Valuations p-adiques dans les factorisations des factorielles (Denise Vella-Chemla, 13.7.2017)

Lucas consacre dans sa théorie des nombres un paragraphe à la divisibilité des factorielles. Il fournit une procédure pour trouver la puissance d'un nombre premier p dans la factorisation de la factorielle d'un nombre entier n. Prenons un exemple ; pour connaître la puissance de 7 dans la factorielle de 10000, on divise successivement 10000 par 7, en obtenant comme quotients successifs 1428, 204, 29 et 4 et on ajoute ces quotients pour obtenir la valuation p-adique de 7 dans 10000 ! et qui est 1428+204+29+4=1665.

En réfléchissant un peu à cette idée, on réalise qu'un nombre premier p est à puissance 0 dans la factorisation de la factorielle de tout nombre qui lui est inférieur, à puissance 1 dans toute factorisation de la factorielle d'un entier de l'intervalle $[p, 2p[$ et à puissance supérieure à 1 pour les factorielles des nombres supérieurs ou égaux à $2p$.

Un nombre composé se distingue d'un nombre premier par le fait qu'il est à puissance au moins 2 dans la factorisation de sa propre factorielle (par exemple, 6 dans la factorielle de 6 apparaît "en tant que lui-même" mais également comme produit de ses 2 sous-facteurs 2 et 3 qui sont dans la factorielle l'un et l'autre séparément).

Cette propriété qu'un nombre premier p apparaît à puissance de 1 dans la factorisation de sa factorielle fournit une fonction qui permet de distinguer les nombres premiers des nombres composés (cette fonction associe à un nombre sa factorielle, puis extrait du nombre obtenu la valuation p-adique du nombre en question) ; les nombres premiers sont les seuls antécédents de 1 par cette fonction.

Ces propriétés permettent à nouveau d'illustrer ce que l'on peut entendre par "coïncidence de fonctions" : représentons le début de la droite numérique ainsi que les premiers nombres premiers. Représentons par des intervalles de valeurs ce qui a été énoncé ci-dessus. La deuxième ligne montre que la valuation p-adique de 3 dans les factorisations des factorielles des nombres compris entre 3 inclus et 6 exclus vaut 1 (et 0 pour des nombres inférieurs à 3 et plus que 1 pour des nombres supérieurs ou égaux à 6).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	8	19	20	21	22	23
2	0	[	1	[							>1												
3		0	[	1		[							>1										
5			0		[		1			[						>1							

203. Divisibilité des factorielles. — Nous commencerons par résoudre le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre a qui ne surpasse pas un nombre donné n.*

Une première méthode, directe, consiste à calculer le Tableau des puissances successives de a, jusqu'à ce que l'on obtienne un exposant α tel que l'on ait

$$a^{\alpha} \leqslant n < a^{\alpha+1},$$

et l'exposant cherché est α; on peut déterminer ainsi, par exemple, le plus grand exposant de la puissance de 2 contenue dans un nombre donné (n° 189, Remarque II).

Mais, au lieu d'employer les multiplications successives par a, on peut aussi employer les divisions successives par a. Cette méthode repose sur le théorème suivant : *Si q désigne le quotient par défaut de la division de n par a, et si q' désigne le quotient par défaut de la division de q par b, le nombre q' est égal*

au quotient par défaut de la division de n par le produit ab. En effet, on a par définition,

$$n = aq + r, \qquad q = bq' + s,$$

r désignant l'une des valeurs 0, 1, 2, ..., $(a-1)$, et s l'une des valeurs 0, 1, 2, ..., $(b-1)$. On déduit

$$n = abq' + (as + r);$$

mais le nombre non négatif $(as + r)$ est au plus égal à

$$a(b-1) + (a-1) \quad \text{ou} \quad (ab-1);$$

donc q' est le quotient exact, ou approché par défaut, de la division de n par ab.

On désigne habituellement le plus grand nombre entier contenu dans $\frac{n}{a}$ par la notation $\mathrm{E}\frac{n}{a}$, que l'on prononce *entier de n par a* : on a donc

$$\mathrm{E}\frac{\mathrm{E}\frac{n}{a}}{b} = \mathrm{E}\frac{n}{ab},$$

et cette formule s'applique, en général, à l'entier de $\frac{n}{abc\ldots}$.

Cela posé, nous résoudrons le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre premier p contenue dans le produit n! des n premiers nombres.* Les entiers qui contiennent p en facteur dans la factorielle $n!$ sont tous les multiples de p

$$p, 2p, 3p, \ldots, \mathrm{E}\frac{n}{p}p, \qquad \text{en nombre } \mathrm{E}\frac{n}{p};$$

par suite, l'exposant de p dans cette factorielle est égal à l'exposant de p dans le produit

$$1.2.3\ldots.\mathrm{E}\frac{n}{p},$$

augmenté du dernier facteur. En répétant le même raisonnement sur cette nouvelle factorielle, et en appliquant le théorème précédent, il en résulte que l'exposant du nombre premier p dans la

factorielle $n!$ est égal à la somme

$$\mathrm{E}\frac{n}{p} + \mathrm{E}\frac{n}{p^2} + \mathrm{E}\frac{n}{p^3} + \dots.$$

Lorsque n est une puissance de p, les quotients de n par $p, p^2, p^3, \dots$, sont tous entiers, et l'on trouve pour l'exposant cherché

$$\frac{n-1}{p-1}.$$

Si l'on écrit le nombre n dans le système de numération de base p, en supposant

$$n = a + bp + cp^2 + dp^3 + \dots,$$

on trouve facilement que l'exposant cherché a pour valeur

$$\frac{n-(a+b+c+\dots)}{p-1},$$

et a pour limite supérieure

$$\frac{n}{p-1}.$$

Exemple I. — Quel est l'exposant de 7 dans le produit des 10000 premiers nombres?

On dispose le calcul de la manière suivante :

10000	7						
30	1428	7					
20	028	204	7				
60	0	64	29	7			
4		1	1	4			

et le nombre cherché est

$$1428 + 204 + 29 + 4 = 1665.$$

Exemple II. — Le produit des 1000 premiers nombres se termine par 249 zéros.

Exemple III. — Trouver le plus grand exposant de la puissance du nombre premier p contenue dans le nombre combinatoire C_m^n.

On a

$$\mathrm{C}_m^n = \frac{m!}{n!(m-n)!},$$