BULLETIN DE LA S. M. F.

PIERRE BOOS

Divisibilité des polynômes relativement aux puissances d'un nombre entier

Bulletin de la S. M. F., tome 76 (1948), p. 65-78

<http://www.numdam.org/item?id=BSMF_1948__76__65_0>

DIVISIBILITÉ DES POLYNOMES RELATIVEMENT AUX PUISSANCES D'UN NOMBRE ENTIER;

PAR M. PIERRE BOOS.

Nous nous proposons d'étudier des congruences dont le module est une puissance du premier coefficient d'un polynome g à coefficients entiers auxquelles satisfont identiquement des polynomes à coefficients entiers.

1. Nous examinons d'abord le cas où

$$g(x) = px^n + ax^{n-1} + a_2 x^{n-2} + \dots,$$

avec a premier avec p (a peut être égal à l'unité).

Quel que soit l'entier k, il existe des polynomes $u_k(x)$ de degré k tels que le produit $g(x)\,u_k(x)$ soit congru mod p^{k+1} à un polynome $v_k(x)$ de degré $n-1$ dans lequel le coefficient de x^{n-1} est premier avec p.

Quand $k = 0$, il suffit manifestement de prendre $u_0 = 1$, le terme de plus haut degré dans v est alors ax^{n-1}.

Supposons qu'on ait trouvé un polynome $u_{k-1} = p^{k-1}x^{k-1} + \dots$ tel que le produit $g\,u_{k-1}$ soit congru mod p^k au polynome v_{k-1} égal à $bx^{n-1} + b'x^{n-2} + \dots$ dans lequel b est premier avec p et montrons que le polynome $U = px\,u_{k-1}(x) - b$ est un polynome u_k. En effet le produit gU est congru mod p^{k+1} à $(pb' - ab)x^{n-1} + \dots$ qui est bien un polynome v puisque $pb' - ab$ est premier avec p comme a et b.

Nous avons donc un procédé qui permet de calculer de proche en proche des polynomes u_k et v_k correspondant aux valeurs croissantes de l'indice; nous remarquons que les polynomes u_k ainsi obtenus sont des polynomes en px dans lesquels le terme indépendant et les coefficients sont premiers avec p.

2. *Deux polynomes u_k et u'_k de même indice sont liés par une congruence*

$$u'_k + \theta u_k \equiv 0 \pmod{p^{k+1}},$$

où θ est premier avec p. Réciproquement tout polynome congru à un produit θu_k est un polynome u'_k (θ premier avec p).

Pour démontrer cette propriété nous établissons d'abord par récurrence le lemme suivant : *Tout polynome $z_k(x)$ de degré au plus égal à k tel que le*

produit $g(x)z_k(x)$ soit congru mod p^{k+1} à un polynome de degré $n-2$ au plus est congru à zéro module p^{k+1} (et alors le produit $g z_k$ est aussi congru à zéro).

Ce résultat est évident si $k = 0$, car alors z_0 est une constante C et $g z_0$ congru (mod p) à $a\,C x^{n-1} + \ldots$ ne peut être congru à un polynome de degré $n-2$ au plus que si C est congru à o.

Supposons alors démontré que tout polynome z_k dont l'indice est inférieur à k, est nécessairement congru à zéro module p^{k+1} et soit z_k un polynome de degré k possédant la propriété indiquée. Si l'on désigne par $A'_k x^k$ le terme de plus haut degré de z_k, le terme de plus haut degré dans le produit $g z_k$ est $A'_k p x^{n+k}$ et il n'est congru à zéro mod p^{k+1} que si $A'_k = A_k p^k$; il en résulte que les k termes de plus bas degré de z_k forment un polynome z_{k-1}, donc d'après l'hypothèse les coefficients de ces termes sont tous divisibles par p^k et l'on peut écrire

$$z_k(x) = A_k p^k x^k + A_{k-1} p^k x^{k-1} + A_{k-2} p^k x^{k-2} + \ldots + A_j p^k x^j + \ldots + A_0 p^k.$$

On voit alors que dans le produit $g z_k$ le terme $(A_k a p^k + A_{k-1} p^{k+1}) x^{k+n-1}$ ne peut être congru à zéro mod p^{k+1} que si A_k est divisible par p. De proche en proche on montre que tous les A_j sont congrus à o mod p; en effet si l'on a démontré que dans z_k tous les coefficients des puissances de x supérieures à la $j^{\text{ième}}$ sont divisibles par p^{k+1}, le terme de degré $n+j-1$ dans le produit $g z_k$ est congru mod p^{k+1} à $a A_j p^k + A_{j-1} p^{k+1}$ et il ne peut être congru à o que si A_j est divisible par p. Il en résulte que z_k est bien congru à zéro mod p^{k+1}.

Cela étant soit u_k et u'_k deux polynomes de degré k tels que

$$g(x)u_k(x) \equiv b\,x^{n-1} + b_1\,x^{n-2} + \ldots \quad (\text{mod } p^{k+1}),$$
$$g(x)u'_k(x) \equiv b'x^{n-1} + b'_1 x^{n-2} + \ldots \quad (\text{mod } p^{k+1}).$$

Comme b et b' sont premiers avec p, il existe un nombre θ, premier avec p, tel que $b' + \theta b \equiv 0 \bmod p^{k+1}$, dès lors

$$g(x)[u'_k(x) + \theta u_k(x)] \equiv (b'_1 + \theta b_1)x^{n-2} + \ldots \quad (\text{mod } p^{k+1}),$$

et d'après le lemme, $u'_k + \theta u_k$ qui est au plus de degré k est congru à zéro; les polynomes v correspondants vérifient la même relation.

La réciproque est évidente car si $u' \equiv \theta u_k \bmod p^{k+1}$, on a

$$g u' \equiv \theta g u_k \equiv \theta v_k \quad (\text{mod } p^{k+1}).$$

Or θv_k est un polynome de degré $n-1$ dont le terme de plus haut degré a un coefficient premier avec p tout comme celui de v_k puisque θ est premier avec p.

3. Le résultat précédent et la forme des polynomes u particuliers obtenus au n° 1 montrent que tous les polynomes u_k sont des polynomes en px dont les coefficients entiers sont premiers avec p. Cette forme des u_k peut d'ailleurs être établie directement par récurrence.

Les termes consécutifs d'un polynome u_k, du terme de degré j au terme de degré h compris ($j < h \leq k$) constituent le produit par $p^j x^j$ d'un polynome u d'indice $h-j$.

En effet si l'on désigne par $p^j x^j \varphi(x)$ le polynome formé par ces termes consécutifs et par $\psi(x)$ celui formé par les termes de u_k ayant un degré inférieur à j, on voit immédiatement que la somme $p^j x^j \varphi + \psi$ constitue un polynome u d'indice h, de sorte que

$$g(x)[p^j x^j \varphi(x) + \psi(x)] \equiv v_h \pmod{p^{h+1}}.$$

Mais dans le premier membre de cette congruence les termes de degré $n+j$ à $n+h$ proviennent uniquement du produit $p^j x^j g(x)\varphi(x)$ et leurs coefficients sont congrus à zéro mod p^{h+1}, par suite dans le produit $g(x)\varphi(x)$ tous les termes de degré supérieur ou égal à n sont congrus à zéro mod p^{h-j+1} et pour démontrer que φ constitue un polygone u_{h-j} il nous reste seulement à prouver que le coefficient b du terme en x^{n-1} du produit $g\varphi$ est premier avec p; or dans le produit $g(p^j x^j \varphi + \psi)$ lui correspond le terme $(bp^j + A_{j-1} p^j) x^{n-j+1}$ si l'on désigne par A_{j-1} le coefficient de $p^{j-1} x^{j-1}$ dans u_k, on a donc

$$bp^j + A_{j-1} p^j \equiv 0 \pmod{p^{h+1}} \qquad \text{d'où} \quad b + A_{j-1} \equiv 0 \pmod{p^{h-j+1}},$$

ce qui exige b premier avec p comme A_{j-1}.

4. A tout polynome U en px, à coefficients entiers, de degré k dont le terme indépendant est premier avec p, on peut faire correspondre un polynome W de degré au plus égal à k tel que UW soit congru à l'unité module p^{k+1}.

Soit

$$U = A_k p^k x^k + A_{k-1} p^{k-1} x^{k-1} + \ldots + A_j p^j x^j + \ldots + A_1 px + A_0,$$

où A_0 est premier avec p; nous allons déterminer de proche en proche les coefficients du polynome W écrit sous la même forme

$$W = B_k p^k x^k + B_{k-1} p^{k-1} x^{k-1} + \ldots + B_j p^j x^j + \ldots + B_1 px + B_0.$$

Le produit UW est en effet congru module p^{k+1} à

$$A_0 B_0 + px(A_0 B_1 + A_1 B_0) + \ldots + p^j x^j \left(A_0 B_j + \sum_{i=1}^{j} A_i B_{j-i} \right) + \ldots + p^k x^k \left(A_0 B_k + \sum_{i=1}^{k} A_i B_{k-i} \right).$$

Nous pouvons trouver B_0, entier premier avec p, tel que

$$A_0 B_0 \equiv 1 \pmod{p^{k+1}},$$

puisque A_0 est premier avec p; la congruence

$$A_0 B_1 + A_1 B_0 \equiv 0 \pmod{p^k}$$

permet ensuite la détermination de B_0 et ainsi de suite : les congruences

$$A_0 B_j + \sum_{i=1}^{j} A_i B_{j-i} \equiv 0 \pmod{p^{k-j+1}}$$

permettent le calcul successif des coefficients de W; on voit ainsi que W est déterminé à une congruence module p^{k+1} près.

Il résulte de cette propriété qu'en particulier à tout polynome u_k correspond un polynome w_k, de degré k au plus, tel que

$$u_k(x)w_k(x) \equiv 1 \pmod{p^{k+1}}.$$

Des congruences

$$u_k w_k \equiv 1 \quad \text{et} \quad g u_k \equiv v_k \pmod{p^{k+1}},$$

on déduit en multipliant la seconde par w_k

$$g(x) \equiv v_k(x)\, w_k(x) \pmod{p^{k+1}}.$$

Les polynomes v_k et w_k sont donc *des diviseurs de $g(x)$ module p^{k+1}*.

Dans le produit $v_k w_k$ les termes de degré supérieur à n sont congrus à zéro module p^{k+1}, cela exige que dans w_k tous les termes de degré supérieur à l'unité soient congrus à zéro puisque le terme de plus haut degré dans v_k a un coefficient premier avec p; par suite le polynome w_k est congru à un polynome du premier degré :

Quel que soit l'entier k, il existe des diviseurs de $g(x)$ module p^{k+1}, les uns $v_k(x)$ sont de degré $n-1$ et ont pour coefficient de x^{n-1} un entier premier avec p, les autres $w_k(x)$ sont du premier degré.

Les relations existant entre les polynomes u de même indice et le fait qu'un diviseur de g module p^{k+1} est *a fortiori* diviseur module $p^{k'+1}$ si k' est inférieur à k montrent que : *Deux diviseurs de g du même degré w_k et $w_{k'}$ ou v_k et $v_{k'}$ sont liés par une congruence*

$$w_k + \theta w_{k'} \equiv 0 \quad \text{ou} \quad \theta v_k + v_{k'} \equiv 0,$$

dont le module est la plus petite des puissances p^{k+1} ou $p^{k'+1}$ et où θ est premier avec p. Réciproquement un polynome congru module p^{k+1} à un diviseur module p^{k+1} est un diviseur module $p^{k'+1}$ où k' est au moins égal au plus petit des 2 nombres k ou h.

Un diviseur du premier degré est de la forme $\mathrm{A}px + \mathrm{B}$, les coefficients A et B sont liés par une congruence. En effet le diviseur v correspondant s'écrit $b_k x^{n-1} + b_1 x^{n-2} + \ldots$ et l'on doit avoir

$$\begin{aligned} \mathrm{A}\, b p &\equiv p \pmod{p^{k+1}} \quad \text{d'où} \quad \mathrm{A}\, b \equiv 1 \pmod{p^k}, \\ \mathrm{A}\, b_1 p + \mathrm{B}\, b &\equiv a \pmod{p^{k+1}} \quad \text{d'où} \quad \mathrm{B}\, b \equiv a \pmod{p}; \end{aligned}$$

en multipliant la dernière congruence par A on obtient

$$\mathrm{BA}\, b \equiv \mathrm{A}\, a \pmod{p} \quad \text{soit} \quad \mathrm{B} \equiv \mathrm{A}\, a \pmod{p}.$$

Les relations existant entre les diviseurs de même degré permettent de rendre égal à l'unité le coefficient de x^{n-1} dans v_k (il suffit de multiplier v_k par le coefficient A du polynome w_k correspondant) l'expression correspondante du diviseur du premier degré s'obtient en multipliant w_k par b et est de la forme

$$px + a + m_k p,$$

où m_k est un entier qui dépend du coefficient de x^{n-2} dans g (on démontre facilement que

$$a_2 + am_k \equiv 0 \pmod{p}.$$

5. Soit maintenant un polynome f à coefficients entiers de degré $n+k$ dans lequel le coefficient de x^{n+k} est premier avec p

$$f_k(x) = \alpha x^{n+k} + \alpha_1 x^{n+k-1} + \ldots \qquad (\alpha \text{ premier avec } p).$$

On remarque que

$$p^{k+1} f_k(x) = g(x)\,\alpha p^k x^k + p^k f_{k-1}(x),$$

où $f_{k-1}(x)$ est un polynome à coefficients entiers de degré $n+k-1$ dont le terme de plus haut degré a pour coefficient $\alpha_1 p - a\alpha$ premier avec p comme a et α. Cette remarque montre que le reste partiel de rang j dans la division de $p^{k+1} f_k(x)$ par $g(x)$ est $p^{k-j+1} f_{k-j}(x)$ où $f_{k-j}(x)$ est un polynome de degré $n+k-j$ dont le terme de plus haut degré a pour coefficient un entier premier avec p; il en résulte que le reste final de cette division est un polynome $r(x)$ à coefficients entiers de degré $n-1$ dont le terme en x^{n-1} a un coefficient premier avec p et comme

$$p^{k+1} f(x) = g(x)\,q(x) + r(x),$$

on a

$$g(x)\,q(x) \equiv -r(x) \pmod{p^{k+1}}.$$

Le polynome $q(x)$ est donc un polynome u_k, le reste $r(x)$ un diviseur de g module p^{k+1}; les polynomes $Q(x)$ et $R(x)$ quotient et reste de la division de $f(x)$ par $g(x)$ sont respectivement $\frac{q(x)}{p^{k+1}}$ et $\frac{r(x)}{p^{k+1}}$.

Désignons par b le coefficient, premier avec p, du terme en x^{n-1} dans le polynome $r(x)$ et par $w(x)$ le diviseur de g du premier degré associé à $r(x)$. La division de $b^2 g(x)$ par $r(x)$ fournit comme quotient et reste des polynomes à coefficients entiers $q_2(x)$ et $r_2(x)$ tels que

$$b^2 g(x) = r(x)\,q_2(x) + r_2(x),$$

comme d'autre part

$$g(x) \equiv r(x)\,w(x) \pmod{p^{k+1}},$$

on a

$$r(x)[b^2 w(x) - q_2(x)] \equiv r_2(x) \pmod{p^{k+1}}.$$

Cela exige que $b^2 w(x) - q_2(x)$ soit congru à zéro mod p^{k+1} puisque $r_2(x)$ est de degré $n-2$ au plus et que le coefficient de x^{n-1} dans $r(x)$ est premier avec p; par suite $r_2(x)$ est congru à zéro. La division de $g(x)$ par $R(x)$ fournit comme quotient le produit de $q_2(x)$ par $\frac{p^{k+1}}{b^2}$ et comme reste le quotient de $r_2(x)$ par b^2. on peut donc énoncer :

Étant donnés un polynome $g(x)$ à coefficients entiers de degré n dont le terme en x^n a un coefficient p premier avec le coefficient du terme en x^{n-1} et un polynome $f(x)$ à coefficients entiers de degré $n+k$ dont le coefficient

de x^{n+k} est premier avec p, la division de f par g fournit pour reste $\mathrm{R}(x)$ *le quotient par p^{k+1} d'un polynome de degré $n-1$ diviseur de $g(x)$ module p^{k+1}* (ce reste n'est donc jamais identiquement nul). *La division de $g(x)$ par* $\mathrm{R}(x)$ *fournit pour reste un polynome dont chaque coefficient a pour dénominateur un nombre premier avec p (ou l'unité) et pour numérateur un nombre divisible par p^{k+1}.*

Ce résultat qui apparaît lorsqu'on effectue les divisions successives pour déterminer le P. G. C. D. de f et g fournit une intéressante vérification des calculs et permet de simplifier l'écriture du reste de la deuxième division.

6. Ce résultat fournit un moyen pratique pour obtenir des diviseurs de g module p^{k+1} : on effectue la division par g d'un polynome $p^{k+1}f(x)$, par exemple $p^{k+1}x^{n+k}$. Le reste de cette division est un polynome $r(x)$ qui est un diviseur de g; si l'on désigne par b le coefficient de son terme de plus haut degré, on détermine un entier c tel que $cb \equiv \pm 1 \pmod{p^{k+1}}$ Le polynome $cr(x)$ est congru (mod p^{k+1}) à un polynome $\mathrm{V}_k(x)$ de degré $n-1$ dans lequel le coefficient de x^{n-1} est égal à ± 1, $\mathrm{V}_k(x)$ est le diviseur de g module p^{k+1} que nous retiendrons pour la suite du calcul.

La division de $g(x)$ par $\mathrm{V}_k(g)$ fournit comme quotient un polynome du premier degré, diviseur de g module p^{k+1}, qui est de la forme

$$\mathrm{W}_k(x) = px + a + \mathrm{M}p.$$

Le reste de cette division de x par V_k est un polynome de degré au plus égal à $n-2$ dont les coefficients sont entiers et tous divisibles au moins par p^{k+1}. On peut donc écrire

$$g(x) = \mathrm{V}_k(x)\,\mathrm{W}_k(x) + p^{k+1}\mathrm{F}(x), \tag{1}$$

où F est un polynome à coefficients entiers de degré inférieur ou égal à $n-2$.

Le diviseur $\mathrm{W}_k(x)$ jouit d'une propriété particulière parmi les diviseurs w_k écrits sous la forme réduite $px + a + mp$. En effet la définition des diviseurs v_k et w_k montre que l'on a encore

$$g(x) = v_k(x)w_k(x) + p^{k+1}\mathrm{F}'(x), \tag{2}$$

mais $\mathrm{F}'(x)$ est en général de degré $n-1$.

Aucune valeur entière de x ne peut donner à un polynome w_k ou W_k une valeur congrue à zéro module p^{k+1} puisque le coefficient de x dans ces polynomes est égal à p; mais ces polynomes s'annulent pour une valeur de x, fraction irréductible de dénominateur p. Si l'on remplace x par cette fraction dans (1) ou dans (2) on voit que g prend alors la même valeur que $p^{k+1}\mathrm{F}(x)$ ou $p^{k+1}\mathrm{F}'(x)$. Or la valeur de F est le quotient d'un nombre entier par une puissance de p au plus égale à la $(n-2)^{\text{ième}}$, tandis que celle prise par F' est en général le quotient d'un nombre entier par p^{n-1}. Il en résulte que si k est assez grand, la valeur numérique prise par g pour la racine d'un polynome w_k est un nombre entier divisible par p^{k-n+2} en général, tandis que la valeur prise par g pour la racine du polynome W_k est une valeur entière divisible au moins par p^{k-n+3}.

On peut préciser ce résultat : w_k est en effet égal à $W_k + \theta p^{k+1}$, donc

$$g(x) = V_k(x) w_k(x) + p^{k+1}[F(x) - \theta V_k(x)].$$

La différence $F(x) - \theta V_k(x)$ est de degré $n-1$ et sa valeur numérique pour la racine de $w_k(x)$ est le quotient d'un nombre congru à $-\theta \pmod p$ par p^{n-1} : si donc θ n'est pas divisible par p, la valeur entière prise par g n'est divisible que par p^{k-n+2}. En conclusion :

Quel que soit l'entier h il existe des fractions irréductibles ayant p pour dénominateur donnant au polynome $g(x)$ une valeur entière divisible par p^h.

Ces fractions s'obtiennent en annulant les polynomes W_{n+h-3}, leurs numérateurs sont congrus module p à l'opposé du coefficient de x^{n-1} dans g et sont déterminés à un multiple de p^{n+h-1} près.

7. Nous nous proposons de généraliser les résultats précédents en supposant que dans le polynome $g(x)$ les coefficients de x^{n-1} et des termes suivants sont divisibles par p jusqu'au coefficient de x^{n-h} qui, lui, est premier avec p. Nous avons donc désormais

$$g(x) = px^n + a_1 px^{n-1} + \ldots + a_j px^{n-j} + \ldots + a_{h-1} px^{n-h+1} + ax^{n-h} + a_{h+1} x^{n-h-1} + \ldots$$

où a est premier avec p (a peut être égal à l'unité).

Quel que soit k, il existe des polynomes $u_k(x)$ de degré hk tels que le produit $g(x) u_k(x)$ soit congru module p^{k+1} à un polynome $v_k(x)$ de degré $n-h$ dans lequel le coefficient de x^{n-h} est premier avec p.

Quand $k = 0$, il suffit de prendre $u_0 = 1$. Nous allons montrer qu'on peut déterminer un polynome u d'indice k en supposant connus un polynome u d'indice $k-1$ et le polynome v correspondant; il en résulte qu'on pourra ainsi calculer de proche en proche des polynomes u et v d'indice quelconque.

Par hypothèse nous avons

$$g u_{k-1} \equiv b x^{n-h} + b_1 x^{n-h-1} + \ldots + b_j x^{n-h-j} + \ldots \pmod{p^k},$$

où b est premier avec p ; montrons qu'on peut déterminer des constantes $A_1, \ldots, A_j, \ldots, A_{h-1}$ de façon que le polynome

$$U = (px^h + A_1 px^{h-1} + \ldots + A_j px^{h-j} + \ldots + A_{h-1} px) u_{k-1} - b,$$

soit un polynome u_k. Le produit gU est congru module p^{k+1} à

$$\begin{aligned} &p(A_1 b + b_1 - ba_1) x^{n-1} + p(A_2 b + A_1 b_1 + b_2 - ba_2) x^{n-2} + \ldots \\ &+ p(A_j b + A_{j-1} b_1 + \ldots + b_j - ba_j) x^{n-j} + \ldots + p(A_{h-1} b + A_{h-2} b_1 + \ldots + b_{h-1} - ba_{h-1}) x^{n-h+1} \\ &+ [-ba + p(b_h + A_1 b_{h-1} + \ldots + A_{h-1} b_1)] x^{n-h} + \ldots . \end{aligned}$$

Pour rendre congrus à zéro module p^{k+1} les coefficients des $h-1$ premiers termes de l'expression ci-dessus, nous pouvons calculer les A de proche en proche en commençant par A_1 car dans chacune des congruences ainsi obtenues l'incon-

nue nouvelle a pour coefficient b qui est premier avec p. Les $h-1$ coefficients A étant déterminés par ce procédé, le produit gU est congru (mod p^{k+1}) à un polynome de degré $n-h$ dont le coefficient de x^{n-h} est bien premier avec p comme a et b. Le polynome U est donc bien un polynome u_k.

Nous voyons que dans les polynomes u, d'indice quelconque k, obtenus par ce procédé le terme indépendant de x est premier avec p et le terme de plus haut degré est $p^k x^{kh}$.

8. ***Deux polynomes u_k et u'_k de même indice sont liés par une congruence $u'_k + \theta u_k \equiv 0$ module p^{k+1} où θ est premier avec p, et réciproquement.***

Comme au n° 2 nous établirons d'abord le lemme suivant : *Tout polynome $z_k(x)$, de degré hk au plus, tel que le produit gz_k soit congru module p^{k+1} à un polynome de degré $n-h-1$ est congru à zéro module p^{k+1}.*

La condition est évidemment nécessaire pour $k=0$; supposons démontré qu'elle est nécessaire pour tout polynome z d'indice inférieur ou égal à $k-1$. Les h termes de plus haut degré de z_k sont de la forme

$$Ax^{hk} + A_1 x^{hk-1} + \ldots + A_{h-1} x^{hk-h+1},$$

et l'on vérifie immédiatement que les h premiers termes du produit gz_k (de degré $hk+n$ à $hk+n-h+1$) ne peuvent être congrus à zéro (mod p^{k+1}) que si les coefficients A sont divisibles par p^k, il en résulte que l'ensemble des autres termes de z_k forme un polynome z_{k-1} et, par suite, leurs coefficients sont divisibles par p^k. On peut donc écrire

$$z_k = A' p^k x^{kh} + A'_1 p^k x^{kh-1} + \ldots + A'_{h-1} p^k x^{kh-h+1} + B p^k x^{kh-h} + \ldots + C p^k x^j + \ldots.$$

Dans le produit gz_k le coefficient de x^{n+kh-h} est égal à

$$p^k [A' a + p(A'_1 a_{h-1} + \ldots + A'_{h-1} a_1)],$$

et il ne peut être congru à 0 module p^{k+1} que si A' est divisible par p : le premier coefficient de z_k est donc congru à zéro module p^{k+1} et l'on démontre de proche en proche qu'il en est de même pour tous les coefficients. En effet, si les premiers coefficients de z_k (ceux des puissances de x supérieures à la $j^{\text{ième}}$) sont congrus à zéro (mod p^{k+1}) le coefficient de x^{n+j-h} dans le produit gz_k ne contient que aCp^k et des termes divisibles par p^{k+1} soit parce qu'ils sont produit d'un coefficient de g par un coefficient d'un des premiers termes de z_k, soit parce qu'ils sont produit d'un des premiers coefficients de g (divisibles par p) par un des coefficients suivants de z_k (divisibles par p^k) ; il en résulte que Cp^k doit lui aussi être divisible par p^{k+1} puisque quel que soit j, $n+j-h$ est supérieur à $n-h-1$ degré de la plus haute puissance du produit gz_k dont le coefficient pourrait ne pas être congru à zéro. Le polynome z_k est donc congru à zéro (mod p^{k+1}).

Le lemme étant établi, un raisonnement analogue à celui du n° 2 montre qu'il existe un entier θ premier avec p tel que $u'_k + \theta u_k$ soit un polynome z_k; donc $v'_k + \theta v_k$ et $v'_k + \theta v_k$ sont congrus à zéro module p^{k+1}.

Nous pouvons préciser maintenant la forme des polynomes u_k en utilisant les résultats de ce paragraphe et du précédent :

$$u_k = A_k^1 p^k x^{kh} + A_k^2 p^k x^{kh-1} + \ldots + A_k^h p^k x^{kh-h+1} + A_{k-1}^1 p^{k-1} x^{kh-h} + \ldots + A_1^h px + A_0^1,$$

où les coefficients d'indice supérieur égal à l'unité sont premiers avec p.

9. Il est possible de déterminer un polynome w_k au plus de degré kh tel que le produit $u_k w_k$ soit congru à l'unité module p^{k+1}.

Nous cherchons ce polynome w_k sous la même forme que celle de u_k

$$w_k = B_k^1 p^k x^{kh} + B_k^2 p^k x^{kh-1} + \ldots + B_k^h p^k x^{kh-h+1} + \ldots + B_j^i p^j x^{jh-i+1} + \ldots + B_1^h px + B_0^1.$$

Nous remarquons que dans le produit $u_k w_k$ tout terme de degré supérieur à hk est congru à o module p^{k+1} et il nous reste $kh+1$ conditions pour déterminer les $kh+1$ coefficients de w_k. Ces conditions s'expriment par des congruences dont les premières sont

$$\begin{aligned} A_0^1 B_0^1 &\equiv 1 \pmod{p^{k+1}}, \\ A_0^1 B_1^h + A_1^h B_0^1 &\equiv 0 \pmod{p^k}, \\ A_0^1 B_1^h + B_1^{h-1} A_1^h p + A_1^{h-1} B_0^1 &\equiv 0 \pmod{p^k}. \end{aligned}$$

Nous allons vérifier que la considération du terme en x^{jh-i+1} dans le produit $u_k w_k$ permet le calcul de B_j^i en supposant connus les coefficients B des puissances de x inférieures à la $(jh-i+1)^{\text{ième}}$. En effet les monomes qui constituent le produit $u_k w_k$ sont de la forme

$$A_c^{c'} B_d^{d'} p^{c+d} x^{(c+d)h-(c'+d')+2}.$$

Pour que l'exposant de x soit $jh-i+1$, il faut que $c+d$ soit au moins égal à j puisque $c'+d'$ est au moins égal à 2 et i au plus égal à h; donc tous les éléments du terme de degré $jh-i+1$ sont divisibles par p^j, en particulier l'élément $A_0^1 B_j^i p^j$ qui contient l'inconnue B_j^i ; ce terme ne peut contenir aucun autre coefficient B encore inconnu puisqu'il faudrait pour cela $d \geq j+1$ avec d' quelconque ou $d=j$ avec $d' < i$ ce qui entraîne $(c+d)h - c' - d' + 2$ supérieur a $jh-i+1$. Donc B_j^i est déterminé par une congruence module p^{k-j+1} dans laquelle le coefficient de l'inconnue est A_0^1 premier avec p. Nous remarquons que B_0^1 est premier avec p.

Des congruences

$$u_k w_k \equiv 1 \quad \text{et} \quad g u_k \equiv w_k \pmod{p^{k+1}},$$

nous déduisons

$$g(x) \equiv v_k(x) w_k(x) \pmod{p^{k+1}}.$$

Comme le coefficient du terme de plus haut degré de v_k est premier avec p, cette congruence exige que les termes de w_k ayant un degré supérieur à h soient congrus à zéro module p^{k+1}, par suite w_k est congru à un polynome de degré h dans lequel le terme indépendant et le coefficient de px^h sont premiers avec p; nous pouvons donc énoncer :

Quel que soit k, il existe des diviseurs de g module p^{k+1} : les uns $v_k(x)$ sont

de degré $n-h$ et ont pour coefficient de x^{n-h} un nombre premier avec p, les autres $w_k(x)$ sont de degré h.

Comme au n° 4 nous voyons que *deux diviseurs de g du même degré v_k et $v_{k'}$, ou w_k et $w_{k'}$, sont liés par une congruence*

$$w_k + \theta w_{k'} \equiv 0 \quad \text{ou} \quad \theta v_k + v_{k'} \equiv 0,$$

où θ est premier avec p et dont le module est la plus petite des puissances p^{k+1} ou $p^{k'+1}$.

Un diviseur de g de degré h est de la forme $Apx^h + \ldots + B$ où A et B sont des entiers premiers avec p liés par une même congruence quel que soit k : en effet le diviseur v correspondant s'écrit $bx^{n-h} + \ldots$ et la considération des termes de degré n et $n-h$ dans le produit vw montre que

$$B \equiv Aa \pmod{p}.$$

Remarquons qu'un diviseur de degré h n'admet aucun diviseur module p dont le degré soit inférieur à h et dans lequel le terme de plus haut degré aurait un coefficient premier avec p. En effet, soit $C_j x^j + \ldots + C$ un tel diviseur, on aura $w_k \equiv (C_j x^j + \ldots + C)F(x) \pmod{p}$, et comme C_j est supposé premier avec p, le polynome F est congru (mod p) à un polynome F′ de degré $h-j$; comme dans w_k tous les termes dépendant de x ont un coefficient divisible par p, tous les coefficients de F′ sont divisibles par p, même le terme indépendant si $j \neq 0$, et dans le produit $(C_j x^j + \ldots + C)F$ le terme indépendant de x est divisible par p, il ne peut être congru au terme indépendant de w_k qui est premier avec p.

En utilisant les congruences qui lient les diviseurs de g, on peut toujours ramener à l'unité le coefficient de x^{n-h} dans v_k et le polynome w_k s'écrit alors sous la forme

$$px^h + pC_1 x^{h-1} + \ldots + pC_{h-1}x + a + mp.$$

10. Nous n'appliquerons ces résultats à la division par le polynome g que dans le cas où $h = 2$, et nous sommes conduits à introduire deux nouveaux types de multiplicateurs : les polynomes y_k dont le produit par g est congru module p^{k+1} à un polynome de degré $n-1$ où le coefficient de x^{n-1} est premier avec p et les polynomes q_k dont le produit par g est congru à un polynome de degré $n-1$ où le coefficient de x^{n-1} est divisible par p et le coefficient de x^{n-2} premier avec p.

Il est évident que le polynome xu_k est un polynome y_k, réciproquement : *tout polynome y_k est congru module p^{k+1} au produit d'un polynome u_k par un polynome du premier degré dans lequel le coefficient de x est premier avec p.* Pour démontrer ce résultat, nous établirons d'abord qu'un polynome U_k de degré $2k+1$ au plus, tel que gU_k soit congru (mod p^{k+1}) à un polynome de degré $n-2$ au plus, est congru (mod p^{k+1}) au produit d'un polynome u_k par une constante.

En effet pour $k = 0$ on aura $U_0 = Ax + B$ et le produit gU_0, congru (mod p) à $(Aa + Ba_1 p)x^{n-1} + \ldots$, n'est congru à un polynome de degré $n-2$ que si A est congru à zéro ; donc U_0 est congru (mod p) à une constante comme tout polynome u_0.

Supposons alors la propriété vraie pour les U d'indice inférieur à k et montrons-la pour U_k qui s'écrit

$$A x^{2k+1} + B x^{2k} + C x^{2k-1} + \dots$$

Dans le produit $g U_k$ les termes de degré $2k+n-1$ et $2k+n$ ne sont congrus à zéro module p^{k+1} que si

$$Ap \equiv 0 \quad \text{et} \quad Bp + A a_1 p \equiv 0 \qquad (\text{mod } p^{k+1}),$$

ce qui exige

$$A = A' p^k \quad \text{et} \quad B = B' p^k,$$

si bien que l'ensemble des termes de degré inférieur ou égal à $2k-1$ dans U_k forme un polynome U_{k-1} et par suite le coefficient C est divisible par p^k, soit $C = C' p^k$. Le terme de degré $2k+n-1$ dans le produit $g U_k$ qui a pour coefficient $(C' + B' a_1) p^{k+1} + A' a p^k$ ne peut être congru à zéro $(\text{mod } p^{k+1})$ que si A' est divisible par p; dès lors U_k est congru $(\text{mod } p^{k+1})$ à un polynome U'_k de degré $2k$ dont le produit par g est congru à un polynome V de degré $n-2$ au plus. Si le coefficient de x^{n-2} dans V est premier avec p, V est un polynome v_k et U'_k un polynome u_k; si ce coefficient p' n'est pas premier avec p, le polynome U'_k n'est pas un polynome u_k, mais si l'on désigne par u_k un polynome tel que

$$g u_k \equiv x^{n-2} + \dots \qquad (\text{mod } p^{k+1}),$$

(nous savons que de tels polynomes existent), le polynome $U'_k - p' u_k$ est tel que $g(U'_k - p' u_k)$ soit congru $(\text{mod } p^{k+1})$ à un polynome de degré $n-3$ au plus, donc (N° 8) cette différence $U'_k - p' u_k$ est congrue à zéro module p^{k+1}. Dans tous les cas U_k est donc bien congru à θu_k (mais θ n'est pas nécessairement premier avec p)

Cela étant, soient y_k et y'_k deux polynomes tels que

$$g y_k \equiv b x^{n-1} + b_1 x^{n-2} + \dots \qquad (\text{mod } p^{k+1}),$$
$$g y'_k \equiv b' x^{n-1} + b'_1 x^{n-2} + \dots \qquad (\text{mod } p^{k-1}),$$

comme b et b' sont premiers avec p, il existe un nombre θ_1 premier avec p tel que

$$b + \theta_1 b' \equiv 0 \qquad (\text{mod } p^{k+1}),$$

alors $g(y_k + \theta_1 y'_k)$ est congru à un polynome de degré $n-2$ au plus; donc, en appliquant le résultat précédent

$$y_k + \theta_1 y'_k \equiv \theta_2 u_k.$$

En choisissant $y'_k = -x u_k$ nous obtenons bien

$$y_k \equiv (\theta_1 x + \theta_2) u_k \qquad (\text{mod } p^{k+1}).$$

Tout produit d'un polynome u_k par un polynome $\theta_3 p x + \theta_4$ où θ_4 est premier avec p constitue un polynome q_k et réciproquement tout polynome q_k est un tel produit.

La définition des polynomes q_k et u_k rend évidente la première partie de cet énoncé. Pour démontrer la réciproque, désignons par y_{k-1} un polynome tel que

$$g y_{k-1} \equiv c x^{n-1} + c_1 x^{n-2} + \dots \pmod{p^k},$$

où c premier avec p, et soit

$$b_1 p x^{n-1} + b x^{n-2} + \dots$$

où b premier avec p, le polynome congru au produit $g q_k$. Il existe un nombre B tel que cB soit congru (mod p^{k+1}) à b_1 et par suite la différence $q_k - Bpy_{k-1}$ est telle que son produit par g est congru à $(b - Bc_1 p)x^{n-2} + \dots$, module p^{k+1}, cette différence est donc un polynome u_k puisque $b - Bc_1 p$ est premier avec p. On peut donc écrire

$$q_k \equiv u_k + Bpy_{k-1} \pmod{p^{k+1}},$$

mais

$$y_{k-1} \equiv (\theta_1 x + \theta_2) u_{k-1} \pmod{p^k},$$

ou encore

$$y_{k-1} \equiv (\theta'_1 x + \theta'_2) u_k \pmod{p^k},$$

puisque

$$u_{k-1} \equiv \theta u_k \pmod{p^k},$$

finalement

$$q_k \equiv (Bp\theta'_1 x + Bp\theta'_2 + 1) u_k = (\theta_3 p x + \theta_4) u_k \pmod{k+1},$$

où θ_3 premier avec p.

11. Soit alors un polynome $f_k(x)$ de degré $n+2k+1$ dans lequel le coefficient de x^{n+2k+1} est premier avec p :

$$f_k(x) = \alpha x^{n+2k+1} + \alpha_1 x^{n+2k} + \dots$$

on a

$$p^{k+1} f_k(x) = g(x)[\alpha p^k x^{2k+1} + (\alpha_1 - a_1 \alpha) p^k x^{2k}] + p^k f_{k-1}(x),$$

où $f_{k-1}(x)$ est un polynome de degré $n+2k-1$ dont le terme de plus haut degré a pour coefficient

$$-a\alpha + p(\alpha a_1^2 - a_1 \alpha_1 + \alpha_2),$$

premier avec p comme a et α. En poursuivant la division de $p^{k+1} f_k(x)$ par $g(x)$ on obtiendra un polynome $f_0(x)$ de degré $n+1$ dont le terme de plus haut degré a pour coefficient α' premier avec p; d'où finalement

$$p f_0(x) = g(x)(\alpha' x + \alpha'_1 - a_1 \alpha') + r(x),$$

où $r(x)$ est de degré $n-1$ et a pour coefficient de x^{n-1} un nombre premier avec p. Donc

$$p^{k+1} f_k(x) = g(x) q(x) + r(x),$$

d'où

$$g(x)\, q(x) \equiv -r(x) \pmod{p^{k+1}},$$

ce qui prouve que $q(x)$ est un polynome $y_k(x)$ et

$$q(x) \equiv (\theta_1 x + \theta_2) u_k(x) \pmod{p^{k+1}}$$

par suite, en tenant compte de la congruence $g u_k \equiv v_k \pmod{p^{k+1}}$

$$r(x) \equiv -(\theta_1 x + \theta_2) v_k(x).$$

Soit b, premier avec p, le coefficient de x^{n-1} dans $r(x)$, en effectuant la division de $b^2 g(x)$ par $r(x)$ nous obtenons

$$b^2 g(x) = r(x)\, q'(x) + r'(x),$$

et il est facile de vérifier que le coefficient de x^{n-2} dans r' est premier avec p. Nous savons qu'il existe un polynome du second degré w_k tel que

$$g(x) \equiv v_k(x) w_k(x) \pmod{p^{k+1}},$$

par suite

$$v_k(x)[b^2 w_k + (\theta_1 x + \theta_2) q'(x)] \equiv r'(x) \pmod{p^{k+1}}.$$

Comme r' est de degré $n-2$ ainsi que v_k et comme le coefficient de x^{n-2} dans v_k est premier avec p, cette congruence n'est possible que si le crochet est congru à une constante, donc :

$$r'(x) \equiv C v_k(x) \pmod{p^{k+1}},$$

où C premier avec p.

Soit maintenant un polynome $f_k(x)$ de degré $n+2k$ dont le premier coefficient est premier avec p :

$$f_k(x) = a x^{n+2k} + a_1 x^{n+2k-1} + \dots.$$

D'une manière analogue à celle utilisée ci-dessus, on montre qu'en effectuant la division de $p^{k+1} f_k(x)$ par $g(x)$ on arrive à un reste partiel $p f_0(x)$ où f_0 est de degré n et a pour coefficient de x^n un nombre a' premier avec p. Finalement

$$p f_0(x) = g(x) a' + r(x),$$

où

$$r(x) = p(a'_1 - a' a_1) x^{n-1} + (p a'_2 - a a') x^{n-2} + \dots$$

Ce polynome $r(x)$ est le reste de la division de $p^{k+1} f_k(x)$ par $g(x)$ et l'identité de la division montre que le quotient $q(x)$ est tel que

$$g(x) q(x) \equiv -r(x) \pmod{p^{k+1}}.$$

Comme le coefficient $p a'_2 - a a' (= b)$ de x^{n-2} dans r est premier avec p, nous en déduisons que $q(x)$ est un polynome q_k si $a'_1 - a_1 a' (= b_1)$ n'est pas congru à zéro (mod p^k) ou un polynome u_k dans le cas contraire. On voit comme ci-dessus qu'il en résulte

$$r(x) \equiv -(\theta_3 p x + \theta_4) v_k \pmod{p^{k+1}},$$

θ_4 est premier avec p, θ_3 peut être nul (en particulier si $b_1 = 0$).

Si b_1 n'est pas nul, pour trouver des polynomes à coefficients entiers en divisant par $r(x)$, nous devons multiplier g par $p b_1^2$; on a

$$p b_1^2 g(x) = r(x)\, q'(x) + r'(x),$$

le coefficient de x^{n-2} dans r' est premier avec p comme b^2. De cette relation et de la congruence

$$g(x) \equiv v_k w_k \pmod{p^{k+1}},$$

résulte encore

$$r'(x) \equiv C v_k(x) \pmod{p^{k+1}},$$

ou C premier avec p.

Dans les deux hypothèses sur le degré de f, sauf si $b_1 = 0$, désignons par c le coefficient de x^{n-2} dans $r'(x)$ et effectuons la division de $c^2 r(x)$ par $r'(x)$; elle fournit pour quotient et reste des polynomes à coefficients entiers tels que

$$c^2 r(x) = r'(x) q''(x) + r''(x);$$

en tenant compte des congruences

$$r(x) \equiv (Ax + B) v_k(x) \qquad \text{et} \qquad r'(x) \equiv C v_k(x) \qquad (\text{mod } p^{k+1}),$$

il vient

$$v_k(Ac^2 x + Bc^2 - Cq'') \equiv r'' \qquad (\text{mod } p^{k+1}).$$

Comme r'' est de degré $n-3$ au plus et que le coefficient de x^{n-2} dans v_k est premier avec p, le crochet doit être congru à zéro (mod p^{k+1}) et

$$r''(x) \equiv 0 \qquad (\text{mod } p^{k+1}).$$

Si f est de degré $n+2k$ et si b_1 est nul, nous aurons d'une manière analogue

$$b^2 g(x) \equiv r(x) q''(x) + r''(x)$$

et comme r est de degré $n-2$ on a r'' au plus de degré $n-3$. De cette relation et des congruences

$$g \equiv v_k w_k \qquad \text{et} \qquad r \equiv \theta_1 v_k \qquad (\text{mod } p^{k+1}),$$

on déduit

$$r'' \equiv v_k (b^2 w_k - \theta_1 q'') \qquad (\text{mod } p^{k+1}),$$

ce qui exige encore

$$r''(x) \equiv 0 \qquad (\text{mod } p^{k+1}).$$

En résumé, nous pouvons énoncer :

Étant donnés un polynome $g(x) = px^n + \ldots$ dans lequel le coefficient de x^{n-1} est divisible par p (ou nul) et le coefficient de x^{n-2} premier avec p (ou égal à l'unité) et un polynome $f(x)$ de degré $n+2k$ ou $n+2k+1$ dans lequel le coefficient du terme de plus haut degré est premier avec p, la division de f par g fournit pour reste le produit par un polynome du premier degré (ou une constante éventuellement) d'un diviseur de g module p^{k+1} de degré $n-2$. Les coefficients de ce polynome du premier degré (ou la constante) ont pour dénominateur p^{k+1} et le numérateur de l'un d'eux au moins est premier avec p.

Les divisions successives effectuées à partir des polynomes f et g fournissent pour reste de la seconde division, en général, le produit par une constante (fraction de numérateur premier avec p) *d'un polynome de degré $n-2$ diviseur de g module p^{k+1}, le reste de la troisième division est alors un polynome dont les coefficients sont des fractions irréductibles à numérateur divisible par p^{k+1}.*

Si $f(x)$ est de degré $n+2k$, il peut arriver que ces résultats soient obtenus respectivement à la première et la seconde division.

Comme au n° 5 ce résultat fournit un moyen d'obtenir des diviseurs de g et il indique une intéressante vérification des calculs de divisions successives.

(Manuscrit remis le 15 février 1948.)