Etudes

Factorielles et coefficients binomiaux Factorisations et congruences

J. BOUTELOUP
Rouen

1 - Introduction

Cette étude m'a été inspirée par un article de Ian STEWART ("*Pour la Science*", juillet 1988) et n'a jamais été publiée. Un exercice proposé dans le *Bulletin* 393 sur les coefficients binomiaux me l'a remise en mémoire, et j'ai pensé qu'elle pourrait intéresser certains collègues. Dans cette étude, p désigne un **entier premier**.

Si l'entier naturel n est tel que : $n = p^a.q$ avec q premier avec p, nous écrivons : $f_p(n) = a$, autrement dit, si p figure dans la décomposition de n en facteurs premiers, alors $f_p(n)$ est son exposant, sinon, $f_p(n) = 0$. Il résulte immédiatement de cette définition que : $f_p(n.n') = f_p(n) + f_p(n')$.

L'écriture française usuelle C_n^k représente le coefficient binomial traduit par $\binom{n}{k}$ en notation anglo-américaine.

2 - Résultat fondamental sur la factorielle

Soit : $n = \sum_{i=0}^{r} a_i \cdot p^i$. $0 \leq a_i \leq p-1$, définissant l'écriture unique de n en base p. Il suffit de prendre r égal à l'indice du dernier coefficient non nul; mais, lorsque cette notation sera utilisée pour plusieurs entiers, nous pourrons supposer que r est le même en ajoutant éventuellement des coefficients égaux à 0.

Nous avons le résultat fondamental :

$$f_p(n!) = \frac{1}{p-1} \cdot \sum_{i=1}^{r} a_i(p^i - 1) = \frac{1}{p-1} \cdot \left(n - \sum_{i=0}^{r} a_i\right)$$

Une démonstration par récurrence de cette relation, sous sa forme de droite est très simple.

La formule est évidente pour $n = 1$, donnant: $0 = 0$. Supposons-la vraie pour n. On a $f_p((n+1)!) = f_p(n!) + f_p(n+1)$.

• Si $a_0 \neq p-1$, $n+1 = (a_0+1) + \sum_{i=1}^{r} a_i p^i$, $f_p(n+1) = 0$, et $f_p((n+1)!) = f_p(n!)$, comme l'indique la formule.

• Supposons $a_0 = a_1 = \ldots = a_{j-1} = p-1$, $a_j < p-1$. On a :

$$n = (p-1)\sum_{i=0}^{j-1} p^i + a_j p^j + \sum_{i=j+1}^{r} a_i p^i \quad \text{et} \quad (p-1)\frac{p^j - 1}{p-1} = p^j - 1$$

d'où $n+1 = (a_j+1).p^j + \sum_{j+1}^{r} a_i p^i$, ($r$ pouvant être supposé $\geq j+1$)

$$f_p((n+1)!) = f_p(n!) + f_p(n+1) = f_p(n!) + j.$$

Or, dans la formule, la somme des a_i diminue de $j(p-1) - 1$. Le crochet augmente de $j(p-1)$, et le deuxième membre augmente bien de j.

Il est possible de donner de ce résultat une démonstration directe. Nous proposons au lecteur de démontrer en exercice : $f_p(n!) = \sum_{i=1}^{r} [E(n/p^i)]$, E désignant la partie entière. $E(n/p^i) = a_i + a_{i+1}.p + \ldots + a_r p^{r-i}$ Le coefficient de a_j dans la somme est : $p^{j-1} + p^{j-2} + \ldots + p + 1 = (p^j - 1)/(p-1)$ et l'on retrouve le résultat initial sous la forme de gauche.

3 - Résultats fondamentaux sur les coefficients binomiaux

Soient : $n = \sum_0^r a_i p^i$, $k = \sum_0^r b_i p^i$, $n-k = \sum_0^r c_i p^i$.

On a : $f_p\left(C_n^k\right) = f_p(n\,!) - f_p(k\,!) - f_p\left((n-k)!\right) =$

$$\frac{1}{p-1}\cdot\left[n-k-(n-k)-\sum_0^r a_i+\sum_0^r b_i+\sum_0^r c_i\right], \text{ d'où}$$

$$\boxed{f_p\left(C_n^k\right) = \frac{1}{p-1}\cdot\sum_0^r (b_i + c_i - a_i)}$$

Considérons l'addition en base p : $k + (n-k) = n$. Posons : $\varepsilon_i = 1$ s'il y a une retenue au rang i, $\varepsilon_i = 0$ s'il n'y en a pas.

Nous avons : $\quad b_0 + c_0 - a_0 = p\varepsilon_0$.

Pour $1 \leq i \leq r-1$: $\quad b_i + c_i - a_i = p\varepsilon_i - \varepsilon_{i-1}$

$$b_r + c_r - a_r = -\varepsilon_{r-1}$$

ε_r étant égal à 0, car sinon $a_{r+1} \neq 0$.

Nous obtenons par addition membre à membre :

$$\sum_0^r (b_i + c_i - a_i) = (p-1)\cdot\sum_0^{r-1} \varepsilon_i$$

D'où le résultat fondamental :

$\boxed{f_p\left(C_n^k\right) \text{ est égal au nombre de retenues de l'additions en base } p \quad k + (n-k) = n.}$

Nous en déduisons en particulier les équivalences logiques conduisant à ce qu'on peut nommer le théorème de Lucas généralisé :

$\boxed{f_p\left(C_n^k\right) = 0 \Leftrightarrow C_n^k \text{ non multiple de } p \Leftrightarrow \text{Pas de retenues dans l'addition de } k \text{ et } n-k \text{ en base } p \Leftrightarrow \forall i,\ b_i + c_i = a_i \Leftrightarrow \forall i\ ,\ b_i \leq a_i.}$

Le théorème de Lucas était relatif au cas de $p = 2$, et caractérisait donc C_n^k impair.

4 - Factorisations des coefficients binomiaux. Applications. Exemples.

Nous pouvons obtenir une décomposition de C_n^k en facteurs premiers en appliquant ce qui précède aux entiers premiers successifs.

Notons que la relation : $n! = k!\,(n-k)!\,C_n^k$ entraîne que tout facteur premier de C_n^k est $\leq n$. D'autre part, si p est un entier premier tel que : Sup $(k, n-k) < p \leq n$, il apparaît dans la décomposition de $n!$, donc dans celle de C_n^k. L'hypothèse sur p entraîne l'expression de k et $n-k$ en base p avec un seul terme, d'où une seule retenue. Tout facteur de ce type apparaît donc dans la décomposition de C_n^k avec l'exposant 1. Il suffit donc de déterminer les facteurs premiers $p \leq \text{Sup}(k, n-k)$.

Prenons l'exemple de C_{40}^{15}. Nous effectuons les additions de 15 et 25 en bases 2, 3, 5,7, I1, 13, 17, 19, 23. Nous trouvons des nombres de retenues respectivements égaux à 5, 2, 0, 0, 0, 1, 1, 1, 0.

Par exemple en base 2, $15 = 1 + 2 + 4 + 8 = 1111$,
$25 = 1 + 8 + 16 = 11001$

$$\begin{array}{r} 15 \\ +\,25 \\ \hline = 40 \end{array} \qquad \begin{array}{r} 1111 \\ +\,11001 \\ \hline = 101000 \end{array} \quad \text{(5 retenues)}.$$

Nous en déduisons : $C_{40}^{15} = 2^5 \times 3^2 \times 13 \times 17 \times 19 \times 29 \times 31 \times 37$.

Nous pouvons ainsi résoudre tout problème utilisant cette décomposition, notamment ceux du p.g.c.d. et du p.p.c.m., avec cas particuliers de divisibilités.

Dans le cas de p.g.c.d., il suffit évidemment de déterminer la partie de la décomposition contenant les facteurs intervenant dans le second nombre. Proposons-nous, par exemple, de trouver les p.g.c.d. de C_{60}^{21} avec 60 et 21. Nous avons : $60 = 2^2 \times 3 \times 5$, $21 = 3 \times 7$. Il nous suffit d'essayer 2, 3, 5, 7. Les additions de 21 et 39 en bases 2, 3, 5, 7 donnent respectivement 3, 1, 2, 1 retenues. Donc, $C_{60}^{21} = 2^3 \times 3 \times 5^2 \times 7 \times \ldots$. Nous en concluons que C_{60}^{21} est divisible par 60 et 21. Reprenons l'exemple de C_{40}^{15} ; $40 = 2^3 \times 5$; $15 = 3 \times 5$ montrent que nous n'avons plus de divisibilités, les p.g.c.d. avec

40 et 15 étant 8 et 3.

Il est intéressant de montrer, en utilisant ce qui précède, que C_n^k est toujours divisible par n lorsque n et k sont premiers entre eux (c'est l'objet du problème 218 - *Bulletin* n° 393).; En effet, si p^j apparaît dans la décomposition de n, k n'est pas divisible par p. On a $a_i = 0$ pour $i < j$, et $b_0 \neq 0$, ce qui nécessite au moins j retenues, d'où C_n^k divisible par p^j. La justification directe résulte de l'application du théorème de Gauss à la relation : $k.C_n^k = n.C_{n-1}^{k-1}$.

Les exemples ci-dessus montrent que la propriété peut être réalisée lorsque n et k ne sont pas premiers entre eux, sans l'être obligatoirement. L'exemple élémentaire de $C_3^2 = 3$ montre que la divisibilité par k peut ne pas être réalisée, même dans le cas de n et k premiers entre eux.

5 - Congruences remarquables relatives à la factorielle

Soit : $n! = p^\lambda.u$, avec $\lambda = f_p(n!)$, donc u premier avec p. On a le résultat remarquable :

$$u \equiv [(p-1)!]^\lambda . \prod_{i=0}^{r} (a_i!) \qquad [p]$$

avec la convention classique $0! = 1$.

Nous démontrons cette formule par récurrence, le résultat étant évident pour $n = 1$. La formule étant supposée vérifiée pour n, nous utilisons les résultats du paragraphe 2.

- Si $a_0 \neq p-1$, nous passons à $n+1$ en conservant λ, en changeant a_0 en $a_0 + 1$, donc en multipliant de second membre par $a_0 + 1$, et en remplaçant u par $u' = (n+1)u \equiv (a_0 + 1)$ (modulo p). La formule est encore vérifiée.
- Si $a_0 = \ldots = a_{j-1} = p-1$, $a_j < p-1$, λ est remplacé par $\lambda + j$, les j premiers coefficients passent de $p-1$ à 0, a_j est remplacé par $a_j + 1$, les autres coefficients étant inchangés. L'exposant de $(p-1)!$ ne change pas et le second membre est multiplié par $a_j + 1$. Si u est remplacé par u', on a : $(n+1).p^\lambda.u = p^{\lambda+j}.u'$, avec $n + 1 = p^j.v$ *et* $v \equiv a_j + 1$, d'où $u' \equiv (a_j + 1).u$. La formule est encore vérifiée.

Le célèbre théorème de Wilson affirme, p étant premier, que $(p-1)! + 1$ est multiple de p, donc que $(p-1)! \equiv -1$, modulo p. La formule s'écrit sous la

forme très simple :

$$\boxed{u \equiv (-1)^{\lambda} . \prod_{i=0}^{r} (a_i\ !)}$$

6 - Un exemple d'application

Trouver le nombre t de zéros à droite de l'écriture décimale de $n!$, ainsi que le chiffre des unités de $(n!)/10^t$.

Nous faisons le calcul pour $n = 1000$.

En base 2, 1000 s'écrit 1111101000, d'où $f_2(1000!) = 1000 - 6 = 994$.

En base 5, 1000 s'écrit 13000, d'où $f_5(1000!) = (1000 - 4)/4 = 249$.

Ainsi, $1000! = 5^{249} \times 2^{994} \times u = 10^{249} \times 2^{745} \times u$.

Il y a 249 zéros et le chiffre des unités demandé est congru à $2^{745} \times u$, modulo 10. Il suffit de le connaître modulo 5, puisqu'il est pair. Le résultat fondamental nous donne, modulo 5 :

$$2^{994} \times u \underset{[5]}{\equiv} (-1)^{249} \times 3! \underset{[5]}{\equiv} 4$$

Donc : $4 \equiv 2^{994} \times u = 2^{745} \times u \times 2^{249}$, avec $2^{249} = (2^4)^{62} \times 2 \equiv 2$, d'où :

$$2^{745} \times u \equiv 2, \text{ et le chiffre des unités est 2.}$$

7 - Congruences remarquables aux coefficients binomiaux.

Soient $n! = p^{\lambda}.u$, $k! = p^{\mu}.v$, $((n-k)! = p^{\nu}.w$, avec u, v, w premiers avec p. On a :

$$C_n^k . p^{\mu+\nu} . v . w = p^{\lambda} . u \text{ , d'où } C_n^k = p^{\alpha} . t \text{ , } t \text{ premier avec } p,$$

$$\alpha = \lambda - \mu - \nu = f_p\left(C_n^k\right), \ t.v.w = u.$$

Les résultats du paragraphe 4 permettent de mettre en évidence des entiers t_1, u_1, v_1, w_1 congrus à t, u, v, w modulo p, avec :

$$u_1 = \prod_{0}^{r} (a_i!) \text{ , } v_1 = \prod_{0}^{r} (b_i!) \text{ , } w_1 = \prod_{0}^{r} (c_i!)$$

$$t_1 . v_1 . w_1 \equiv (-1)^{\alpha} u_1$$

ce qui permet de calculer t_1 modulo p, les classes de v_1 et w_1 étant inversibles sur $\mathbb{Z}/p\,\mathbb{Z}$

Un résultat particulièrement intéressant est obtenu lorsque $f_p\left(C_n^k\right) = 0$.

On a $\forall i,\ c_i = a_i - b_i$, d'où $\frac{u_1}{v_1 w_1} = \prod_0^r C_{a_i}^{b_i}$. Nous obtenons ainsi la congruence remarquable modulo p :

$$C_n^k \text{ non multiple de } p \Rightarrow C_n^k \equiv \prod_0^i \left(C_{a_i}^{b_i}\right)$$

Ce résultat est classique. On en trouvera notamment une démonstration intéressante, différente, dans l'article de Vincent Lefèvre pour "*Quadrature*" n°12.

Bien entendu, ce résultat n'est intéressant que pour les entiers premiers p suffisamment faibles. Si $p > n$, les développements de n et k se réduisent à leur premier terme, et le résultat devient : $C_n^k \equiv C_n^k$, simple vérification !

8 - Cas particulier. Exemples

Le résultat est trivial pour $p = 2$: (C_n^k impair congru à 1).

Il est par contre intéressant d'examiner le cas particulier $p = 3$. Dans l'hypothèse de $f_3\left(C_n^k\right) = 0$, $\prod\left(C_{a_i}^{b_i}\right) = 2^s$ s'il y a s couples pour lesquels $a_i = 2$, $b_i = 1$. On obtient donc une congruence à 1 si ce nombre de couples est pair, à 2 s'il est impair.

Reprenons l'exemple C_{40}^{15}, factorisé au paragraphe 4. Les écritures de 40 et 15 en base 5 : 130 et 30 nous conduisent à la congruence à 1 modulo 5. En base 7, nous obtenons 55 et 21 correspondant à la congruence à 50, donc à 1, modulo 7. En base 11, nous obtenons 37 et 14 correspondant à la congruence à 3×35, donc à 6 modulo 11.

9 - Congruence modulo un entier primaire

Nous désignons $n!$ ou C_n^k par x, et supposons que $f_p(x) = \lambda$ (λ quelconque, égal ou non à 0). On a $x = p^\lambda.u$, et nous savons trouver un entier u_2, tel que $0 < u_2 < p$ congru à u modulo p. Le développement de x correspondant à son écriture en base p s'écrit : $x = p^\lambda.u_2 + p^{\lambda+1}.q$.

Soit $\alpha > 0$. Modulo p^α, x est congru à 0 si $\alpha \leq \lambda$, à $p^\lambda.u_2$ si $\alpha = \lambda + 1$. Notons que, dans le cas de $p = 2$, $u_2 = 1$; il n'y a pas d'autre détermination à faire que celle de λ.

Par contre, ce qui précède nous donne des renseignements insuffisants pour la congruence modulo p^α lorsque $\alpha > \lambda + 1$. Nous rencontrons là un problème très difficile, même dans le cas très particulier de $p = 2$, $\lambda = 0$, $\alpha = 2$, c'est-à-dire de la congruence modulo 4 pour x impair, qui peut être 1 ou 3. Ce problème ne sera donc pas abordé dans cette étude.

Reprenons l'exemple de C_{40}^{15}. Dans le cas de $p = 2$, on a $\lambda = 5$. On a donc la congruence à 32 modulo 64. Modulo 128, il y a ambiguïté entre 32 ou 96. Dans le cas de $p = 3$, les écritures de 40, 15, 25 en base 3 : 1111, 120, 221 conduisent aux valeurs : $3^{18}.u$, $3^6.v$, $3^{10}.w$ pour les factorielles correspondantes, avec $u \equiv 1$, $v \equiv 2$, $w \equiv 4 \equiv 1$. En notant que, sur $\mathbb{Z}/3\mathbb{Z}$ inverse de 2 est 2, on obtient finalement la valeur $3^2.t$, avec $t \equiv 2$. Il en résulte que C_{40}^{15} est congru à 18 modulo 27. Modulo 81, il y a ambiguïté entre 18, 45 ou 63.

Etudions, pour finir, le cas de $p = 13$. Les écritures de 40, 15, 25 en base 13 sont : 31, 12, 1(12). Donc $40! = 13^3.u$, avec $u \equiv (-1)^3 \times 6 \equiv 7$; $15! = 13.v$, avec $v \equiv (-1) \times 2! \equiv 11$; $25! = 13.w$, avec $w \equiv (-1) \times 12! \equiv 1$ (Wilson). Sur $\mathbb{Z}/3\mathbb{Z}$, l'inverse de 11 est 6. On a $7 \times 6 \equiv 3$.

Finalement, $C_{40}^{15} = 3 \times 13 + 169q$, est congru à 39 modulo 169.

10 - Utilisation du théorème chinois

Soit $s = \prod_i^j q_i$, les q_i étant premiers entre eux 2 à 2.

Supposons que nous ayons, pour tout i, une congruence : $x \equiv u_i$ modulo q_i. Le théorème chinois nous amène à déterminer des entiers v_i tels que : $\frac{v_i s}{q_i} \equiv 1$ modulo q_i. De tels entiers existent car l'hypothèse entraîne que si $\frac{s}{q_i}$ est premier avec q_i donc que sa classe est un élément inversible de $\mathbb{Z}/q_i\mathbb{Z}$.

Le théorème affirme alors que $x \equiv \sum_i \frac{u_i . v_i . s}{q_i}$ modulo s.

Utilisons les résultats obtenus sur $x = C_{40}^{15}$ pour deux exemples :

- $s = 27 \times 11 = 297$. On a : $x \equiv 18$ modulo 27, $x \equiv 6$ modulo 11. $v_1 \times 11 \equiv 1$ modulo 27 a pour solution $v_1 = 5$; $v_2 \times 27 \equiv 1$ modulo 11 a pour solution $v_2 = 9$. Nous avons donc, modulo 297 :

$x \equiv 18 \times 5 \times 11 + 6 \times 9 \times 27 = 2448 \equiv 72$.

- $s = 5 \times 7 \times 11 = 385$. On a $x \equiv 1$ modulo 5 et 7. Les congruences $v_1 \times 77 \equiv 1$, modulo 5 ; $v_2 \times 55 \equiv 1$, modulo 7, $v_3 \times 35 \equiv 1$ modulo 11 ont pour solutions $v_1 = 3$, $v_2 = -1$, $v_3 = 6$. Nous obtenons donc, modulo 385 : $x \equiv 1 \times 3 \times 77 + 1 \times (-1) \times 55 + 6 \times 6 \times 35 = 1436 \equiv 281$.