiv 0 \\ g(x) &\equiv b_0 x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n \equiv 0 \end{aligned} \pmod{p},$$

ayant pour module un nombre premier p, admettent une racine commune, il est nécessaire que le résultant des polynomes $f(x)$ et $g(x)$ soit nul $(\mathrm{mod}\, p)$, mais cette condition, à elle seule, n'est pas suffisante. Trouver les conditions nécessaires et suffisantes, sera un des objets du présent travail. La solution trouvée permettra de former des critères pour l'existence d'une racine multiple d'une congruence ayant pour module un nombre premier.

Un second groupe de théorèmes aura pour objet les congruences dont le module est la puissance d'un nombre premier.

On sait que l'étude d'une congruence dont le module n'est pas premier peut se ramener à l'étude de congruences ayant pour modules des puissances de nombres premiers. Si, par exemple, on a à résoudre la congruence

$$f(x) \equiv 0 \pmod{m}$$

et que le module m s'écrit

$$m = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

($p_1, p_2, \dots, p_r$ désignant des nombres premiers distincts), la congruence proposée est équivalente au système des r congruences

$$f(x) \equiv 0 \pmod{p_i^{a_i}} \qquad (i = 1, 2, \dots, r).$$

Soient, en effet,

$$\alpha_1^{(i)}, \quad \alpha_2^{(i)}, \quad \dots, \quad \alpha_{j_i}^{(i)}, \quad \dots, \quad \alpha_{\nu_i}^{(i)} \qquad (i = 1, 2, \dots, r)$$

les solutions des congruences précédentes et choisissons les ξ_i de telle façon que l'on ait

$$\frac{m}{p_i^{a_i}} \xi_i \equiv 1 \pmod{p_i^{a_i}} \qquad (i = 1, 2, \dots, r),$$

alors toutes les racines incongrues (mod m) au nombre de $\nu_1, \nu_2, \dots, \nu_r$, vérifiant la congruence au module non premier m, seront données, comme on sait, par la formule

$$x \equiv \frac{m}{p_1^{a_1}} \xi_1 \alpha_{j_1}^{(1)} + \frac{m}{p_2^{a_2}} \xi_2 \alpha_{j_2}^{(2)} + \dots + \frac{m}{p_r^{a_r}} \xi_r \alpha_{j_r}^{(r)} \pmod{m}$$

$$(j_1 = 1, 2, \dots, \nu_1; \; j_2 = 1, 2, \dots, \nu_2; \; \dots; \; j_r = 1, 2, \dots, \nu_r).$$

Dans ce travail, j'aurai l'occasion de montrer en détail que la résolution d'une congruence, ayant pour module une puissance d'un nombre premier, peut toujours se ramener à la résolution d'une congruence qui a pour module un nombre premier. Mais il y a là, entre ces deux espèces de congruences, une différence profonde, sur laquelle il con-

vient d'insister. Si le module est un nombre premier, le nombre des racines distinctes ne peut surpasser le degré de la congruence, mais il n'en est plus de même si le module est une puissance de degré supérieur à 1 d'un nombre premier. Pourtant — et ce sera un des résultats auxquels nous arriverons — cette dernière circonstance ne peut se présenter qu'exceptionnellement à savoir lorsque, le premier membre de la congruence étant un polynome donné, le module est la puissance d'un nombre pris entre certains nombres premiers singuliers.

Pour terminer, je donnerai un théorème qui établit un lien entre la résolution de certaines équations algébriques et des congruences formées à l'aide de ces équations.

I. — Conditions pour l'existence d'une racine commune de deux congruences.

Si les congruences

$$\begin{aligned} f(x) &\equiv a_0 x^m + a_1 x^{m-1} + \ldots + a_m \equiv 0 \\ g(x) &\equiv b_0 x^n + b_1 x^{n-1} + \ldots + b_n \equiv 0 \end{aligned} \pmod p$$

ont une racine commune $x = \alpha$, on peut former, à l'exemple du procédé dialytique de Sylvester qu'on emploie dans la théorie des équations algébriques, les congruences suivantes :

$$\begin{aligned} &\alpha^{n-1} f(\alpha) \equiv 0, \quad \alpha^{n-2} f(\alpha) \equiv 0, \quad \ldots, \quad \alpha^0 f(\alpha) \equiv 0 \\ &\alpha^{m-1} g(\alpha) \equiv 0, \quad \alpha^{m-2} g(\alpha) \equiv 0, \quad \ldots, \quad \alpha^0 g(\alpha) \equiv 0 \end{aligned} \pmod p$$

qui représentent, par rapport aux valeurs

$$\alpha^{m+n-1}, \quad \alpha^{m+n-2}, \quad \ldots, \quad \alpha^1, \quad \alpha^0,$$

un système de $m + n$ congruences linéaires et homogènes. Il faut donc que le résultant

$$\mathrm{R} = \mathrm{Rés.}[f(x), g(x)] = \begin{vmatrix} a_0 & a_1 & \ldots & a_m & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & a_0 & \ldots & \ldots & a_m & \\ b_0 & b_1 & \ldots & b_n & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & b_0 & \ldots & \ldots & b_n & \end{vmatrix}$$

soit congru à zéro (mod p). La congruence

$$R = \text{Rés.}[f(x), g(x)] \equiv 0 \pmod{p}$$

est donc une condition nécessaire pour que les deux congruences données admettent une racine commune. On peut voir aisément que cette condition n'est pas suffisante. Néanmoins on peut tirer de cette condition nécessaire quelques conséquences importantes. Si le résultant des polynomes $f(x)$ et $g(x)$ n'est pas identiquement nul, c'est-à-dire si $f(x)$ et $g(x)$ sont algébriquement premiers entre eux, la condition

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

ne peut être vérifiée que par un nombre fini de nombres premiers p, d'où ce théorème :

THÉORÈME I. — *Si les polynomes $f(x)$ et $g(x)$ sont premiers entre eux, les modules p, par rapport auxquels les congruences*

$$\begin{aligned} f(x) &\equiv 0 \\ g(x) &\equiv 0 \end{aligned} \pmod{p}$$

admettent une racine commune, sont en nombre limité.

Prenons en particulier $g(x)$ égal à $f'(x)$, dérivée de $f(x)$, on a alors comme corollaire ce théorème :

THÉORÈME II. — *Si le polynome $f(x)$ est premier avec sa dérivée $f'(x)$, la congruence*

$$f(x) \equiv 0 \pmod{p}$$

ne peut avoir de racine multiple que pour un nombre limité de modules premiers p.

Cela étant, nous allons chercher les conditions nécessaires et suffisantes pour l'existence d'une racine commune à deux congruences données. Comme on peut constater immédiatement la présence de la racine $x \equiv 0$, nous pouvons nous borner à rechercher les racines communes différentes de zéro (mod p). Écrivons donc les congruences

sous la forme (¹)

$$(1)\qquad \begin{cases} f(x) \equiv a_0 x^{p-2} + a_1 x^{p-3} + \ldots + a_{p-2} \equiv 0 \\ g(x) \equiv b_0 x^{p-2} + b_1 x^{p-3} + \ldots + b_{p-2} \equiv 0 \end{cases} \pmod p$$

et, en supposant qu'il existe une racine commune non nulle, cherchons les conditions auxquelles les coefficients doivent satisfaire. Cette racine commune (qui, par hypothèse, n'est pas divisible par p) vérifiera toutes les congruences

$$uf(x) + g(x) \equiv 0 \pmod p \qquad (u = 0, 1, 2, \ldots, p-1).$$

Or la congruence

$$uf(x) + g(x) \equiv 0 \pmod p$$

n'a de racine différente de zéro que si

$$\Phi(u) \equiv \begin{vmatrix} a_0 & u + b_0 & a_1 u + b_1 & \ldots & a_{p-2} u + b_{p-2} \\ a_1 & u + b_1 & a_2 u + b_2 & \ldots & a_0 \quad u + b_0 \\ \ldots\ldots\ldots & \ldots\ldots & \ldots & & \ldots\ldots\ldots \\ a_{p-2} u + b_{p-2} & a_0 u + b_0 & \ldots & & a_{p-3} u + b_{p-3} \end{vmatrix} \equiv$$

$$\equiv R_0 u^{p-1} + R_1 u^{p-2} + \ldots + R_{p-2} u + R_{p-1} \equiv 0 \pmod p,$$

ainsi que je l'ai démontré dans mon Mémoire K cité plus haut.

Donc, il résulte de l'existence d'une racine, commune aux deux congruences (1), que la congruence en u

$$\Phi(u) \equiv R_0 u^{p-1} + R_1 u^{p-2} + \ldots + R_{p-2} u + R_{p-1} \equiv 0 \pmod p$$

(où les coefficients sont des polynomes par rapport aux a et aux b) est vérifiée pour

$$u \equiv 0, 1, 2, \ldots, p-1 \pmod p.$$

Le nombre de ces valeurs étant supérieur au degré de la congruence en u, il faut que l'on ait

$$(I)\qquad R_0 \equiv 0, \quad R_1 \equiv 0, \quad \ldots, \quad R_{p-1} \equiv 0 \pmod p.$$

(¹) *Voir* mes Mémoires : *Sur la théorie des congruences de degré supérieur*, paru en hongrois [*A felsöbbfokú kongruenciák elméletéhez* (*Math. és Fermészett. Értesétö*, t. I, 1883, p. 296)]; *Zur Theorie der Congruenzen höheren Grades* (*Journal für die reine und angewandte Mathematik*, t. XCIX, p. 258). Pour abréger, je citerai ces Mémoires par la lettre K.

Ces conditions sont *nécessaires* pour qu'une racine commune existe.

Les considérations simples suivantes montreront qu'elles sont aussi *suffisantes*. Supposons toutes les conditions (I) vérifiées. Dans ce cas, le déterminant $\Phi(u)$ étant nul pour toutes les valeurs incongrues de u

$$u \equiv 0, 1, 2, \ldots, p-1 \pmod{p},$$

chacune des congruences

$$(2) \qquad \begin{cases} uf(x) + g(x) \equiv 0 \pmod{p} \\ (u = 0, 1, 2, \ldots, p-1) \end{cases}$$

aura une racine différente de zéro. Or ces congruences sont au nombre de p et il n'y a que $p-1$ valeurs de u distinctes de zéro. Donc, deux au moins des congruences (2)

$$\begin{matrix} u' f(x) + g(x) \equiv 0 \\ u'' f(x) + g(x) \equiv 0 \end{matrix} \pmod{p}$$

auront une racine commune ξ différente de zéro :

$$\begin{matrix} u' f(\xi) + g(\xi) \equiv 0 \\ u'' f(\xi) + g(\xi) \equiv 0 \end{matrix} \pmod{p}.$$

D'autre part,

$$\begin{vmatrix} u' & 1 \\ u'' & 1 \end{vmatrix} \not\equiv 0 \pmod{p},$$

donc

$$f(\xi) \equiv 0, \qquad g(\xi) \equiv 0 \pmod{p};$$

c'est dire que les congruences (1) admettent la racine commune ξ.

Nous pouvons donc énoncer le théorème suivant :

THÉORÈME III. — *Pour que les congruences*

$$f(x) \equiv 0, \qquad g(x) \equiv 0 \pmod{p}$$

admettent une racine commune, il est nécessaire et suffisant qu'on ait

$$R_0 \equiv 0, \qquad R_1 \equiv 0, \qquad R_{p-1} \equiv 0 \pmod{p}.$$

Écrivons explicitement ces conditions (I). Pour cela, convenons de

désigner une colonne quelconque des matrices

$$\left\Vert \begin{matrix} a_0 & a_1 & \ldots & a_{p-2} \\ a_1 & a_2 & \ldots & a_0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{p-2} & a_0 & \ldots & a_{p-3} \end{matrix} \right\Vert \quad \text{et} \quad \left\Vert \begin{matrix} b_0 & b_1 & \ldots & b_{p-2} \\ b_1 & b_2 & \ldots & b_0 \\ \ldots & \ldots & \ldots & \ldots \\ b_{p-2} & b_0 & \ldots & b_{p-3} \end{matrix} \right\Vert$$

par le premier élément de la colonne et un déterminant quelconque (composé de ces colonnes) par les éléments de la première ligne. Ainsi le symbole

$$| a_0, a_1, \ldots, a_{i_1-1}, b_{i_1}, a_{i_1+1}, \ldots, a_{i_k-1}, b_{i_k}, a_{i_k+1}, \ldots, a_{p-2} |$$

représente le déterminant d'ordre $p - 1$ qui contient les colonnes ayant pour premiers éléments

$$a_0 \quad a_1, \quad \ldots, \quad a_{i_1-1}, \quad b_{i_1}, \quad a_{i_1+1}, \quad \ldots, \quad a_{i_k-1}, \quad b_{i_k}, \quad a_{i_k+1}, \quad \ldots, \quad a_{p-2}.$$

Les quantités $R_0, R_1, \ldots, R_{p-1}$ s'expriment alors sous la forme

$$R_0 = | a_0, a_1, \ldots, a_{p-2} |,$$

$$R_1 = \sum_{(i_1)} | a_0, a_1, \ldots, a_{i-1}, b_i, a_{i+1}, \ldots, a_{p-2} |,$$

$$R_2 = \sum_{(i_1, i_2)} | a_0, a_1, \ldots, a_{i_1-1}, b_{i_1}, a_{i_1+1}, \ldots, a_{i_2-1}, b_{i_2}, a_{i_2+1}, \ldots, a_{p-2} |$$

. . . .

$$R_k = \sum_{(i_1, i_2, \ldots, i_k)} | a_0, a_1, \ldots, a_{i_1-1}, b_{i_1}, a_{i_1+1}, \ldots, a_{i_k-1}\, b_{i_k}, \alpha_{i_k+1}, \ldots, a_{p-2} |,$$

$$R_{p-1} = | b_0, b_1, \ldots, b_{-1} |$$

où le signe Σ dans l'expression de R_k signifie qu'il faut prendre pour

$$i_1, \quad i_2, \quad \ldots, \quad i_k$$

toutes les combinaisons k à k des éléments

$$0, \quad 1, \quad 2, \quad \ldots, \quad p-2.$$

Éclaircissons ceci par un exemple. Les conditions nécessaires et suffisantes pour que les congruences

$$\left. \begin{aligned} f(x) &\equiv a_0 x^3 + a_1 x^2 + a_2 x + a_3 \equiv 0 \\ g(x) &\equiv b_0 x^3 + b_1 x^2 + b_2 x + b_3 \equiv 0 \end{aligned} \right\} \pmod 5$$

aient une racine commune sont les suivantes :

$$R_0 \equiv \begin{vmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 & a_0 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_0 & a_1 & a_2 \end{vmatrix} \equiv 0 \pmod 5;$$

$$R_1 \equiv \begin{vmatrix} b_0 & a_1 & a_2 & a_3 \\ b_1 & a_2 & a_3 & a_0 \\ b_2 & a_3 & a_0 & a_1 \\ b_3 & a_0 & a_1 & a_2 \end{vmatrix} + \begin{vmatrix} a_0 & b_1 & a_2 & a_3 \\ a_1 & b_2 & a_3 & a_0 \\ a_2 & b_3 & a_0 & a_1 \\ a_3 & b_0 & a_1 & a_2 \end{vmatrix} + \begin{vmatrix} a_0 & a_1 & b_2 & a_3 \\ a_1 & a_2 & b_3 & a_0 \\ a_2 & a_3 & b_0 & a_1 \\ a_3 & a_0 & b_1 & a_2 \end{vmatrix} + \begin{vmatrix} a_0 & a_1 & a_2 & b_3 \\ a_1 & a_2 & a_3 & b_0 \\ a_2 & a_3 & a_0 & b_1 \\ a_3 & a_0 & a_1 & b_2 \end{vmatrix} \equiv 0 \pmod 5;$$

$$R_2 \equiv \begin{vmatrix} b_0 & b_1 & a_2 & a_3 \\ b_1 & b_2 & a_3 & a_0 \\ b_2 & b_3 & a_0 & a_1 \\ b_3 & b_0 & a_1 & a_2 \end{vmatrix} + \begin{vmatrix} b_0 & a_1 & b_2 & a_3 \\ b_1 & a_2 & b_3 & a_0 \\ a_3 & b_2 & b_0 & a_1 \\ b_3 & a_0 & b_1 & a_2 \end{vmatrix} + \begin{vmatrix} b_0 & a_1 & a_2 & b_3 \\ b_1 & a_2 & a_3 & b_0 \\ b_2 & a_3 & a_0 & b_1 \\ b_3 & a_0 & a_1 & b_2 \end{vmatrix} + \begin{vmatrix} a_0 & b_1 & & a_3 \\ a_1 & b_2 & b_3 & a_0 \\ a_2 & b_3 & b_0 & a_1 \\ a_3 & b_0 & b_1 & a_2 \end{vmatrix} + \begin{vmatrix} a_0 & b_1 & a_2 & b_3 \\ a_1 & b_2 & a_3 & b_0 \\ a_2 & b_3 & a_0 & b_1 \\ a_3 & b_0 & a_1 & b_2 \end{vmatrix} + \begin{vmatrix} a_0 & a_1 & b_2 & b_3 \\ a_1 & a_2 & b_3 & b_0 \\ a_2 & a_3 & b_0 & b_1 \\ a_3 & a_0 & b_1 & b_2 \end{vmatrix}$$

$$R_3 \equiv \begin{vmatrix} a_0 & b_1 & b_2 & b_3 \\ a_1 & b_2 & b_3 & b_0 \\ a_2 & b_3 & b_0 & b_1 \\ a_3 & b_0 & b_1 & b_2 \end{vmatrix} + \begin{vmatrix} b_0 & a_1 & b_2 & b_3 \\ b_1 & a_2 & b_3 & b_0 \\ b_2 & a_3 & b_0 & b_1 \\ b_3 & a_0 & b_1 & b_2 \end{vmatrix} + \begin{vmatrix} b_0 & b_1 & a_2 & b_3 \\ b_1 & b_2 & a_3 & b_0 \\ b_2 & b_3 & a_0 & b_1 \\ b_3 & b_0 & a_1 & b_2 \end{vmatrix} + \begin{vmatrix} b_0 & b_1 & b_2 & a_3 \\ b_1 & b_2 & b_3 & a_0 \\ b_2 & b_3 & b_0 & a_1 \\ b_3 & b_0 & b_1 & a_2 \end{vmatrix} \pmod 5;$$

$$R_4 \equiv \begin{vmatrix} b_0 & b_1 & b_2 & b_3 \\ b_1 & b_2 & b_3 & b_0 \\ b_2 & b_3 & b_0 & b_1 \\ b_3 & b_0 & b_1 & b_2 \end{vmatrix} \pmod 5.$$

Si, dans le théorème III, nous posons

$$g(x) \equiv \frac{df(x)}{dx},$$

la fonction $\Phi(u)$ qui figurait dans la démonstration sera remplacée par la suivante :

$$\Phi_1(u) \equiv \begin{vmatrix} a_0 u & a_1 u + (p-1)a_0 & a_2 u + (p-2)a_1 & \dots & a_{p-2} u + a_{p-3} \\ a_1 u + (p-1)a_0 & a_2 u + (p-2)a_1 & a_3 u + (p-3)a_2 & \dots & a_0 u \\ \dots\dots\dots & \dots\dots\dots & \dots\dots\dots & \dots & \dots \\ a_{p-2} u + a_{p-3} & a_0 u & a_1 u + (p-1)a_0 & \dots & a_{p-3} u + 2a_{p-4} \end{vmatrix}$$
$$\equiv D_0 u^{p-2} + D_1 u^{p-3} + \dots + D_{p-2}$$

et nous arriverons à ce théorème :

THÉORÈME IV. — *Pour que la congruence*

$$f(x) \equiv 0 \pmod p$$

ait une racine multiple, il faut et il suffit que les conditions

$$(II) \qquad D_0 \equiv 0, \quad D_1 \equiv 0, \quad \dots, \quad D_{p-2} \equiv 0 \pmod p$$

soient vérifiées.

Il est évident que les conditions (II) peuvent s'écrire sous forme explicite aussi facilement que les conditions (I).

Je ferai observer que la méthode qui nous a conduit au théorème III peut s'appliquer à un nombre quelconque de congruences. Pour abréger l'écriture, nous raisonnerons sur *trois* congruences, mais cela n'implique, je le répète, aucune restriction.

Soient les congruences

$$\begin{aligned} f(x) &\equiv a_0 x^{p-2} + a_1 x^{p-3} + \dots + a_{p-2} \equiv 0 \\ g(x) &\equiv b_0 x^{p-2} + b_1 x^{p-3} + \dots + b_{p-2} \equiv 0 \\ h(x) &\equiv c_0 x^{p-2} + c_1 x^{p-3} + \dots + c_{p-2} \equiv 0 \end{aligned} \pmod p$$

et supposons qu'elles aient une racine commune différente de zéro qui vérifiera naturellement chacune des p^2 congruences

$$uf(x) + vg(x) + h(x) \equiv 0 \pmod p$$
$$(u, v = 0, 1, 2, \dots, p-1).$$

Mais alors, d'après le théorème établi dans mon Mémoire K, on aura

$$\Phi(u, v) \equiv \begin{vmatrix} a_0 u + b_0 v + c_0 & \dots & a_{p-2} u + b_{p-2} v + c_{p-2} \\ \dots\dots\dots\dots & \dots & \dots\dots\dots\dots\dots \\ a_{p-2} u + b_{p-2} v + c_{p-2} & \dots & a_{p-3} u + b_{p-3} v + c_{p-3} \end{vmatrix}$$

$$\equiv \sum_{k=0}^{p-1} (R_{k0} u^k + R_{k1} u^{k-1} v + \dots + R_{kk} v^k) \equiv \pmod p,$$

et cela pour tous les systèmes de valeurs

$$(u = k,\ v = l),$$
$$(k = 0, 1, 2, \dots, p-1;\ l = 0, 1, 2, \dots, p-1).$$

Or la congruence

$$\Phi(u, v) \equiv 0 \pmod p$$

est de degré $p-1$ et il est aisé à démontrer qu'elle ne peut être vérifiée par les p^2 systèmes de valeurs (k, l) que si

$$(I') \qquad R_{k0} \equiv 0, \quad R_{k1} \equiv 0, \quad \dots, \quad R_{kk} \equiv 0 \pmod p.$$

Ces conditions sont donc *nécessaires* pour qu'il existe une racine commune.

Elles sont aussi *suffisantes* et l'on peut s'en convaincre par les considérations qui suivent. Supposons les conditions (I') vérifiées. Le déterminant $\Phi(u, v)$ étant nul, quelques valeurs que prennent les indéterminées u et v, on en conclut, d'après le théorème III, que les congruences

$$f(x) \equiv 0, \qquad vh(x) + g(x) \equiv 0 \pmod p$$

ont, quelle que soit la valeur de v, une racine commune différente de zéro. Comme le nombre de ces systèmes de congruences dépasse d'une unité le nombre des valeurs incongrues $(\mathrm{mod}\, p)$ différentes de zéro, il y aura deux systèmes admettant la même racine commune ξ. On aura donc

$$f(\xi) \equiv 0, \qquad v' g(\xi) + h(\xi) \equiv 0 \pmod p$$

et

$$f(\xi) \equiv 0, \qquad v'' g(\xi) + h(\xi) \equiv 0 \pmod p$$
$$(v'' \not\equiv v'),$$

d'où il résulte

$$f(\xi)\equiv 0, \qquad g(\xi)\equiv 0, \qquad h(\xi)\equiv 0 \qquad (\mathrm{mod}\, p).$$

C'est dire que les congruences (1′) ont une racine commune. Nous pouvons donc énoncer ce théorème :

THÉORÈME V. — *Pour que les congruences*

$$f(x)\equiv 0, \qquad g(x)\equiv 0, \qquad h(x)\equiv 0 \qquad (\mathrm{mod}\, p)$$

admettent une racine commune différente de zéro, il faut et il suffit que l'on ait

$$(\mathrm{I}') \qquad \begin{cases} R_{k0}\equiv 0, \quad R_{k1}\equiv 0, \quad \ldots, \quad R_{kk}\equiv 0 \quad (\mathrm{mod}\, p) \\ (k=0,1,\ldots,p-1). \end{cases}$$

Si, en particulier, on pose

$$g(x)\equiv \frac{df(x)}{dx}, \qquad h(x)\equiv \frac{d^2 f(x)}{dx^2},$$

les conditions (I′) ainsi transformées deviennent *nécessaires et suffisantes pour que la congruence*

$$f(x)\equiv 0 \qquad (\mathrm{mod}\, p)$$

ait une racine de multiplicité égale ou supérieure à 3.

II. — Congruence ayant pour module une puissance d'un nombre premier.

$$(1) \qquad \begin{cases} f(x)\equiv a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \qquad (\mathrm{mod}\, p^k) \\ (k\geq 2). \end{cases}$$

Il est évident que toute racine de cette congruence vérifie aussi la suivante :

$$(2) \qquad f(x)\equiv 0 \qquad (\mathrm{mod}\, p^{k-1}).$$

Donc si la congruence (2) n'a pas de solution, la congruence (1) n'en aura pas non plus. Si, au contraire, la congruence (2) a pour racines

les nombres

$$\alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_i, \quad \ldots, \quad \alpha_r,$$

les racines de la congruence (1) se trouvent parmi les termes des progressions arithmétiques

$$\alpha_1 + p^{k-1}y, \quad \alpha_2 + p^{k-1}y, \quad \ldots, \quad \alpha_r + p^{k-1}y \qquad (y = 0, 1, 2, \ldots).$$

Il est naturel de se poser la question : comment choisir la valeur de y pour que

$$\alpha_i + p^{k-1}y$$

vérifie la congruence (1)? On trouve la condition

$$f(\alpha_i + p^{k-1}y) \equiv f(\alpha_i) + p^{k-1}\frac{f'(\alpha_i)}{1!}y + p^{2k-2}\frac{f''(\alpha_i)}{2!}y^2 + \ldots + p^{nk-n}\frac{f^{(n)}(\alpha_i)}{n!}y^n \equiv 0 \pmod{p^k}$$

qui s'écrit, grâce à l'inégalité

$$k \geq 2,$$

sous la forme plus simple

$$f(\alpha_i + p^{k-1}y) \equiv f(\alpha_i) + p^{k-1}y f'(\alpha_i) \equiv 0 \pmod{p^k},$$

parce que tous les termes, à partir du troisième, du développement taylorien sont divisibles par p^k.

Tout se réduit donc à résoudre la congruence du premier degré

$$p^{k-1}f'(\alpha_i)\,y = -f(\alpha_i) \pmod{p^k} \tag{3}$$

où y désigne l'inconnue.

Ici il y a deux cas à considérer suivant que le plus grand commun diviseur de $p^{k-1}f'(\alpha_i)$ et p^k est

$$[p^{k-1}f'(\alpha_i), p^k] = p^{k-1} \tag{I}$$

ou

$$[p^{k-1}f'(\alpha_i), p^k] = p^k. \tag{II}$$

Dans le cas (I) les solutions de la congruence (3) vérifieront la congruence du premier degré

$$f'(\alpha_i)\,v \equiv -\frac{f(\alpha_i)}{p^{k-1}} \pmod{p} \tag{4}$$

qui a pour unique solution

$$v \equiv -\frac{f(\alpha_i)}{p^{k-1}}[f'(\alpha_i)]^{p-2} \pmod{p};$$

donc, dans ce cas, les solutions distinctes de la congruence (3) se trouveront parmi les valeurs

$$y = -\frac{f(\alpha_i)}{p^{k-1}}[f'(\alpha_i)]^{p-2} + pu \qquad (u = 0, 1, 2, \ldots).$$

Les valeurs correspondantes de x

$$x = \alpha_i + p^{k-1}y = \alpha_i - f(\alpha_i)[f'(\alpha_i)]^{p-2} + p^k u$$

seront congrues (mod p^k) à

$$x \equiv \alpha_i - f(\alpha_i)[f'(\alpha_i)]^{p-2};$$

ainsi à chaque racine de la congruence (2) correspondra une racine de la congruence (1)

$$x \equiv \alpha_1 - f(\alpha_i)[f'(\alpha_i)]^{p-2} \pmod{p^k}.$$

Si le cas (I) se présente pour toutes les racines de la congruence (2), c'est-à-dire que

$$f'(\alpha_i) \not\equiv 0 \pmod{p}$$
$$(i = 1, 2, \ldots, r),$$

alors la congruence (1) aura exactement autant de racines que la congruence (2).

Nous avons affaire au cas (II), si

$$f'(\alpha_i) \equiv 0 \pmod{p}$$

et observons que, dans ce cas, α_i est aussi racine commune des congruences

$$f(x) \equiv 0 \pmod{p},$$
$$f'(x) \equiv 0 \pmod{p}.$$

Ici encore on a à envisager deux circonstances différentes qui peuvent arriver l'une ou l'autre.

Dans la première, on a

$$(\mathrm{II}^a) \qquad \frac{-f(\alpha_i)}{p^{k-1}} \not\equiv 0 \pmod{p},$$

ce qui exclut la possibilité de résoudre la congruence (3), donc la suite

$$\alpha_i + p^{k-1}y \qquad (y = 0, 1, 2, \ldots)$$

ne renferme aucune solution de la congruence (1). Si cela arrive pour toutes les racines

$$\alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_r,$$

la congruence (1) n'aura aucune solution, quoique la congruence (2) en ait.

La deuxième circonstance se présente si

$$(\mathrm{II}^b) \qquad \frac{-f(\alpha_i)}{p^{k-1}} \equiv 0 \pmod{p},$$

c'est-à-dire que α_i est une racine commune des congruences

$$f(x) \equiv 0 \pmod{p^{k-1}} \qquad \text{et} \qquad f(x) \equiv 0 \pmod{p^k}.$$

Dans ce cas, la congruence (y) étant vérifiée par chacune des p valeurs

$$v \equiv 0, 1, 2, \ldots, p-1 \pmod{p},$$

la racine α_i de la congruence

$$f(x) \equiv 0 \pmod{p^{k-1}}$$

nous donnera les solutions suivantes de la congruence (1)

$$x \equiv \alpha_i, \quad \alpha_i + p^{k-1}, \quad \alpha_i + 2p^{k-1}, \quad \ldots, \quad \alpha_i + (p-1)p^{k-1} \pmod{p^k}.$$

Si cela arrive pour toutes les racines de la congruence (2), la congruence (1) aura pr racines.

En passant de la congruence (1) à la congruence (2), de là, à la congruence

$$f(x) \equiv 0 \pmod{p^{k-2}},$$

puis à la congruence

$$f(x) \equiv 0 \pmod{p^{k-3}},$$

et ainsi de suite, le nombre des racines ne peut varier que si quelques-unes de ces congruences présentent le cas (II). Notamment, le nombre des racines augmente à chaque cas (II^a) et diminue à chaque cas (II^b). Si ce dernier cas ne se présente jamais la congruence (1) aura au plus autant de racines que la congruence

$$f(x) \equiv 0 \pmod{p}$$

et pour celle-là on sait que le nombre des racines ne peut dépasser le degré de la congruence.

En résumé, le nombre des racines de la congruence (1) ne peut dépasser le degré de la congruence que si les congruences

$$f(x) \equiv 0, \qquad \frac{df(x)}{dx} \equiv 0 \pmod{p}$$

admettent une racine commune et que, par suite, la congruence

$$f(x) \equiv 0 \pmod{p}$$

a une racine multiple. Mais, d'après le théorème II du paragraphe précédent, si les polynomes $f(x)$ et $f'(x)$ sont premiers entre eux, la congruence

$$f(x) \equiv 0 \pmod{p}$$

n'admet de racine multiple que pour quelques modules singuliers. De là résulte le théorème suivant :

THÉORÈME I. — *Si les polynomes $f(x)$ et $f'(x)$ sont premiers entre eux, il n'y a qu'un nombre limité de nombres premiers p, pour lesquels le nombre des racines de la congruence*

$$f(x) \equiv 0 \pmod{p^k}$$

dépasse le degré de la congruence.

Le cas général est donc celui où le nombre des racines de la congruence, ayant pour module une puissance d'un nombre premier, est inférieur au degré de la congruence.

Il ne sera peut-être pas inutile d'éclaircir ce qui précède par un exemple.

Soit donnée la congruence

$$f(x) \equiv x^5 - 7x^4 + 16x^3 - 8x^2 - 16x - 327 \equiv 0 \pmod{7^3}.$$

Nous la résolvons d'abord mod 7. Par rapport à ce module, elle se met sous la forme plus simple

$$f(x) \equiv x^5 + 2x^3 - x^2 - 2x + 2 \equiv 0 \pmod 7$$

qui est vérifiée par

$$\alpha \equiv -1, \qquad \beta \equiv 2 \pmod 7.$$

Comme

$$f'(\alpha) \equiv 5\alpha^4 - 28\alpha^3 + 48\alpha^2 - 16\alpha - 16 \equiv 81 \not\equiv 0 \pmod 7,$$
$$f'(\beta) \equiv 5\beta^4 - 28\beta^3 + 48\beta^2 - 16\beta - 16 \equiv 0 \pmod 7,$$

nous voyons le cas (I) se présenter pour la racine α et le cas (II) pour la racine β. On a ensuite

$$f(\beta) \equiv \beta^5 - 7\beta^4 + 16\beta^3 - 8\beta^2 - 16\beta - 327 \equiv 0 \pmod{7^2};$$

la racine β rentre donc dans la catégorie (II^b). Les racines de la congruence

$$f(x) \equiv x^5 - 7x^4 + 16x^3 - 8x^2 - 16x - 327 \equiv 0 \pmod{7^2}$$

s'obtiennent toutes par le procédé expliqué plus haut. La racine α donnera naissance à une racine et la racine β à sept. Ces racines seront

$$\alpha' \equiv -1, \qquad \beta'_{k_1} \equiv 2 + 7k_1 \pmod{7^2}$$
$$(k_1 = 0, 1, 2, 3, 4, 5, 6).$$

Revenons enfin à la congruence proposée

$$f(x) \equiv x^5 - 7x^4 + 16x^3 - 8x^2 - 16x - 327 \equiv 0 \pmod{7^3}.$$

Nous trouvons

$$f'(\alpha') \not\equiv 0, \qquad f'(\beta'_{k_1}) \equiv 0 \pmod 7$$
$$(k_1 = 1, 2, \ldots, 6)$$

et puis

$$f(\beta'_{k_1}) \equiv 0 \pmod{7^3}.$$

Donc la racine α' fait apparaître le cas (I) et les racines β'_{k_1} le cas (II^b).

Les racines de la congruence proposée s'expriment comme il suit

$$\alpha'' \equiv -1, \qquad \beta''_{k_1 k_2} = 2 + 7k_1 + 7^2 k_2 \qquad (\mathrm{mod}\, 7^3)$$
$$(k_1, k_2 = 0, 1, 2, 3, 4, 5, 6).$$

Elles sont au nombre de cinquante.

Si l'on se donnait la congruence

$$f(x) \equiv x^5 - 7x^4 + 16x^3 - 8x^2 - 16x - 327 \equiv 0 \qquad (\mathrm{mod}\, 7^4),$$

celle-là n'aurait qu'une seule racine. En effet,

$$f'(\alpha'') \not\equiv 0, \qquad f'(\beta''_{k_1 k_2}) \equiv 0 \qquad (\mathrm{mod}\, 7),$$
$$f(\beta''_{k_1 k_2}) \not\equiv 0 \qquad (\mathrm{mod}\, 7^4)$$
$$(k_1, k_2 = 1, 2, \ldots, 6),$$

cela revient à dire que la racine α'' appartient au cas (I) et toutes les racines $\beta_{k_1 k_2}$ au cas (II^a). A α'' correspondra une racine, aux $\beta_{k_1 k_2}$ aucune. Ainsi la congruence donnée du cinquième degré ayant pour module 7^4 admet une racine unique.

Comme conséquence intéressante des considérations qui précèdent, énonçons le théorème suivant :

THÉORÈME II. — *Soit*

$$f(x) = 0$$

une équation algébrique à coefficients entiers, admettant les racines rationnelles

$$\frac{g_1}{h_1}, \quad \frac{g_2}{h_2}, \quad \ldots, \quad \frac{g_m}{h_m}$$

avec les degrés de multiplicité

$$k_1, \quad k_2, \quad \ldots, \quad k_m$$

et soit p un nombre premier quelconque. Nous pouvons écrire immédiatement mp^{k-1} *racines de la congruence*

$$f(x) \equiv 0 \qquad (\mathrm{mod}\, p^k),$$

pourvu que k ne dépasse aucun des entiers

$$k_1, \quad k_2, \quad \ldots, \quad k_m.$$

Ces racines sont données par la formule

$$x \equiv g_i h_i^{p-2} + c_1^{(i)} p + c_2^{(i)} p^2 + \ldots + c_{k-1}^{(i)} p^{k-1} \pmod{p^k}$$
$$(c_1^{(i)}, c_2^{(i)}, \ldots, c_{k-1}^{(i)} = 0, 1, 2, \ldots, p-1; \; i = 1, 2, \ldots, m).$$

Ces racines ne sont autres que les entiers qu'on peut écrire avec k chiffres dans le système de numération ayant pour base p, le premier chiffre étant congru à $g_i h_i^{p-2} \pmod{p}$.