QUELQUES REMARQUES SUR LA DIVISIBILITÉ DES COEFFICIENTS BINOMIAUX

QUELQUES REMARQUES SUR LA DIVISIBILITÉ DES COEFFICIENTS BINOMIAUX

par P. CARTIER (Strasbourg)

1. Dans toute cette note, on désigne par p un nombre premier. Rappelons tout d'abord un résultat classique: pour tout entier i compris entre 1 et $p-1$, le coefficient binomial $\binom{p}{i}$ (égal à $\dfrac{p!}{i!\,(p-i)!}$ par définition) est divisible par p. Il revient au même de dire que le polynôme à coefficients entiers $(X+Y)^p - X^p - Y^p$ en les indéterminées X et Y a tous ses coefficients divisibles par p. La démonstration est très simple; elle consiste à remarquer que p divise le numérateur $p!$, mais non le dénominateur $i!\,(p-i)!$ de la fraction $\binom{p}{i}$ et à appliquer le lemme d'Euclide: si p divise ab, mais non b, il divise a.

Nous nous proposons de généraliser le résultat précédent aux coefficients binomiaux de la forme $\binom{p^h}{i}$ où h est un entier positif et i un entier compris entre 1 et p^h. Ecrivons i sous la forme $j \cdot p^a$ où a est un entier positif et j un entier positif non divisible par p; on a nécessairement $0 \leqq a \leqq h$ et $1 \leqq j \leqq p^{h-a}$. Nous allons prouver que $\binom{p^h}{i}$ *est divisible par* p^{h-a}, *mais non par* p^{h-a+1}. (1)

On peut exprimer ce résultat en formule de la manière suivante. Pour tout entier $n \geqq 1$, il existe un entier m positif déterminé par les conditions: n est divisible par p^m, mais non par p^{m+1}; cet entier m sera noté $v_p(n)$. Par définition, on peut donc écrire n sous la forme $p^{v_p(n)} \cdot n'$ où n' n'est pas divisible par p. Ceci étant posé, notre résultat peut s'énoncer sous la forme

(F) $\boxed{v_p(\binom{p^h}{i}) + v_p(i) = h}$ pour $h \geqq 0$ et $1 \leqq i \leqq p^h$.

2. Avant de passer à la démonstration, donnons quelques exemples numériques simples. On a posé $a = v_p(\binom{p^h}{i})$ et $b = v_p(i)$.

a) $p = 2$, $h = 2$, d'où $p^h = 4$:

i	1	2	3	4
$\binom{p^h}{i}$	4	6	4	1
a	2	1	2	0
b	0	1	0	2
$a+b$	2	2	2	2

1) Ce résultat est conséquence de congruences établies par Artin (Collected papers, pages 157-158, Addison-Wesley, Reading, 1965).

b) $p = 2$, $h = 3$, d'où $p^h = 8$:

i	1	2	3	4	5	6	7	8
$\binom{p^h}{i}$	8	28	56	70	56	28	8	1
a	3	2	3	1	3	2	3	0
b	0	1	0	2	0	1	0	3
$a+b$	3	3	3	3	3	3	3	3

c) $p = 2$, $h = 4$, d'où $p^h = 16$:

i	1	2	3	4	5	6	7	8
$\binom{p^h}{i}$	16	120	560	1.820	4.368	8.008	11.440	12.870
a	4	3	4	2	4	3	4	1
b	0	1	0	2	0	1	0	3
$a+b$	4	4	4	4	4	4	4	4

d) $p = 3$, $h = 2$, d'où $p^h = 9$:

i	1	2	3	4	5	6	7	8	9
$\binom{p^h}{i}$	9	36	84	126	126	84	36	9	1
a	2	2	1	2	2	1	2	2	0
b	0	0	1	0	0	1	0	0	2
$a+b$	2	2	2	2	2	2	2	2	2

e) $p = 5$, $h = 2$, d'où $p^h = 25$:

i	1	2	3	4	5	6	7	8	9	10	11	12
$\binom{p^h}{i}$	25	300	2.300	12.650	53.130	177.100	480.700	1.081.575	2.042.975	3.268.760	4.457.400	5.200.300
a	2	2	2	2	1	2	2	2	2	1	2	2
b	0	0	0	0	1	0	0	0	0	1	0	0
$a+b$	2	2	2	2	2	2	2	2	2	2	2	2

On notera que pour $i = p^h$, le coefficient binomial $\binom{p^h}{i}$ vaut 1, donc $v_p(\binom{p^h}{i}) = 0$, alors qu'on a évidemment $v_p(i) = h$; la relation (F) est donc toujours satisfaite dans ce cas. Par ailleurs, si l'on change i (différent de p^h) en son complémentaire $p^h - i$, on ne change pas $\binom{p^h}{i}$ donc aussi $v_p(\binom{p^h}{i})$, et l'on ne change pas non plus $v_p(i)$. Cette remarque explique pourquoi nous nous sommes limités aux i compris entre 1 et $p^h/2$ dans les exemples c) et e), et confirme les symétries observées dans les autres exemples.

3. Nous donnerons deux démonstrations de la formule (F). La première est très courte et se fait par récurrence sur i. Si a et b sont deux entiers tels que $0 \leqq b < a$, la définition du coefficient binomial $\binom{a}{b} = \dfrac{a\,!}{(a-b)\,!\,b\,!}$

entraîne immédiatement la relation

$$\binom{a}{b+1} \cdot (b+1) = \binom{a}{b} \cdot (a-b) \left(= \frac{a!}{(a-b-1)!\,b!} \right).$$

Appliquons cette relation au cas $a = p^h$, $b = i$, et tenons compte des relations $v_p(mn) = v_p(m) + v_p(n)$ et $v_p(p^h - i) = v_p(i)$ (pour $1 \leqq i \leqq p^h - 1$); on obtient

$$v_p\left(\binom{p^h}{i+1}\right) + v_p(i+1) = v_p\left(\binom{p^h}{i}\right) + v_p(i)$$

pour i compris entre 1 et $p^h - 1$. La quantité $v_p(\binom{p^h}{i}) + v_p(i)$ est donc indépendante de i; on obtient sa valeur en faisant $i = 1$ et l'on trouve h car $\binom{p^h}{1} = p^h$.

4. La seconde démonstration utilise une évaluation classique de $v_p(n!)$. Si nous développons l'entier n dans la base p, nous obtenons la relation

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_r p^r ;$$

les entiers $a_o, a_1, \ldots, a_r$ sont compris entre 0 et $p-1$, et a_r n'est pas nul. Autrement dit, n s'écrit sous la forme $a_r \ldots a_1 a_0$ en base p, et $a_0, a_1, \ldots, a_r$ sont les « chiffres » de son développement en base p. Soit $s = a_0 + a_1 + \ldots + a_r$ la somme de ces « chiffres ». On a alors

$$v_p(n!) = \frac{n - s}{p - 1}. \tag{1}$$

La démonstration de (1) est une application immédiate d'un principe de comptage fort utile en Calcul des Probabilités, et qui n'est autre qu'un cas élémentaire de la transformation d'Abel ou « sommation par parties ». On considère l'ensemble fini X formé des entiers de 1 à n, et la fonction f sur X qui à i associe l'entier positif $v_p(i)$. Comme on a $v_p(ab) = v_p(a) + v_p(b)$ pour deux entiers strictement positifs a et b, et que, par définition, la factorielle $n!$ est le produit des entiers de 1 à n, le nombre $v_p(n!)$ est la somme Σ des nombres $f(i)$ pour i parcourant X. Il est clair que r est la plus grande des valeurs prises par f sur X; comme f est à valeurs entières positives, on voit donc que f prend b_0 fois la valeur 0, b_1 fois la valeur 1, ..., b_r fois la valeur r; dans cette assertion, $b_0, \ldots, b_r$ sont des entiers positifs, $b_0, \ldots, b_{r-1}$ peuvent être nuls, mais b_r ne l'est pas. Avec cette définition, on a évidemment

$$\Sigma = b_1 + 2b_2 + \ldots + r\,b_r . \tag{2}$$

Par ailleurs, notons c_1 le nombre d'éléments i de X tels que $f(i) \geqq 1$, c_2 le nombre d'éléments i de X tels que $f(i) \geqq 2$, ..., c_r le nombre d'éléments i de X tels que $f(i) \geqq r$. On a évidemment

$$\begin{aligned}
c_1 &= b_1 + b_2 + b_3 + \ldots + b_{r-1} + b_r \\
c_2 &= \quad b_2 + b_3 + \ldots + b_{r-1} + b_r \\
c_3 &= \quad\quad b_3 + \ldots + b_{r-1} + b_r \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
c_{r-1} &= \quad\quad\quad\quad b_{r-1} + b_r \\
c_r &= \quad\quad\quad\quad\quad b_r ,
\end{aligned}$$

d'où immédiatement $c_1 + \ldots + c_r = b_1 + 2b_2 + \ldots + rb_r$. Par comparaison avec la formule (2), on obtient la formule de comptage cherchée

$$\Sigma = c_1 + \ldots + c_r . \tag{3}$$

Il reste à évaluer les entiers c_1, ..., c_r. Or, par définition, c_j est le nombre d'entiers i compris entre 1 et n et tels que $v_p(i) \geqq j$, c'est-à-dire le nombre des multiples de p^j compris entre 1 et n. Par suite, c_j est égal à la partie entière de n/p^j; en utilisant le développement de base p de n, on obtient finalement

$$\begin{aligned}
c_1 &= a_1 + a_2 p + a_3 p^2 + \ldots + a_{r-1} p^{r-2} + a_r p^{r-1} \\
c_2 &= \quad a_2 + a_3 p + \ldots + a_{r-1} p^{r-3} + a_r p^{r-2} \\
c_3 &= \quad\quad a_3 + \ldots + a_{r-1} p^{r-4} + a_r p^{r-3} \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
c_{r-1} &= \quad\quad\quad\quad a_{r-1} + a_r p \\
c_r &= \quad\quad\quad\quad\quad a_r .
\end{aligned}$$

Par sommation, on a donc

$$v_p(n!) = \Sigma = \sum_{j=1}^{r} a_j (1 + p + p^2 + \ldots + p^{j-1}) = \sum_{j=0}^{r} a_j \frac{p^j - 1}{p - 1} = \frac{n - s}{p - 1}.$$

5. Soit h un entier positif et soit i un entier compris entre 1 et $p^h - 1$. Nous écrirons de nouveau i sous la forme $j \,.\, p^a$ où j n'est pas divisible par p. Comme j est compris entre 1 et $p^{h-a} - 1$, son développement en base p est de la forme

$$j = \alpha_0 + \alpha_1 p + \ldots + \alpha_{b-1} p^{b-1} \tag{4}$$

avec $b = h-a$; les entiers $\alpha_0, \alpha_1, \ldots, \alpha_{b-1}$ sont compris entre 0 et $p-1$, et α_0 n'est pas nul puisque j n'est pas divisible par p. De $i = j \cdot p^a$, on déduit $p^h - i = k \cdot p^a$ où $k = p^b - j$ a un développement de base p de la forme

$$k = \beta_0 + \beta_1 p + \ldots + \beta_{b-1} p^{b-1} \tag{5}$$

avec

$$\beta_0 = p - \alpha_0, \beta_1 = p - 1 - \alpha_1, \ldots, \beta_{b-1} = p - 1 - \alpha_{b-1}.$$

Des relations précédentes, on déduit les développements de base p de i et $p^h - i$ sous la forme

$$i = \alpha_0 p^a + \alpha_1 p^{a+1} + \ldots + \alpha_{b-1} p^{a+b-1}$$

$$p^h - i = \beta_0 p^a + \beta_1 p^{a+1} + \ldots + \beta_{b-1} p^{a+b-1}.$$

D'après la formule (1) du n° 4, on a donc

$$v = v_p(p^h!) = \frac{p^h - 1}{p - 1}$$

$$v' = v_p(i!) = \frac{i - \alpha_0 - \alpha_1 - \ldots - \alpha_{b-1}}{p - 1}$$

$$v'' = v_p((p^h - i)!) = \frac{p^h - i - \beta_0 - \beta_1 - \ldots - \beta_{b-1}}{p - 1}.$$

On en déduit

$$v_p\left(\binom{p^h}{i}\right) = v - v' - v'' = \frac{(\alpha_0 + \beta_0 - 1) + (\alpha_1 + \beta_1) + \ldots + (\alpha_{b-1} + \beta_{b-1})}{p - 1} =$$

$$= b = h - a = h - v_p(i).$$

Nous avons donc terminé les démonstrations de notre résultat fondamental.

6. Nous allons traduire les résultats précédents en termes de polynômes. Pour simplifier les notations, nous considérerons des polynômes en deux indéterminées X et Y, mais les raisonnements sont parfaitement généraux et s'appliquent à un nombre quelconque d'indéterminées.

Examinons d'abord le cas $h = 1$, c'est-à-dire le théorème classique selon lequel le coefficient binomial $\binom{p}{i}$ est divisible par p pour i compris entre 1 et $p-1$. Il revient au même de dire que les coefficients du polynôme $(X+Y)^p$ sont divisibles par p à l'exception de ceux de X^p et Y^p. Autrement

dit, $(X+Y)^p$ appartient à l'ensemble W_1 de polynômes ainsi défini: les éléments de W_1 sont les polynômes à coefficients entiers en X et Y, dans lesquels le coefficient d'un monôme X^iY^j est divisible par p si i et j ne sont pas tous deux divisibles par p. Il est clair que W_1 est un groupe pour l'addition des polynômes, et qu'il se compose des combinaisons linéaires à coefficients entiers des polynômes de la forme M^p ou pM, où M est un monôme X^iY^j.

Soient A et B deux polynômes à coefficients entiers en X et Y; comme $\binom{p}{i}$ est divisible par p pour $0 < i < p$, la formule du binôme montre qu'il existe un polynôme à coefficients entiers C tel que

$$(A \pm B)^p = A^p \pm B^p + pC.$$

Si A' et B' sont deux autres polynômes de même espèce, on a donc

$$(A^p + pA') \pm (B^p + pB') = (A \pm B)^p + p(A' \pm B' - C);$$

par suite, l'ensemble des polynômes de la forme $A^p + pA'$ est un groupe W_1' pour l'addition.

Montrons que W_1' *est égal à* W_1. Rappelons d'abord la notation classique $A \equiv B \mod . p$ pour deux polynômes A et B à coefficients entiers; elle signifie que tous les coefficients de $A-B$ sont divisibles par p. On peut traduire ce qui précède par la congruence

$$(A+B)^p \equiv A^p + B^p \qquad \text{mod. } p\,. \tag{6}$$

Soit alors A un polynôme de la forme $c_1M_1 + \ldots + c_rM_r$, où $c_1, \ldots, c_r$ sont des entiers et $M_1, \ldots, M_r$ des monômes; en tenant compte de la relation d'Euler $c^p \equiv c \mod . p$ (pour tout entier c) et de la congruence (6), on démontre par récurrence sur r la congruence

$$A^p \equiv c_1M_1^p + \ldots + c_rM_r^p \qquad \text{mod. } p\,. \tag{7}$$

Si A' est un autre polynôme à coefficients entiers, $A^p + pA'$ est congru modulo p à $c_1M_1^p + \ldots + c_rM_r^p$; pour qu'un polynôme soit de la forme $A^p + pA'$, il faut et il suffit par suite qu'il soit une combinaison linéaire à coefficients entiers de monômes du type $c_1M_1^p + \ldots + c_rM_r^p + pc_1M_1' + \ldots + pc_s'M_s'$. Ceci prouve que W_1 et W_1' sont égaux.

7. Dans le cas $h = 2$, les propriétés de divisibilité des coefficients binomiaux $\binom{p^2}{i}$ sont résumées dans le tableau suivant:

$$\begin{array}{l} 0 \ldots\ldots p \ldots\ldots 2p \ldots\ldots 3p \ldots\ldots\ldots\ldots (p-1)p \ldots\ldots p^2 \\ 1 \underbrace{\quad\quad} p \underbrace{\quad\quad} p \underbrace{\quad\quad} p \qquad\qquad\qquad\qquad p \underbrace{\quad\quad\quad\quad} 1 \\ \quad\; p^2 \qquad p^2 \qquad p^2 \qquad\qquad\qquad\qquad\qquad\quad p^2 \end{array}$$

La première ligne symbolise la suite des entiers de 0 à p^2, mais on n'a explicitement indiqué que des multiples de p; dans la deuxième ligne, on a figuré en-dessous de chaque entier i de la première ligne la plus grande puissance de p divisant $\binom{p^2}{i}$. On peut donc dire que $(X+Y)^{p^2}$ est combinaison linéaire à coefficients entiers de termes de l'une des formes M^{p^2}, pM^p et p^2M où M est un monôme. Plus généralement, en raisonnant comme au n° 6, on voit que tout polynôme A^{p^2}, où A est à coefficients entiers, a la structure précédente.

De manière générale, soit h un entier positif. Nous introduisons deux ensembles de polynômes à coefficients entiers en X et Y:

a) W_h se compose des polynômes de la forme $\sum_{i,j} c_{ij}X^iY^j$ où c_{ij} est divisible par p^{h-a} si a est un entier compris entre 0 et h tel que p^a divise i et j. Il revient au même de définir W_h comme l'ensemble des combinaisons linéaires à coefficients entiers des termes de l'une des formes M^{p^h}, $pM^{p^{h-1}}$, $p^2M^{p^{h-2}}$, ..., $p^{h-1}M^p$, p^hM, où M est un monôme.

b) W'_h se compose des polynômes de la forme

$$\sum_{i=0}^{h} p^i A_i^{p^{h-i}} = A_0^{p^h} + pA_1^{p^{h-1}} + \ldots + p^{h-1}A_{h-1}^p + p^hA_h,$$

où A_0, ..., A_h sont des polynômes à coefficients entiers.

Nous prouverons au n° suivant que W_h *et* W'_h *sont égaux*. Voici un corollaire immédiat: le théorème sur la divisibilité des coefficients binomiaux $\binom{p^h}{i}$ exprime que le polynôme $\frac{1}{p}\,[(X+Y)^{p^h} - X^{p^h} - Y^{p^h}]$ appartient à W_{h-1}. Comme on a $W_{h-1} = W'_{h-1}$, il existe donc des polynômes A_1, ..., A_h à coefficients entiers en X et Y, pour lesquels on a l'identité

$$(8) \qquad (X+Y)^{p^h} = X^{p^h} + Y^{p^h} + pA_1^{p^{h-1}} + p^2A_2^{p^{h-2}} + \ldots + p^hA_h\,.$$

Par exemple, pour $p = 3$, $h = 2$, on a

$$A_1 = X^2Y + XY^2\,,\quad A_2 = (X^8Y + XY^8) + 4(X^7Y^2 + X^2Y^7) + \\ + 9(X^6Y^3 + X^3Y^6) + 13(X^5Y^4 + X^4Y^5),$$

et pour $p = 5$, $h = 2$, on a

$$A_1 = (X^4Y + XY^4) + 2(X^3Y^2 + X^2Y^3)\,,$$

$$A_2 = \sum_{i=1}^{12} a_i(X^{25-i}Y^i + X^iY^{25-i})$$

avec le tableau suivant de coefficients

i	1	2	3	4	5	6	7	8	9	10	11	12
a_i	1	12	92	506	2.125	7.082	19.218	43.230	81.639	130.600	178.070	207.736

8. Passons à la démonstration de l'égalité $W_h = W'_h$. Nous raisonnerons par récurrence sur l'entier positif h. Il est clair que W_0 et W'_0 se composent de tous les polynômes à coefficients entiers en X et Y. Supposons désormais que l'on ait $h \geqq 1$ et $W_{h-1} = W'_{h-1}$. Soient A et B deux polynômes à coefficients entiers; d'après la formule du binôme et les propriétés de divisibilité des coefficients $\binom{p^h}{i}$, le polynôme $(A+B)^{p^h} - A^{p^h} - B^{p^h}$ est somme de termes du type

$$c p^{h-a} A^{j p^a} B^{k p^a}$$

avec des entiers positifs c, a, j et k tels que $a < h$ et $j + k = p^{h-a}$. Chacun des termes précédents est de la forme $p \,.\, c p^{h-a-1} C^{p^a}$, donc appartient au groupe additif $p W'_{h-1} = p W_{h-1}$. On a donc établi la congruence

$$(9) \qquad (A+B)^{p^h} \equiv A^{p^h} + B^{p^h} \qquad \text{mod. } p W_{h-1} \,.$$

Soit alors $A = c_1 M_1 + \ldots + c_r M_r$ un polynôme à coefficients entiers; dans cette formule, $c_1, \ldots, c_r$ sont des entiers et $M_1, \ldots, M_r$ des monômes. En raisonnant par récurrence sur r et en utilisant les congruences $c_i^{p^h} \equiv c_i$ mod . p, on déduit de (9) la congruence

$$(10) \qquad A^{p^h} \equiv c_1 M_1^{p^h} + \ldots + c_r M_r^{p^h} \qquad \text{mod. } p W_{h-1} \,.$$

La construction même de W_h et W'_h montre que W_h se compose des polynômes de la forme $c_1 M_1^{p^h} + \ldots + c_r M_r^{p^h} + pB$, où $c_1, \ldots, c_r$ sont des entiers, $M_1, \ldots, M_r$ des monômes et B un élément de W_{h-1}; par ailleurs, W'_h se compose des polynômes de la forme $A^{p^h} + pB$ avec B dans W'_{h-1}. L'égalité postulée $W_{h-1} = W'_{h-1}$ et la congruence (10) entraînent l'égalité $W_h = W'_h$.

9. Expliquons sur un exemple élémentaire les principes du calcul de Witt, en les déduisant de l'égalité $W_h = W'_h$. Nous considérons des polynômes à coefficients entiers en des indéterminées $X_0, X_1, \ldots, X_h$, $Y_0, Y_1, \ldots, Y_h$, et les ensembles W_h et W'_h correspondants. Nous introduirons les polynômes

$$F_h = X_0^{p^h} + p X_1^{p^{h-1}} + \ldots + p^h X_h$$

$$G_h = Y_0^{p^h} + p Y_1^{p^{h-1}} + \ldots + p^h Y_h.$$

Il est clair que ces polynômes appartiennent à W_h, et l'on se convainc aisément qu'il en est de même des polynômes $F_h + G_h$, $F_h - G_h$ et $F_h G_h$.

Comme on a $W_h = W'_h$, il existe donc des polynômes à *coefficients entiers* S_i, D_i et P_i (pour $0 \leqq i \leqq h$) satisfaisant aux relations

$$F_h + G_h = S_0^{p^h} + pS_1^{p^{h-1}} + \ldots + p^h S_h \tag{11}$$

$$F_h - G_h = D_0^{p^h} + pD_1^{p^{h-1}} + \ldots + p^h D_h \tag{12}$$

$$F_h G_h = P_0^{p^h} + pP_1^{p^{h-1}} + \ldots + p^h P_h. \tag{13}$$

Nous noterons par ailleurs V_h l'ensemble des « vecteurs » $\mathbf{a} = (a_0, a_1, \ldots, a_h)$ dont les $h+1$ composantes sont des entiers modulo p, et Z_h l'ensemble des entiers modulo p^{h+1}. Les ensembles V_h et Z_h ont le même nombre fini p^{h+1} d'éléments. Nous allons définir une bijection T_h de V_h sur Z_h, c'est-à-dire un « codage » des entiers modulo p^{h+1} au moyen de suites de $h+1$ entiers modulo p. Tout d'abord, la formule du binôme et les congruences $\binom{p}{i} \equiv 0 \mod p$ pour $0 < i < p$ entraînent le résultat suivant: si x et y sont deux entiers congrus modulo p^i, les entiers x^p et y^p sont congrus modulo p^{i+1}. Soient $x_0, x_1, \ldots, x_h, y_0, y_1, \ldots, y_h$ des entiers; les congruences

$$x_0 \equiv y_0,\ x_1 \equiv y_1,\ \ldots,\ x_h \equiv y_h \quad \mod p \tag{14}$$

entraînent alors la congruence

$$x_0^{p^h} + px_1^{p^{h-1}} + \ldots + p^h x_h \equiv y_0^{p^h} + py_1^{p^{h-1}} + \ldots + p^h y_h \quad \mod p^{h+1}. \tag{15}$$

Réciproquement, on montre par récurrence sur h que la congruence (15) entraîne les congruences (14): en effet, le résultat étant supposé vrai pour $h-1$, on déduit de (15) les congruences $x_i^p \equiv y_i^p \mod p$ pour $0 \leqq i \leqq h-1$; la congruence d'Euler $x^p \equiv x \mod p$ permet alors de conclure qu'on a $x_i \equiv y_i \mod p$ pour $0 \leqq i \leqq h-1$; de (15), on tire alors $p^h x_h \equiv p^h y_h \mod p^{h+1}$, d'où $x_h \equiv y_h \mod p$.

La définition de T_h est maintenant aisée: étant donné un vecteur $\mathbf{a} = (a_0, a_1, \ldots, a_h)$ appartenant à V_h, on choisit des représentants x_0 pour a_0, x_1 pour $a_1, \ldots, x_h$ pour a_h, et $T_h(\mathbf{a})$ est la classe de l'entier $x_0^{p^h} + px_1^{p^{h-1}} + \ldots + p^h x_h$ modulo p^{h+1}. La bijection T_h permet de transporter de Z_h à V_h les opérations de somme, différence et produit. D'autre part, $S_0, S_1, \ldots, S_h$ étant des polynômes à coefficients entiers, on peut substituer aux variables des entiers modulo p dans ces polynômes, et le résultat est un entier modulo p. La formule (11) et la définition de T_h montrent que la somme de deux vecteurs $\mathbf{a} = (a_0, a_1, \ldots, a_h)$ et $\mathbf{b} = (b_0, b_1, \ldots, b_h)$ est le vecteur $\mathbf{c} = (c_0, c_1, \ldots, c_h)$ donné par

$$c = S(a_0, a_1, \ldots, a_h; b_0, b_1, \ldots, b_h) \text{ pour } 0 \leqq i \leqq h.$$

De manière analogue, la différence et le produit de **a** et **b** se calculent en utilisant respectivement les polynômes D_i et P_i.

En résumé, les opérations de somme, différence et produit dans l'ensemble des entiers modulo p permettent de définir un calcul polynomial pour les entiers modulo p, et les polynômes S_i, D_i et P_i permettent d'introduire dans l'ensemble V_h des vecteurs $\mathbf{a} = (a_0, a_1, ..., a_h)$ des opérations de somme, différence et produit. Le calcul ainsi défini dans V_h est le *calcul de Witt* (1936); la bijection T_h permet en principe de ramener les calculs algébriques sur les entiers modulo p^{h+1} à des calculs analogues (mais plus compliqués) sur les entiers modulo p.

Pour terminer, explicitons le cas $p = 5$, $h = 1$; nous représentons chaque classe de congruence modulo 5 ou 25 par le plus petit entier positif qu'elle contient, de sorte que $T_1(x, y)$ est le reste de la division par 25 de $x^5 + 5y$. Le tableau suivant donne les valeurs de $T_1(x, y)$:

y \ x	0	1	2	3	4
0	0	1	7	18	24
1	5	6	12	23	4
2	10	11	17	3	9
3	15	16	22	8	14
4	20	21	2	13	19

Les opérations sur les vecteurs sont les suivantes:

$$(a_0, a_1) + (b_0, b_1) = (a_0+b_0,\ a_1+b_1-a_0^4b_0-2a_0^3b_0^2-2a_0^2b_0^3-a_0b_0^4)$$

$$(a_0, a_1) - (b_0, b_1) = (a_0-b_0,\ a_1-b_1+a_0^4b_0-2a_0^3b_0^2+2a_0^2b_0^3-a_0b_0^4)$$

$$(a_0, a_1)(b_0, b_1) = (a_0b_0,\ a_1b_0^5+a_0^5b_1).$$

On en déduit par exemple $(2, 3) + (4, 1) = (1, 0)$, et T_1 transforme cette relation en la congruence $22 + 4 \equiv 1 \bmod. 25$.

Institut de recherche mathématique avancée
Rue René-Descartes, 67
Strasbourg

(Reçu le 1er novembre 1969)