Časopis pro pěstování matematiky a fysiky

Štefan Schwarz

Sur le nombre des racines et des facteurs irréductibles d'une congruence donnée

Časopis pro pěstování matematiky a fysiky, Vol. 69 (1940), No. 3-4, 128--145

Persistent URL: http://dml.cz/dmlcz/123330

Sur le nombre des racines et des facteurs irréductibles d'une congruence donnée.

Štefan Schwarz, Praha.

Publié avec le concours de la Fondation Masaryk du Conseil national des recherches.

(Reçu le 1 décembre 1938.)

Soit

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n \equiv 0 \pmod{p} \qquad (1)$$

une congruence de degré n, à coefficients entiers, ayant un discriminant $D \not\equiv 0 \pmod{p}$. p soit un nombre premier.

On entend sous une racine x_i de la congruence (1) un nombre entier pour lequel la congruence (1) est vérifiée. Par j_i ($i = 1, \ldots, n$) nous désignons les imaginaires de Galois [c'est-à-dire les solutions imaginaires de la congruence (1)], qui sont toutes contenues dans une extension convenable du corps des restes (mod p).[1])

Posons la question quel est le nombre des racines de la congruence (1). Notre but est de déterminer ce nombre en fonction des coefficients de (1), ou en fonction des expressions, qui sont étroitement liées aux coefficients.

Beaucoup d'auteurs se sont occupés de ce problème, mais la plupart des travaux se rattache aux diverses congruences specialisées.[2])

Quant aux considérations générales les résultats peuvent être partagés en deux groupes. Le premier groupe se rapporte aux travaux des M. M. König, Rados, Kronecker et Gegenbauer et son résultat principal est le théorème suivant: La congruence

$$f(x) = a_0 x^{p-2} + a_1 x^{p-1} + \ldots + a_{p-2} \equiv 0 \pmod{p}^3) \qquad (a)$$

[1]) On peut se borner à la plus petite extension dans laquelle le polynôme $f(x)$ se décompose totalement (mod p).

[2]) On trouve une liste complète de tous ces travaux dans le livre bien connu L. E. Dickson: History of the Theory of Numbers, New York 1934, Vol. I., p. 224—233.

[3]) On doit se rendre compte qu'on peut écrire chaque congruence, avec $p - 2 > n$ dans la forme (a) pourvu qu'on pose quelques a_k ($k = 0, 1, \ldots$) égaux à zéro. Si $n > p - 2$ on peut au moyen de la congruence $x^{p-1} \equiv 1 \pmod{p}$, qui a lieu pour chaque racine de (a), réduire le degré n au degré $p - 2$.

[avec un discriminant $D \not\equiv 0 \pmod p$] a précisément $s \pmod p$ différentes racines, si le rang de la matrice cyclique de l'ordre $(p-1)$

$$\begin{pmatrix} a_0 & a_1 & a_2 \ldots a_{p-1} & a_{p-2} \\ a_1 & a_2 & a_3 \ldots a_{p-2} & a_0 \\ \vdots & & & \vdots \\ a_{p-2} & a_0 & a_1 \ldots a_{p-4} & a_{p-3} \end{pmatrix},$$

est $p-1-s$.[4])

Une seconde formule a été donnée par A. Hurwitz[5]) par une méthode, qui est tout-à fait différente des méthodes du premier groupe. Le nombre r_1 des racines de la congruence

$$a_0 + a_1 x + \ldots + a_n x^n \equiv 0 \pmod p$$

est donné par la relation

$$r_1 + 1 \equiv (p-1)! \cdot \sum \frac{a_0^{\alpha_0}}{\alpha_0!} \frac{a_1^{\alpha_1}}{\alpha_1!} \ldots \frac{a_n^{\alpha_n}}{\alpha_n!} \pmod p,[6]) \qquad (b)$$

la somme étant étendue à toutes les solutions non négatives de

$$\alpha_0 + \alpha_1 + \ldots + \alpha_n = p-1$$
$$\alpha_1 + 2\alpha_2 + \ldots + n\alpha_n \equiv 0 \pmod{p-1}.$$

Ce théorème a été de même généralisé par M. Dickson[7]) et Cipolla.[8])

Je donne une solution nouvelle du problème posé et je resous un problème plus général, c'est-à-dire, je donne des formules pour le nombre des facteurs du seconde, troisième etc. degré de la congruence (1). A la fin nous ferons voir l'importance des résultats obtenus en traitant quelques applications.

1. *La formule pour le nombre des racines de la congruence* (1).

Nous partons du théorème suivant de M. K. Petr.[9])

Construisons au moyen de la congruence (1) — en l'élevant successivement aux puissances diverses — les expressions

$$x^{kp} \equiv c_{k,0} + c_{k,1} x + c_{k,2} x^2 + \ldots + c_{k,n-1} x^{n-1} \pmod p \qquad (2)$$

pour $k = 0, 1, 2, \ldots, n-1$.

[4]) On trouve la démonstration de ce théorème dans les travaux cités chez Dickson et surtout dans les: „Vorlesungen über Zahlentheorie" de Kronecker (éd. par. K. Hensel, 1901) p. 388—415.

[5]) A. Hurwitz: Archiv Math. Phys. (3), 5, 1903, 17—27.

[6]) D'après le théorème de Wilson on peut écrire -1 au lieu de $(p-1)!$ La congruence (1) a au plus n racines. La formule (b) nous donne la classe (mod p) dans laquelle se trouve r_1; donc, si $p > n$ la détermination de r_1 par (b) est unique.

[7]) Bull. Amer. Math. Soc. 14, 1907—8, p. 313.

[8]) Periodico di Mat., 22, 1907, p. 36—41.

[9]) K. Petr, Časopis 66, (1937), p. 85—94.

Si le polynôme $f(x)$ possède (mod p) une décomposition en m facteurs irréductibles des degrés $l_1, l_2, \ldots, l_m$, l'équation caractéristique de la matrice $(c_{i,k})$ peut être écrite sous la forme

$$(-1)^n \cdot (\lambda^{l_1} - 1) \ldots (\lambda^{l_m} - 1),$$

c'est-à-dire, il est

$$\begin{vmatrix} c_{0,0} - \lambda, & c_{0,1}, & \ldots & c_{0,n-1} \\ c_{1,0}, & c_{1,1} - \lambda, & \ldots & c_{1,n-1} \\ \vdots & & & \\ c_{n-1,0}, & c_{n-1,1}, & \ldots & c_{n-1,n-1} - \lambda \end{vmatrix} \equiv (-1)^n \cdot (\lambda^{l_1} - 1) \ldots (\lambda^{l_m} - 1) \pmod{p}. \quad (3)$$

On voit aisément que sous la condition $p > n$ (mais aussi pour quelques autres cas) la décomposition à droite est déterminée d'une manière unique, c'est-à-dire, il n'existe pas deux décompositions de la forme $\prod_i (\lambda^{q_i} - 1)^{r_i}$ et $\prod_i (\lambda^{q_i'} - 1)^{r_i'}$, sauf le cas $q_i = q_i'$ et $r_i = r_i'$.[10])

Nous démontrerons tout d'abord

Lemme 1. *Le nombre des racines de la congruence* (1) *est donné par la relation*

$$r_1 \equiv c_{0,0} + c_{1,1} + \ldots + c_{n-1,n-1} \pmod{p}. \quad (4)$$

Démonstration. Soit r_k le nombre des facteurs irréductibles (mod p) du degré k. On peut alors mettre la décomposition de (3) sous la forme

$$(-1)^n \cdot (\lambda - 1)^{r_1} \cdot (\lambda^2 - 1)^{r_2} \cdot (\lambda^3 - 1)^{r_3} \ldots, \quad (4')$$

où

$$r_1 + 2r_2 + 3r_3 + \ldots = n. \quad (4'')$$

Le coefficient de λ^{n-1} dans le déterminant de (3) est

$$(-1)^{n-1} \cdot (c_{0,0} + c_{1,1} + \ldots + c_{n-1,n-1}).$$

De la décomposition (4'), qui peut être mise sous la forme

$$(-1)^n \{\lambda^{r_1} - \binom{r_1}{1} \lambda^{r_1-1} + \ldots\} (\lambda^2 - 1)^{r_2} \cdot (\lambda^3 - 1)^{r_3} \ldots,$$

on obtient pour le coefficient de $\lambda^{n-1} = \lambda^{(r_1-1)+2r_2+3r_3+\ldots}$ la valeur $(-1)^n \cdot -\binom{r_1}{1}$.

Alors

$$(-1)^{n-1} \cdot (c_{0,0} + c_{1,1} + \ldots + c_{n-1,n-1}) \equiv (-1)^n \cdot -\binom{r_1}{1} \pmod{p},$$

d'où la congruence (4) résulte.

[10]) Voir d'ailleurs l. c.[9]). Un exemple: pour $n = p$ il est $(\lambda^p - 1) \equiv (\lambda - 1)^p \pmod{p}$, pour $p = n - 1$ on a $(\lambda - 1)^n \equiv (\lambda^{n-1} - 1)(\lambda - 1)$ etc.; mais pour $p > n$ cela est impossible. Je rappelle que même dans les cas, où il existe plusieurs décompositions on peut donner au produit envisagé toujours la forme de (3).

Il nous faut alors trouver les expressions $c_{k,k}$ dans la relation (4).

Lemme 2. *Soit* (1) *la congruence donnée. Soient* s_k $(k=0, 1, 2, \ldots)$ *les sommes des puissances* k-ièmes *des solutions imaginaires de* (1).[11]) *Soit* $m > n$. *Construisons au moyen de la congruence* (1) — *en l'élevant successivement au puissances* $(n+1), (n+2) \ldots$ *et en réduisant les puissances* $> (n-1)$ *à l'aide de* (1) — *l'expression*

$$x^m \equiv c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \pmod{p}. \tag{5}$$

La congruence que nous avons ainsi obtenue

$$x^m - c_{n-1} x^{n-1} - c_{n-2} x^{n-2} - \ldots - c_0 \equiv 0 \pmod{p} \tag{6}$$

est de la forme

$$\frac{1}{D} \cdot \begin{vmatrix} s_0 & s_1 & \ldots & s_{n-1} & 1 \\ s_1 & s_2 & \ldots & s_n & x \\ \vdots & \vdots & & \vdots & \vdots \\ s_{n-1} & s_n & \ldots & s_{2n-2} & x^{n-1} \\ s_m & s_{m+1} & \ldots & s_{m+n-1} & x^m \end{vmatrix} \equiv 0 \pmod{p}. \tag{7}$$

Le déterminant

$$D = \begin{vmatrix} s_0 & s_1 & \ldots & s_{n-1} \\ s_1 & s_2 & \ldots & s_n \\ \vdots & \vdots & & \vdots \\ s_{n-1} & s_n & \ldots & s_{2n-2} \end{vmatrix} = \begin{vmatrix} s_{0,0} & s_{0,1} & \ldots & s_{0,n-1} \\ s_{1,0} & s_{1,1} & \ldots & s_{1,n-1} \\ \vdots & \vdots & & \vdots \\ s_{n-1,0} & s_{n-1,1} & \ldots & s_{n-1,n-1} \end{vmatrix}$$

est le discriminant de la congruence (1).

Démonstration. La congruence (5) resp. (6) est déterminée par la congruence (1) d'une manière unique. C'est une congruence de degré m à coefficients entiers, dans laquelle les coefficients de $x^{m-1}, x^{m-2}, \ldots, x^n$ sont égaux à zéro et qui est vérifiée (dans un élargissement convenable) par toutes les solutions de la congruence (1) de degré n. Il n'existe qu'une seule congruence de ce genre. Soient en effet dans la congruence (6), qui est de la forme considérée, les coefficients c_i $(i = 0, 1, \ldots, n-1)$ des grandeurs inconues. La condition que (6) soit vérifiée par toutes les imaginaires de Galois j_i $(i = 0, 1, \ldots, n-1)$ donne n congruences linéaires pour c_i.

$$c_0 + c_1 j_i + c_2 j_i^2 + \ldots + c_{n-1} j_i^{n-1} \equiv j_i^m \pmod{p} \quad (i = 1, 2, \ldots, n)$$

et en vertu de la supposition $D \not\equiv 0 \pmod{p}$ ce système a une solution et une seule. Pour démontrer alors que (6) et (7)

[11]) Il est alors $s_k \equiv j_1^k + j_2^k + \ldots + j_n^k \pmod{p}$. On sait que c'est un nombre entier.

sont identiques, il suffit de démontrer que chaque solution j_i $(i = 0, \ldots, n-1)$ de (1) vérifie la congruence (7). Il résulte d'abord de la congruence (5) pour les sommes s_k prises de la congruence (1)

$$s_{m+k} \equiv \sum_{i=0}^{n-1} c_i s_{i+k} \pmod{p} \tag{8}$$

pour chaque $k \geqq 0$. Posons dans (7) $x = j_i$ $(1 \leqq i \leqq n)$. En multipliant la première ligne par c_0, la seconde par c_1, etc. et en soustrayant de la dernière, on obtient — en vue de (5) et (8) — sur toutes les places dans la dernière ligne des zéros et alors (7) est égal à zéro, ce qu'il fallait démontrer.

Théorème 1. *Le nombre des racines de la congruence* (1) *vérifie la rélation*

$$r_1 \equiv \frac{1}{D}\left(D^{(0)} + D^{(1)} + \ldots + D^{(n-1)}\right) \pmod{p}, \tag{9}$$

où l'on obtient $D^{(k)}$ du discriminant D, si l'on y remplace les éléments de la $(k+1)$-ième ligne $(k = 0, \ldots, n-1)$ par les expressions $s_{kp}, s_{kp+1}, \ldots, s_{kp+n-1}$,[12]) *c'est à dire*[13])

$$D^{(k)} \equiv \begin{vmatrix} s_0, & s_1, & s_2, & \ldots, s_{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ s_{k-1}, & s_k, & s_{k+1}, & \ldots, s_{k+n-2} \\ s_{kp}, & s_{kp+1}, & s_{kp+2}, & \ldots, s_{kp+n-1} \\ s_{k+1}, & s_{k+2}, & s_{k+3}, & \ldots, s_{k+n} \\ \vdots & \vdots & \vdots & \vdots \\ s_{n-1}, & s_n, & s_{n+1}, & \ldots, s_{2n-2} \end{vmatrix} \pmod{p}.$$

Démonstration. Si l'on pose dans (7) $m = kp$ on obtient d'après le lemme 2 la relation (2). Le coefficient de x^k est

$$c_{k,k} \equiv -(-1)^{n-1+k+1} \cdot \frac{1}{D} \begin{vmatrix} s_0, & s_1, & \ldots, s_{n-1} \\ \vdots & \vdots & \vdots \\ s_{k-1}, & s_k, & \ldots, s_{k+n-2} \\ s_{k+1}, & s_{k+2}, & \ldots, s_{k+n} \\ \vdots & \vdots & \vdots \\ s_{kp}, & s_{kp+1}, & \ldots, s_{kp+n-1} \end{vmatrix} \equiv$$

$$\equiv (-1)^{n+k+1} \cdot \frac{1}{D} \cdot D_k \cdot (-1)^{n-1-k} \equiv \frac{D_k}{D} \pmod{p}.$$

En substituant cela en (4) on obtient la formule cherchée (9).

[12]) On trouve aisément $s_{kp} \equiv s_k \pmod{p}$ $(k = 0, 1, 2, \ldots)$. Cela vient du fait bien connu, que j_i^p est, en même temps que j_i, une solution de (1).

[13]) Dans notre notation $D^{(0)} = D$.

Remarques. 1. Pour $p > n$, la formule (9), comme nous l'avons remarqué sub [6]), détermine le nombre r_1 d'une manière unique.

2. Si l'on désigne par $D_{i,k}$ le mineur de D relatif à l'élément $s_{i,k}$, on peut écrire (9) dans une forme plus simple

$$r_1 \equiv \frac{1}{D} \sum_{\substack{k=0,1,\ldots n-1 \\ l=0,1,\ldots n-1}} s_{pk+l} D_{k,l} \pmod{p}. \tag{9'}$$

2. *Une autre démonstration de la formule* (9).

On peut vérifier maintenant la formule (9) d'une manière formelle plus simple. Nous nous servirons plusieurs fois de cette méthode dans ce qui suit.

Multiplions la relation (2) $x^{kp} \equiv \sum_{\nu=0}^{n-1} c_{k,\nu} x^\nu \pmod{p}$ par x^l; par l'addition des n relations de cette forme, où l'on pose successivement $x = j_1, j_2, \ldots, j_n$, on obtient

$$s_{kp+l} \equiv \sum_{\nu=0}^{n-1} c_{k,\nu} s_{\nu+l} \quad (k, l = 0, 1, \ldots, n-1). \tag{10}$$

On a

$$D^{(k)} \equiv \begin{vmatrix} \ldots & s_l & \ldots \\ \ldots & s_{l+1} & \ldots \\ & \vdots & \\ \ldots & s_{kp+l} & \ldots \\ & \vdots & \\ \ldots & s_{l+n-1} & \ldots \end{vmatrix} \equiv \begin{vmatrix} \ldots & s_l & \ldots \\ \ldots & s_{l+1} & \ldots \\ & \vdots & \\ \ldots & \sum_{\nu=0}^{n-1} c_{k,\nu} s_{\nu+l} & \ldots \\ & \vdots & \\ \ldots & s_{l+n-1} & \ldots \end{vmatrix}.$$

Si nous soustrayons de la $(k+1)$-ième ligne, la ligne $(i+1)$-ième multipliée par $c_{k,i}$, pour tous les $i \neq k$ le dernier déterminant se reduit à $c_{k,k} \cdot D$. Alors $D^{(k)} = c_{k,k} \cdot D$ et l'on obtient à l'aide de (4) la formule (9).

3. *La seconde formule pour le nombre des racines de la congruence* (1).

Outre le discriminant $D = |s_{i-1+k-1}| \begin{pmatrix} i = 1, \ldots, n \\ k = 1, \ldots, n \end{pmatrix}$ considérons le déterminant $d = |s_{(i-1)p+k-1}| \begin{pmatrix} i = 1, \ldots, n \\ k = 1, \ldots, n \end{pmatrix}$, c'est-à-dire

$$d = \begin{vmatrix} s_0 & s_1 & s_2 & \dots & s_{n-1} \\ s_p & s_{p+1} & s_{p+2} & \dots & s_{p+n-1} \\ s_{2p} & s_{2p+1} & s_{2p+2} & \dots & s_{2p+n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ s_{(n-1)p} & s_{(n-1)p+1} & s_{(n-1)p+2} & \dots & s_{(n-1)p+n-1} \end{vmatrix}.$$

Le déterminant d est en relation étroite avec le discriminant D. Il est en effet

$$d = \begin{vmatrix} s_0, & s_1, & \dots, & s_{n-1}, \\ s_p, & s_{p+1}, & \dots, & s_{p+n-1} \\ \vdots & \vdots & & \vdots \\ s_{(n-1)p}, & s_{(n-1)p+1}, & \dots, & s_{(n-1)p+n-1} \end{vmatrix} \equiv$$

$$\equiv \begin{vmatrix} 1, & 1, & \dots, & 1 \\ j_1, & j_2, & \dots, & j_n \\ \dots & \dots & \dots & \dots \\ j_1^{n-1}, & j_2^{n-1}, & \dots, & j_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1, & 1, & \dots, & 1, \\ j_1^p, & j_2^p, & \dots, & j_n^p \\ \dots & \dots & \dots & \dots \\ j_1^{(n-1)p}, & j_2^{(n-1)p} & \dots, & j_n^{(n-1)p} \end{vmatrix}$$

$$\equiv \begin{vmatrix} 1, & 1, & \dots, & 1, \\ j_1, & j_2, & \dots, & j_n \\ \vdots & \vdots & & \vdots \\ j_1^{n-1}, & j_2^{n-1}, & \dots, & j_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1, & 1, & \dots, & 1 \\ j_1, & j_2, & \dots, & j_n \\ \vdots & \vdots & & \vdots \\ j_1^{n-1}, & j_2^{n-1}, & \dots, & j_n^{n-1} \end{vmatrix}^p \equiv$$

$$\equiv | j_k^{i-1} |^{p+1} \equiv D^{\frac{p+1}{2}} \pmod p. \tag{11}$$

Pour obtenir la formule cherchée il nous faut comparer les coefficients de λ dans la relation (3).

On voit que dans l'expression

$$(-1)^n (\lambda - 1)^{r_1} . (\lambda^2 - 1)^{r_2} (\lambda^3 - 1)^{r_3} \dots =$$

$$= (-1)^n \{\lambda^{r_1} - \binom{r_1}{1} \lambda^{r_1 - 1} + \dots +$$

$$+ (-1)^{r_1 - 1} \binom{r_1}{1} \lambda + (-1)^{r_1}\} (\lambda^2 - 1)^{r_2} \dots$$

le coefficient de λ est égal au nombre

$$(-1)^n . (-1)^{r_1 - 1} \binom{r_1}{1} . (-1)^{r_2 + r_3 + \dots} =$$

$$= (-1)^{n+1} . r_1 . (-1)^{r_1 + r_2 + \dots} = (-1)^{n+v+1} . r_1,$$

si l'on désigne par v le nombre de tous les facteurs irréductibles de $f(x) \pmod p$.

Le coefficient de λ dans le déterminant à gauche de la relation (3) est donné par la somme négative de n mineurs princi-

paux de l'ordre $n-1$, c'est-à-dire — si l'on désigne par $C_{i,k}$ le mineur de la matrice $(c_{i,k})$ relatif à l'élément $c_{i,k}$ —

$$-(C_{0,0}+C_{1,1}+\ldots+C_{n-1,n-1}).$$

Alors

$$(-1)^{n+v}\,.\,r_1 \equiv C_{0,0}+C_{1,1}+\ldots+C_{n-1,n-1} \pmod p. \quad (12)$$

Les nombres $C_{i,i}$ sont de nouveau en relation étroite avec d resp. D. Soit $d^{(k)}$ le déterminant formé du déterminant d, si l'on y remplace les éléments de la $(k+1)$-ième ligne par les éléments $s_k, s_{k+1}, \ldots$ $\ldots, s_{k+n-1}$. D'après la formule (10) on a

$$d^{(k)} = \begin{vmatrix} s_0, & s_1, & \ldots, s_{n-1} \\ \vdots & \vdots & \vdots \\ s_{p(k-1)}, & s_{p(k-1)+1}, & \ldots, s_{p(k-1)+n-1} \\ s_k, & s_{k+1}, & \ldots, s_{k+n-1} \\ s_{p(k+1)}, & s_{p(k+1)+1}, & \ldots, s_{p(k+1)+n-1} \\ \vdots & \vdots & \vdots \\ s_{pn} & s_{pn+1} & \ldots, s_{pn+n-1} \end{vmatrix} \equiv$$

$$\equiv \begin{vmatrix} \sum_{v=0}^{n-1} c_{0,v}s_v, & \sum_{v=0}^{n-1} c_{0,v}s_{v+1}, \ldots, & \sum_{v=0}^{n-1} c_{0,v}s_{v+n-1} \\ \vdots & \vdots & \vdots \\ \sum_{v=0}^{n-1} c_{k-1,v}s_v, & \sum_{v=0}^{n-1} c_{k-1,v}s_{v+1}, \ldots, & \sum_{v=0}^{n-1} c_{k-1,v}s_{v+n-1} \\ s_k, & s_{k+1}, \ldots, & s_{k+n-1} \\ \sum_{v=0}^{n-1} c_{k+1,v}s_v, & \sum_{v=0}^{n-1} c_{k+1,v}s_{v+1}, \ldots, & \sum_{v=0}^{n-1} c_{k+1,v}s_{v+n-1} \\ \vdots & \vdots & \vdots \\ \sum_{v=0}^{n-1} c_{n-1,v}s_v, & \sum_{v=0}^{n-1} c_{n-1,v}s_{v+1}, \ldots, & \sum_{v=0}^{n-1} c_{n-1,v}s_{v+n-1} \end{vmatrix}.$$

Pour obtenir la relation énoncée on doit soustraire de la ligne $(i+1)$-ième la ligne $(k+1)$-ième multipliée par $c_{i,k}$ (pour tous les $i \neq k$). Développons le déterminant ainsi transformé suivant les éléments de la $(k+1)$-ième ligne. On a

$$s_k\,.\,S_{k,0}+s_{k+1}S_{k,1}+\ldots+s_{k+n-1}S_{k,n-1},$$

où $S_{k,l}$ désigne le mineur du déterminant considéré relatif à l'élément s_{k+l}. Mais chaque $S_{k,l}$ est un produit de deux déterminants: du déterminant $C_{k,k}$ et du déterminant $D_{k,l}$ (mineur du déterminant D relatif à l'élément $s_{k,l}$). Alors

$$d_k \equiv s_k S_{k,0} + \ldots + s_{k+n-1} S_{k,n-1} \equiv C_{k,k} (s_k D_{k,0} + s_{k+1} D_{k,1} + \ldots + s_{k+n-1} D_{k,n}) \equiv C_{k,k} . D \pmod{p}.$$

En substituant cette expression dans (12) on a enfin:

Théorème 2. *Le nombre des racines de la congruence* (1) r_1 *et le nombre de tous les facteurs irréductibles v sont liés par la relation*

$$r_1 \equiv (-1)^{n+v} \frac{1}{D} (d^{(0)} + d^{(1)} + \ldots + d^{(n-1)}) \pmod{p}, \quad (13)$$

où D est le discriminant de (1) *et* $d^{(k)}$ *est le déterminant formé de d si l'on y remplace les éléments de la* $(k+1)$*-ième ligne par* $s_k, s_{k+1}, \ldots, s_{k+n-1}$.

Remarque. Soit $d_{k,l}$ le mineur de d rélatif à l'élément s_{kp+l}; avec cette notation on peut écrire (13) sous la forme plus simple

$$r_1 \equiv (-1)^{n+v} \frac{1}{D} \cdot \sum_{\substack{k=0,1,\ldots n-1 \\ l=0,1,\ldots n-1}} s_{k+l} d_{k,l} \pmod{p}.$$

4. *Les coefficients du polynôme* (4').

On voit maintenant la voie, qui nous rend possible de calculer les nombres $r_2, r_3, \ldots$ etc. Il nous faut déterminer d'abord les coefficients du polynôme (4').

Soit

$$(-1)^n . (\lambda - 1)^{r_1} (\lambda^2 - 1)^{r_2} \ldots = \tau_n \lambda^n + \tau_{n-1} \lambda^{n-1} + \ldots + \tau_1 \lambda + \tau_0 \quad (14)$$

$$r_1 + 2r_2 + 3r_3 + \ldots = n.$$

Il est

$$\tau_n = (-1)^n, \ \tau_0 = (-1)^{n+v}.$$

Dans 1 et 3 nous avons trouvé

$$\tau_{n-1} = (-1)^{n+1} \binom{r_1}{1}, \quad \tau_1 = (-1)^{n+v+1} \binom{r_1}{1}.$$

Pour trouver τ_2 écrivons (14) sous la forme

$$(-1)^n \left\{ \lambda^{r_1} - \ldots + (-1)^{r_1-1} \binom{r_1}{1} \lambda + (-1)^{r_1} \right\} .$$

$$\left\{ \lambda^{2r_2} - \ldots + (-1)^{r_2-1} \binom{r_2}{1} \lambda^2 + (-1)^{r_2} \right\} (\lambda^3 - 1)^{r_3} \ldots$$

et il s'ensuit

$$\tau_2 = (-1)^{n+r_2+r_4+\ldots} \left\{ (-1)^{r_1-2} \binom{r_1}{2} (-1)^{r_2} + (-1)^{r_1} . (-1)^{r_2-1} \binom{r_2}{1} \right\} = (-1)^{n+v} . \left\{ -\binom{r_2}{1} + \binom{r_1}{2} \right\}.$$

D'une manière analogue on obtient

$$\tau_3 = (-1)^{n+v}\left\{-\binom{r_3}{1} + \binom{r_2}{1}\binom{r_1}{1} - \binom{r_1}{3}\right\},$$

$$\tau_4 = (-1)^{n+v}\left\{-\binom{r_4}{1} + \binom{r_3}{1}\binom{r_1}{1} + \binom{r_2}{2} + \binom{r_1}{4}\right\}$$

et par l'induction

$$\tau_k = (-1)^{n+v}\sum (-1)^{k_1+k_2+\ldots+k_l}\binom{r_{i_1}}{k_1}\binom{r_{i_2}}{k_2}\ldots\binom{r_{i_l}}{k_l},$$

la somme se rapportant à toutes les solutions entières, non-négatives de l'équation $i_1k_1 + i_2k_2 + \ldots + i_lk_l = k$, où $i_1 \neq i_2 \neq i_3 \ldots$

Le polynôme (4') est évidemment réciproque, par conséquent, il en résulte immédiatement la relation

$$\tau_{n-k} = (-1)^v \tau_k \text{ (pour chaque } k = 1, 2, \ldots). \qquad (15)$$

5. *Détermination du nombre des facteurs irréductibles du second degré de la congruence* (1).

Le coefficient de λ^2 dans le polynôme (4') est

$$\tau_2 = (-1)^{n+v}\cdot\left\{-\binom{r_2}{1} + \binom{r_1}{2}\right\}. \qquad (15')$$

D'après (15) le coefficient de λ^{n-2} est

$$\tau_{n-2} = (-1)^v \tau_2 = (-1)^n\cdot\left\{-\binom{r_2}{1} + \binom{r_1}{2}\right\}.$$

Nous obtiendrons comme précédemment deux formules.

a)

Dans le déterminant caractéristique (3) le coefficient de λ^{n-2} est égal à la somme de tous les mineurs principaux du seconde degré, qui sont au nombre $\binom{n}{2}$, alors

$$\tau_{n-2} \equiv (-1)^{n-2}\sum_{\substack{i=0,\ldots,n-2\\ k=1,\ldots n-1\\ i<k}}\begin{vmatrix} c_{i,i} & c_{i,k} \\ c_{k,i} & c_{k,k}\end{vmatrix} \pmod p. \qquad (16)$$

Mais on peut exprimer, comme précédemment, ces déterminants à l'aide du discriminant D. Soit $D^{(i,k)}$ le déterminant formé de D si l'on y remplace les éléments de la $(i+1)$-ième ligne par les nombres $s_{ip}, s_{ip+1}, \ldots, s_{ip+n-1}$ et les éléments de la $(k+1)$-ième ligne par $s_{kp}, s_{kp+1}, \ldots, s_{kp+n-1}$. On a

$$D^{(i,k)} = \begin{vmatrix} s_0 & s_1 & \dots & s_{n-1} \\ \vdots & \vdots & & \vdots \\ s_{ip} & s_{ip+1} & \dots & s_{ip+n-1} \\ \vdots & \vdots & & \vdots \\ s_{kp} & s_{kp+1} & \dots & s_{kp+n-1} \\ \vdots & \vdots & & \vdots \\ s_{n-1} & s_n & \dots & s_{2n-2} \end{vmatrix}. \qquad (17)$$

Remplaçons les éléments $s_{ip}, \dots, s_{kp}, \dots$, par les sommes (10). Multiplions dans le déterminant ainsi obtenu la première ligne par $c_{i,0}$, la seconde par $c_{i,1}$ etc. [excepté la ligne $(i+1)$-ième et $(k+1)$-ième] et soustrayons de la ligne $(i+1)$-ième, puis multiplions la première ligne par $c_{k,0}$, la deuxième par $c_{k,1}$ etc. et soustrayons de la ligne $(k+1)$-ième.

Nous développons maintenant ce nouveau déterminant d'après la règle de Laplace, suivant les lignes $(i+1)$-ième et $(k+1)$-ième. On a

$$D^{(i,k)} \equiv \sum \begin{vmatrix} c_{i,i}s_l + c_{i,k}s_q, & c_{i,i}s_r + c_{i,k}s_t \\ c_{k,i}s_l + c_{k,k}s_q, & c_{k,i}s_r + c_{k,k}s_t \end{vmatrix} . S_{\binom{l,q}{r,t}},$$

où $S_{\binom{l,q}{r,t}}$ est le sous-déterminant complémentaire de $\begin{vmatrix} s_l & s_q \\ s_r & s_t \end{vmatrix}$ dans D.

$$D^{(i,k)} \equiv \begin{vmatrix} c_{i,i} & c_{i,k} \\ c_{k,i} & c_{k,k} \end{vmatrix} . \sum \begin{vmatrix} s_l, & s_q \\ s_r, & s_t \end{vmatrix} . S_{\binom{l,q}{r,t}} \equiv \begin{vmatrix} c_{i,i}, & c_{i,k} \\ c_{k,i}, & c_{k,k} \end{vmatrix} . D.$$

D'après (16)

$$\tau_{n-2} \equiv (-1)^{n-2} \sum_{\substack{i=0,\dots n-2 \\ k=1,\dots n-1 \\ i<k}} \frac{D^{(i,k)}}{D} \equiv (-1)^n \left\{ -\binom{r_2}{1} + \binom{r_1}{2} \right\} \pmod{p}.$$

Enfin nous obtenons

Théorème 3. *Le nombre des facteurs irréductibles du second degré de la congruence* (1) r_2 *est donné par la formule*

$$-r_2 + \binom{r_1}{2} \equiv \frac{1}{D} \sum_{\substack{i=0,\dots n-2 \\ k=1,\dots n-2 \\ i<k}} D^{(i,k)} \pmod{p},$$

où r_1 *est le nombre des facteurs linéaires,* D *le discriminant de la congruence donée et la somme se rapporte à* $\binom{n}{2}$ *déterminants* $D^{(i,k)}$ *de la forme* (17).

b)

Dans le déterminant caractéristique (3) le coefficient de λ^2 est égal à la somme de tous les mineurs principaux de la matrice

$(c_{i,k})$ de degré $n-2$. On détermine ces sous-déterminants de la manière suivante. Attribuons à la lettre $d^{(i,k)}$ une signification analogue à celle de $D^{(i,k)}$, c'est à dire $d^{(i,k)}$ soit le déterminant formé de d, si l'on y remplace les éléments de la $(i+1)$-ième ligne par $s_i, s_{i+1}, \ldots$ et les éléments de la $(k+1)$-ième ligne par $s_k, s_{k+1}, \ldots$ Nous portons les valeurs correspondantes d'après la formule (10) dans toutes les lignes du déterminant $d^{(i,k)}$ excepté les lignes $(i+1)$-ième et $(k+1)$-ième. Puis nous soustrayons des autres lignes un multiple convenable des lignes $(i+1)$-ième et $(k+1)$-ième. On peut écrire le déterminant, qu'on obtient ainsi, comme produit de deux déterminants, du discriminant D et du sous-déterminant principal d'ordre $n-2$, qui est complémentaire au sous-déterminant $\begin{vmatrix} c_{i,i} & c_{i,k} \\ c_{k,i} & c_{k,k} \end{vmatrix}$ du déterminant $|c_{i,k}|$. Le coefficient de λ^2 est alors

$$\frac{1}{D} \sum_{\substack{i=0,\ldots n-2 \\ k=1,\ldots n-1 \\ i<k}} d^{(i,k)}.$$

Tenant compte de (15′) on a

Théorème 4. *Le nombre des facteurs irréductibles de la congruence* (1) *v, le nombre des facteurs linéaires* r_1 *et le nombre des facteurs du seconde degré* r_2 *sont liés par la relation*

$$-r_2 + \binom{r_1}{2} \equiv (-1)^{n+v} \cdot \frac{1}{D} \sum d^{(i,k)} \pmod{p},$$

où la somme se rapporte à toutes les $\binom{n}{2}$ *combinaisons des* i, k $(i \neq k)$.

6. *Le résultat général.*

Il est maintenant facile de généraliser les résultats que nous avons obtenus. Tenant compte des résultats de 4 on peut énoncer le

Théorème 5. *Soit* k *un nombre entier,* $0 < k \leqq n$; *soit* $r_\varkappa$ $(\varkappa = 1, 2, \ldots, n)$ *le nombre des facteurs irréductibles de la congruence* (1) *de degré* $\varkappa$. *Soit* v *le nombre de tous les facteurs irréductibles. Désignons par* $D^{(\lambda_1, \lambda_2, \ldots \lambda_k)}$ *le déterminant formé du discriminant* D, *si l'on y remplace les lignes* (λ_1+1)-*ième,* (λ_2+1)-*ième,* $\ldots$, (λ_k+1)-*ième par les éléments* $s_{\lambda_1 p}, s_{\lambda_1 p+1}, \ldots, s_{\lambda_1 p+n-1}$, *etc. Par analogie désignons par* $d^{(\lambda_1, \lambda_2, \ldots, \lambda_k)}$ *le déterminant formé de* d, *si l'on y remplace les lignes* (λ_1+1)-*ième etc. par les éléments* $s_{\lambda_1}, s_{\lambda_1+1}, \ldots, s_{\lambda_1+n-1}$ *etc.*

Entre les grandeurs ainsi définies les rélations suivantes ont lieu

$$\sum_{\substack{i_1 k_1 + \ldots + i_l k_l = k \\ i_1 \neq i_2 \neq i_3 \ldots}} (-1)^{k_1 + \ldots + k_l} \binom{r_{i_1}}{k_1} \ldots \binom{r_{i_l}}{k_l} \equiv (-1)^k \cdot \frac{1}{D} \cdot \sum D^{(\lambda_1, \lambda_2 \ldots \lambda_k)} \pmod{p}, \quad (18)$$

$$\sum_{\substack{i_1k_1+\ldots+i_lk_l=k \\ i_1\neq i_2\neq i_3\ldots}} (-1)^{k_1+\ldots+k_l}\binom{r_{i_1}}{k_1}\ldots\binom{r_{i_l}}{k_l} \equiv (-1)^{n+v+k}\cdot\frac{1}{D}\sum d^{(\lambda_1,\lambda_2,\ldots\lambda_k)} \pmod p, \quad (19)$$

où la somme à droite se rapporte à toutes les $\binom{n}{k}$ *combinaisons de la k-ième classe des nombres* $1, 2, \ldots, n$.

Les formules (18), (19) peuvent être considérées comme des relations recurrentes; en effet, si l'on y pose $k = 1, 2, 3, \ldots$, on détermine successivement $r_1, r_2, r_3, \ldots$

Applications.

a) La congruence quadratique.

Soit $x^2 + ax + b \equiv 0 \pmod p$ la congruence donnée.

D'après (9) on a pour le nombre des racines

$$r_1 \equiv \frac{1}{\begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix}}\cdot\left\{\begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix} + \begin{vmatrix} s_0 & s_1 \\ s_p & s_{p+1} \end{vmatrix}\right\} \pmod p.$$

$$r_1 \equiv 1 + \frac{\begin{vmatrix} s_0 & s_1 \\ s_p & s_{p+1} \end{vmatrix}}{\begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix}} \equiv 1 + \frac{\begin{vmatrix} 1 & 1 \\ j_1^p & j_2^p \end{vmatrix}\cdot\begin{vmatrix} 1 & 1 \\ j_1 & j_2 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ j_1 & j_2 \end{vmatrix}^2} \equiv 1 + \frac{\begin{vmatrix} 1 & 1 \\ j_1 & j_2 \end{vmatrix}^p}{\begin{vmatrix} 1 & 1 \\ j_1 & j_2 \end{vmatrix}} \equiv$$

$$\equiv 1 + \begin{vmatrix} 1 & 1 \\ j_1 & j_2 \end{vmatrix}^{p-1} \pmod p.^{14})$$

Donc, pour $p > 2$: $r_1 \equiv 1 + D^{\frac{p-1}{2}} \equiv 1 + \left(\frac{D}{p}\right) \pmod p$.

Pour $p = 2$: $r_1 \equiv 1 + j_2 - j_1 \equiv 1 + j_1 + j_2 \equiv 1 + a \pmod 2$.[15])

C'est un résultat bien connu.

Théorème 6. *La congruence* $x^2 + ax + b \equiv 0 \pmod p$, $p > 2$ *a deux ou n'a aucune racine suivant qu'il est* $\left(\frac{D}{p}\right) = 1$ *ou* $\left(\frac{D}{p}\right) = -1$, *où D est le discriminant de la congruence donnée et* $\left(\frac{D}{p}\right)$ *le symbole de Legendre.*

b) La congruence cubique.[16])

[14]) Quant à la signification de j_1, j_2, voir 1.

[15]) (Mod 2) il n'existe que deux congruences avec $D \not\equiv 0 \pmod 2$; ce sont $x^2 + x + 1 \equiv 0$, $x^2 + x \equiv 0$; on y vérifie aisément notre résultat.

[16]) On trouve chez Dickson l. c. [2]) p. 252—256 tous les résultats connus pour la congruence cubique. Quelques de ces résultats sont contenus en (21).

Soit

$$x^3 + ax^2 + bx + c \equiv 0 \pmod{p} \tag{20}$$

la congruence donnée. D'après (9) on a

$$r_1 \equiv \frac{1}{D} \cdot \left\{ \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} + \begin{vmatrix} s_0 & s_1 & s_2 \\ s_p & s_{p+1} & s_{p+2} \\ s_2 & s_3 & s_4 \end{vmatrix} + \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_{2p} & s_{2p+1} & s_{2p+2} \end{vmatrix} \right\} \pmod{p}. \tag{21}$$

D'après (13) on obtient aussi

$$r_1 \equiv (-1)^{3+v} \cdot \frac{1}{D} \left\{ \begin{vmatrix} s_0 & s_1 & s_2 \\ s_p & s_{p+1} & s_{p+2} \\ s_{2p} & s_{2p+1} & s_{2p+2} \end{vmatrix} + \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_{2p} & s_{2p+1} & s_{2p+2} \end{vmatrix} + \right.$$

$$\left. + \begin{vmatrix} s_0 & s_1 & s_2 \\ s_p & s_{p+1} & s_{p+2} \\ s_2 & s_3 & s_4 \end{vmatrix} \right\} \pmod{p}, \tag{21'}$$

$v = r_1 + r_2 + r_3$.

On peut trouver facilement de ces deux expressions pour r_1 une relation intéressante entre le nombre des racines de la congruence (20) et le caractère quadratique du discriminant D.

La somme du deuxième et du troisième déterminant dans (21) est égale à la même somme dans (21'). Nous la désignons par δ; alors — tenant compte de (11) — on a

$$r_1 \cdot D \equiv D + \delta$$

$$r_1 \cdot D \cdot (-1)^{3+v} \equiv D^{\frac{p+1}{2}} + \delta \pmod{p}.$$

En éliminant δ on obtient

$$r_1 \cdot [1 - (-1)^{3+r_1+r_2+r_3}] \equiv 1 - D^{\frac{p-1}{2}} \pmod{p}. \tag{22}$$

Ici seulement trois cas existent

$\alpha)$ $r_3 = 1$, $r_2 = r_1 = 0$, il suit de (22) $\left(\frac{D}{p}\right) = +1$,

$\beta)$ $r_3 = 0$, $r_2 = r_1 = 1$, il suit de (22) $\left(\frac{D}{p}\right) = -1$,

$\gamma)$ $r_3 = 0$, $r_2 = 0$, $r_1 = 3$, il suit de (22) $\left(\frac{D}{p}\right) = 1$.

Il s'ensuit

Théorème 7. *Si la congruence cubique* (20) *possède trois ou ne possède aucune racine, le discriminant de cette congruence D est*

résidu quadratique (mod p). *Au contraire, si* (20) *n'a qu' une racine, D est non-résidu quadratique* (mod p).[17])

c) La théorie des congruences binomes.

On obtient de la formule (9) par des considérations simples toute la théorie des congruences binomes.

Posons la question quel est le nombre des racines r_1 de la congruence

$$x^n - a \equiv 0, \; n < p \pmod{p}. \tag{23}$$

Il suit de (23) que $s_0 = n, s_1 = s_2 = \ldots = s_{n-1} = 0, \; s_n = an$; de manière plus générale $s_k = a^\tau n$, pour $k = n\tau$, τ entier; $s_k = 0$, pour les autres k.

$$D = \begin{vmatrix} n & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & s_n \\ \vdots & & & & & \\ 0 & 0 & s_n & \ldots & 0 & 0 \\ 0 & s_n & 0 & \ldots & 0 & 0 \end{vmatrix} = (-1)^{\frac{(n-1)(n-2)}{2}} . n . (an)^{n-1}.$$

Posons $D_k = D^{(k)}$. Le déterminant D_k ne diffère du discriminant D que par la propriété, que la $(k+1)$-ième ligne contient les éléments $s_{kp}, s_{kp+1}, \ldots, s_{kp+n-1}$. Soit $k > 0$ (pour $k = 0, D_0 = D$). Parmi les n nombres entiers $kp, kp+1, \ldots, kp+n-1$ il y a un et seulement un qui est divisible par n. Si le nombre s_l de la $(k+1)$-ième ligne avec l'indice l divisible par n ne se trouve pas dans le déterminant D_k sur la même place, où se trouve dans D la somme s_n, il est clair, qu'un tel D_k est égal à zéro.

L'élément de la $(k+1)$-ième ligne, qui se trouve dans D_k sur la place occupée par s_n dans D est

$$s_{kp+n-k}.$$

Autrement dit, le déterminant D_k ne sera différent de nul, que pour les k, pour lesquels

$$kp + n - k \equiv 0 \pmod{n}.$$
$$k . (p-1) \equiv 0 \pmod{n}.$$

Posons $\delta = (p-1, n)$, les nombres k cherchés sont alors

$$0, \frac{n}{\delta}, 2\frac{n}{\delta}, \ldots, (\delta - 1)\frac{n}{\delta}.$$

[17]) Ce théorème est bien connu. On voit dans la littérature que ce théorème a été plusiers fois démontré; récemment par M. Th. Skolem, Norske Vid. Selsk. Forh. 10, p. 89—92, 1937 [Voir Zentralblatt 18, 1938, p. 343]. Il est aussi une conséquence du théorème 9 que nous démontrerons dans ce qui suit.

Au nombre $l \cdot \frac{n}{\delta}$ correspond

$$s_{l.\frac{n}{\delta}p+n-l.\frac{n}{\delta}} = s_{\left\{l.\frac{p-1}{\delta}+1\right\}n} = n \cdot a^{l.\frac{p-1}{\delta}+1}.$$

Le déterminant D_k correspondant au nombre $k = l \cdot \frac{n}{\delta}$ est alors

$$D_{l.\frac{n}{\delta}} = (-1)^{\frac{(n-1)(n-2)}{2}} n \cdot (an)^{n-2} \cdot n \cdot a^{l.\frac{p-1}{\delta}+1}.$$

Le nombre des racines de la congruence (23) est donné par

$$r_1 \equiv \frac{1}{(-1)^{\frac{(n-1)(n-2)}{2}} n\,(an)^{n-1}} \cdot \sum_{l=0}^{\delta-1} (-1)^{\frac{(n-1)(n-2)}{2}} n\,(an)^{n-2} \cdot$$

$$\cdot n \cdot a^{l.\frac{p-1}{\delta}+1} \pmod{p}.$$

$$r_1 \equiv \sum_{l=0}^{\delta-1} a^{l.\frac{p-1}{\delta}} \pmod{p}. \qquad (24)$$

Soit $a^{\frac{p-1}{\delta}} \not\equiv 1 \pmod{p}$. La somme à droite est la somme d'une série géometrique

$$r_1 \equiv \frac{a^{p-1} - 1}{a^{\frac{p-1}{\delta}} - 1} \equiv 0 \pmod{p}.$$

La congruence (23) n'a pas des racines.

Soit $a^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$. En ce cas, il résulte directement de (24)

$$r_1 \equiv \sum_{l=0}^{\delta-1} \left(a^{\frac{p-1}{\delta}}\right)^l \equiv \sum_{l=0}^{\delta-1} 1 \equiv \delta \pmod{p}.$$

Alors, nous avons démontré le

Théorème 8. *La condition nécessaire et suffisante pour que la congruence* (23) *admette des racines est qu'on ait*

$$a^{\frac{p-1}{\delta}} \equiv 1 \pmod{p},$$

où $\delta = (p-1, n)$. *Cette condition étant satisfaite la congruence* (23) *a exactement* δ *racines.*[18])

[18]) Notre démonstration du théorème 8 est intéressante aussi au point de vue méthodique. La théorie classique des congruences binomes est basée sur la théorie des indices, mais — comme on voit — dans notre déduction nous n'avons pas eu besoin de cette théorie.

d) **Théorème 9.** (La formule de Pellet-Voronoï-Stickelberger).[19]) *Le nombre v des facteurs irréductibles* (mod p) *de la congruence* (1) *à discriminant* $D \not\equiv 0 \pmod{p}$, *vérifie l'équation*

$$\left(\frac{D}{p}\right) = (-1)^{n+v},$$

où $\left(\frac{D}{p}\right)$ *est le symbole de Legendre.*

Démonstration. Il résulte des formules (18) et (19) du théorème 5 que pour chaque k, $(0 < k \leqq n)$

$$(-1)^k \cdot \frac{1}{D} \sum D^{(\lambda_1,\ldots,\lambda_k)} \equiv (-1)^{n+v+k} \frac{1}{D} \cdot \sum d^{(\lambda_1,\ldots,\lambda_k)} \pmod{p}$$

$$\sum D^{(\lambda_1,\ldots,\lambda_k)} \equiv (-1)^{n+v} \sum d^{(\lambda_1,\ldots,\lambda_k)}.$$

Posons $k = n$; on a:

$$D^{(\lambda_1,\ldots,\lambda_n)} = D^{(0,1,2,\ldots,n-1)} \equiv d \pmod{p},$$

$$d^{(\lambda_1,\ldots,\lambda_n)} = d^{(0,1,\ldots,n-1)} \equiv D \pmod{p}.$$

Alors $$d \equiv (-1)^{n+v} \cdot D \pmod{p}.$$

Tenant compte de (11), on a

$$D^{\frac{p+1}{2}} \equiv (-1)^{n+v} \cdot D$$

$$\left(\frac{D}{p}\right) = (-1)^{n+v}, \text{ c. q. f. d.}$$

*

O počtu koreňov a nerozložiteľných faktorov danej kongruencie.

(Obsah predošlého článku.)

Nech je daná kongruencia $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}$. Koreňom takejto kongruencie budeme volať celé číslo x_i, ktoré tejto kongruencii vyhovuje. Označme počet nerozložiteľných faktorov danej kongruencie stupňa k-tého znakom r_k; počet koreňov je teda r_1. Konečne nech značí D diskriminant poly-

[19]) Pellet: Comptes Rendus, 1878, p. 1071—2. — Voronoi: Verhandl. d. III. Math. Kongress, Heidelberg (Leipzig 1904). Cette formule a été récemment trouvé de nouveau par M. S. Lubelski, Acta Aritmetica 1, p. 169—183, (1935). — Voir aussi: K. Hensel, Crelles Journal 129, 1905, p. 68—86 et Hensel-Mirimanoff ibid p. 87—88, où les auteurs donnent à l'aide de ce théorème une démonstration extraordinairement simple de la loi de réciprocité.

nomu $f(x)$ a v počet všetkých irreducibilných faktorov všetkých stupňov.

V článku sme dokázali: Pre počeť koreňov r_1 platí vzťah (9), alebo analogický vzťah (13). Rovnako pre r_k najdeme dva rekurrentné vzťahy (18) a (19), z ktorých možno $r_2, r_3, \ldots$ po rade vypočítať.

V druhej čiasti podali sme niekoľko aplikácií výsledkov, ktoré sme obdržali. A to predovšetkým na kvadratickú a kubickú kongruenciu; potom sme na niekoľkých riadkach odvodili celú teoriu binomických kongruencií a na koniec sme dokázali vzťah vyslovený vo vete 9. týkajúci sa kvadratického charakteru diskriminantu polynomu $f(x)$.

*

Über die Anzahl der Wurzeln und der irreduziblen Faktoren einer gegebenen Kongruenz.

(Auszug aus dem vorstehenden Artikel.)

Die vorgelegte Kongruenz sei

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}.$$

Als Wurzel dieser Kongruenz wird jede ganze Zahl x_i bezeichnet, welche dieser Kongruenz genügt. Die Anzahl der irreduziblen Faktoren der gegebenen Kongruenz vom Grad k werde mit r_k bezeichnet; also ist r_1 die Anzahl der Wurzeln. Endlich sei D die Diskriminante von $f(x)$ und v die Anzahl aller irreduziblen Faktoren überhaupt.

Im Artikel wurde bewiesen: Für die Anzahl der Wurzeln r_1 gilt die Beziehung (9), oder die analoge Beziehung (13). Ebenso findet man für r_k zwei rekurrente Beziehungen (18), (19), aus welchen man der Reihe nach $r_2, r_3, \ldots$ berechnen kann.

Im zweiten Teile haben wir einige Anwendungen der erhaltenen Resultate gegeben, und zwar zunächst auf die quadratische und kubische Kongruenz; dann haben wir auf einigen Zeilen die Theorie der binomischen Kongruenzen abgeleitet und endlich haben wir im Satz 9 eine Beziehung abgeleitet, welche den quadratischen Charakter der Diskriminante von $f(x)$ betrifft.