# Ecrit 2, problème 2. Quelques théorèmes d'arithmétique

Le sujet est disponible sur le site du CAPES : http://capes-math.org/data/uploads/EP2_2013.pdf

## Eléments de correction

### Partie A : Théorème de Lagrange

**1**. Pour tout entier $n \geq 1$ et tout entier $k$ de $[1\,;\,n]$, $\binom{n-1}{k-1}$ est défini et : $n \times \binom{n-1}{k-1} = \frac{n \times (n-1)!}{(n-k)!(k-1)!} = k \times \frac{n!}{(n-k)!\,k!} = k \times \binom{n}{k}$

**2.** Le résultat de la première question peut s'appliquer quel que soit l'entier $k$ de $[1\,;\,p-1]$: $k \times \binom{p}{k} = p \times \binom{p-1}{k-1}$. L'entier $p$ divise le produit $k \times \binom{p}{k}$ et, puisque c'est un nombre premier, il est premier avec tous les entiers strictement positifs qui le précèdent, en particulier avec $k$. D'après le théorème de Gauss, il divise $\binom{p}{k}$.

**3.1.** Compte tenu de la définition de $f$ : $f(x+1) = \prod_{k=1}^{k=p-1}(x+1+k) = \prod_{k=2}^{k=p}(x+k)$. Par rapport à l'expression de $f(x)$ on note l'absence du facteur $(x+1)$ associé à l'indice 1 et la présence d'un terme supplémentaire $(x+p)$ associé à l'indice $p$. Par conséquent :

$(x+1) \times f(x+1) == \prod_{k=1}^{k=p}(x+k) = (x+1) \times \prod_{k=1}^{k=p-1}(x+k) = (x+p)\,f(x)$, ce qui revient à la relation à démontrer.

**3.2.** L'expression de $f(x)$ est un produit de $p-1$ facteurs du premier degré en $x$. C'est donc la forme factorisée d'un polynôme de degré $p-1$ en $x$. D'où l'existence d'un $p$-uplet de nombres réels associé à sa forme développée. Les racines de ce polynôme sont par construction les entiers de – 1 à $1-p$. Or les coefficients d'un polynôme sont tous fonctions symétriques des racines, cocktails de sommes et de produits : le $p$-uplet de nombres réels est donc un $p$-uplet d'entiers.

**3.3.** Le terme de plus haut degré est le produit de tous les termes en $x$ qui ont tous pour coefficient 1, et le terme constant est le produit de tous les termes constants donc des entiers $k$ depuis 1 jusqu'à $p-1$.

**3.4.** $p\,a_k$ est le coefficient du terme de degré $p-1-k$ du polynôme $p\,f(x)$. Compte tenu de la question 1, c'est aussi celui du terme de même degré du polynôme $(x+1)\,f(x+1) - x\,f(x)$. Il s'agit de déterminer ce coefficient.
Dans $x\,f(x)$, c'est $a_{k+1}$

D'autre part : $(x+1)\,f(x+1) = (x+1)\sum_{i=0}^{i=p-1} a_i (x+1)^{p-1-i} = \sum_{i=0}^{i=p-1} a_i (x+1)^{p-i}$ .

En faisant intervenir le binôme de Newton : $\sum_{i=0}^{i=p-1} a_i (x+1)^{p-i} = \sum_{i=0}^{i=p-1} a_i \left( \sum_{j=0}^{j=p-i} \binom{p-i}{j} x^{p-i-j} \right)$.

Si $i > k+1$, $p-i < p-k-1$ et il n'y a pas de terme de degré $p-1-k$ dans la parenthèse ci-dessus.
Si $i = k+1$, on obtient un tel terme pour $j = 0$ et ce terme a pour coefficient $a_{k+1}$. Celui-ci est neutralisé par le terme de degré $p-1-k$ figurant dans $x\,f(x)$.

Si $i < k+1$, on obtient un tel terme pour $j = k+1-i$ et ce terme a pour coefficient $a_i \binom{p-i}{k+1-i}$.

Il s'agit en fin de compte de sommer de $i = 0$ jusqu'à $i = k$ et le coefficient recherché est $\sum_{i=0}^{i=k} a_i \binom{p-i}{k+1-i}$.

D'où la relation de l'énoncé.

**3.5.** En appliquant la relation précédente pour $k = 1$ : $p\,a_1 = \sum_{i=0}^{i=1} \binom{p-i}{2-i} a_i = \binom{p}{2} a_0 + \binom{p-1}{1} a_1 = \binom{p}{2} a_0 + (p-1) a_1$ ce qui donne $a_1 = \binom{p}{2} a_0$.

Plus généralement, en sortant les termes d'indices 0 et $k$ de la sommation de la question précédente : $p\,a_k = \sum_{i=0}^{i=k} a_i \binom{p-i}{k+1-i} = \binom{p}{k+1} + \sum_{i=1}^{i=k-1} a_i \binom{p-i}{k+1-i} + a_k \times (p-k)$.

Finalement : $k\,a_k = \binom{p}{k+1} + \sum_{i=1}^{i=k-1} a_i \binom{p-i}{k+1-i}$

**3.6.** Soit $p$ un entier premier impair. Alors $p-1$ est un entier pair et $a_1 = p \times \frac{p-1}{2}$ est divisible par $p$.
Soit $j$ tel que $1 < j \leq p-3$ et supposons que les coefficients de rangs 1, 2, …, $j$ soient tous divisibles par $p$.
Alors : $(j+1)\,a_{j+1} = \binom{p}{j+2} + \sum_{i=1}^{i=j} \binom{p-i}{j+2-i} a_i$. Au second membre, tous les termes de la somme sont divisibles par $p$ d'après l'hypothèse de récurrence et $\binom{p}{j+2}$ l'est aussi d'après la question 2 (l'entier $j+2$ précède $p$, la question 2 peut s'appliquer). Donc, $(j+1)\,a_{j+1}$ est divisible par $p$ comme somme de termes tous divisibles par $p$. Mais l'entier $j+1$ est un précédent de $p$, il est premier avec $p$. D'après le théorème de Gauss, $p$ divise $a_{j+1}$ : la divisibilité par $p$ est héréditaire jusqu'à l'héritier de rang $p-2$.
Il en résulte que $p$ divise tous les $a_i$ pour $1 < i \leq p-2$

## Partie B : Théorème de Wilson

**1.**R.A.S.

**2.** En appliquant la relation **3.4** au rang $p-1$ :

$$p\,a_{p-1} = p(p-1)! = p! = \sum_{i=0}^{i=p-1} \binom{p-i}{p-i} a_i = a_0 + \sum_{i=1}^{i=p-2} a_i + a_{p-1} = 1 + \sum_{i=1}^{i=p-2} a_i + (p-1)!$$

D'après le théorème de Lagrange, tous les termes de $\sum_{i=1}^{i=p-2} a_i$ sont divisibles par $p$. En passant la relation précédente à la congruence modulo $p$ il reste : $1 + (p-1)! \equiv 0\ (p)$, ce qu'on voulait.

**3.** Réciproquement, soit $p$ un entier ≥ 2 et tel que $(p-1)! \equiv -1\ (p)$. Ou bien $p = 2$ auquel cas $p$ est premier, ou bien $p > 2$ et pour tout entier $k$ tel que $1 < k \leq p-1$, il existe un entier $u$ : $k \times \frac{(p-1)!}{k} = -1 + pu$. L'égalité de Bézout est vérifiée et $k$ est premier avec $p$. Le nombre $p$ est un entier ≥ 3 premier avec tous ses précédents, c'est alors un nombre premier impair.

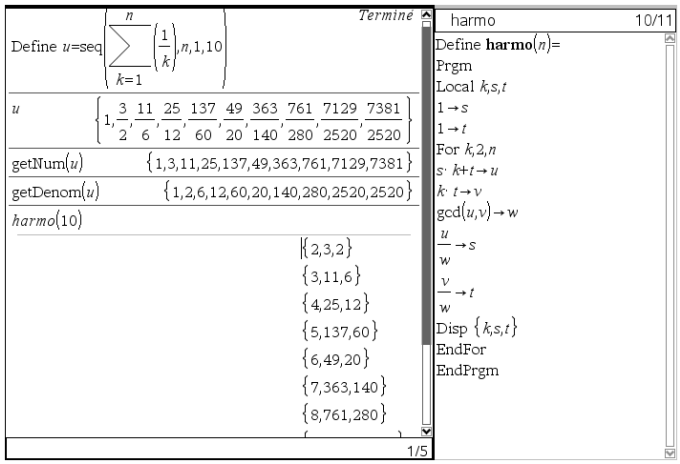
**4.1.** Par hypothèse la décomposition en produit de facteurs premiers de $n$ est de la forme : $n = {p_1}^{k_1} \times {p_2}^{k_2} \times n'$ . Les trois entiers ${p_1}^{k_1}$, ${p_2}^{k_2}$ et $n'$ figurent comme facteurs distincts dans la factorielle $(n-1)!$ (ils sont tous les trois < $n$ et sont premiers entre eux deux à deux). Le nombre $(n-1)!$ est multiple de leur produit, donc de $n$. D'où la congruence.

**4.2.** Par hypothèse, puisque l'exposant $\alpha$ est plus grand que 2, $n$ est de la forme : $n = p \times p^{\alpha-1} \times n'$ avec $1 < p < p^{\alpha-1} < n$ et $n'$ premier avec $p$. Les trois entiers $p$, $p^{\alpha-1}$ et $n'$ sont trois facteurs distincts dans la factorielle $(n-1)!$. Le nombre $(n-1)!$ est multiple de leur produit, donc de $n$.

**4.3.** Puisque $p$ est un entier premier impair, $p > 2$ et donc $p^2 > 2p$. Les entiers $p$ et $2p$ figurent comme facteurs distincts dans la factorielle $(n-1)!$. Le nombre $(n-1)!$ est multiple de leur produit, donc de $n$.

## Partie C : Théorème de Wolstenholme

**1.** et **2**.
Deux façons d'obtenir les entiers demandés. On remarque que $s_4 = 25$, que $s_6 = 49$ et que $s_{10} = 7381 = 121 \times 61$




**3**. Le coefficient $a_{p-2}$ est celui du terme du premier degré du polynôme $f$.

En général, pour un polynôme de degré $n$ dont la forme factorisée est $\prod_{k=1}^{k=n}(x - r_k)$, le coefficient du premier degré est $(-1)^{n-1}(r_2 \ldots r_n + r_1 r_3 \ldots r_n + \ldots + r_1 r_2 \ldots r_{n-1})$ qu'il est plus commode d'écrire : $(-1)^{n-1}(r_1 \ldots r_n)\left(\frac{1}{r_1} + \frac{1}{r_2} + \ldots + \frac{1}{r_n}\right)$

Ici, $p$ étant un nombre premier strictement supérieur à 3 (donc impair et au moins égal à 5), le polynôme $f$ en question est un polynôme de degré $p-1$, donc de degré pair et au moins égal à 4, dont les racines sont les entiers de – 1 à $1-p$, déjà mentionnées plus haut.

Dans l'expression précédente, l'exposant de -1 est un nombre impair, le produit des racines est le nombre $(p-1)!$ et la parenthèse vaut $\left(-\frac{1}{1}-\frac{1}{2}-...-\frac{1}{p-1}\right)$. Au bout du compte : $a_{p-2}=(p-1)!\left(1+\frac{1}{2}+...+\frac{1}{p-1}\right)=(p-1)!H_{p-1}$

**4.** $f(-p)=\prod_{k=1}^{k=p-1}(k-p)$. En effectuant le changement d'indice $j=p-k$, une expression équivalente en est : $f(-p)=\prod_{j=1}^{j=p-1}(-j)=(p-1)!$

On obtient ainsi que : $f(-p)=(p-1)!=(-p)^{p-1}+a_1(-p)^{p-2}+....+a_{p-2}(-p)+a_{p-1}$. Compte tenu que $(p-1)!=a_{p-1}$, il apparaît que : $(-p)^{p-1}+a_1(-p)^{p-2}+....+a_{p-2}(-p)=0$ c'est-à-dire, en tenant compte des parités, que : $a_{p-2}=(p)^{p-2}-a_1(p)^{p-3}+....+a_{p-3}p=p^2\left(p^{p-4}-a_1p^{p-5}...-a_{p-4}\right)+a_{p-3}p$.

D'après la partie précédente, $a_{p-3}$ est divisible par *p*, donc $a_{p-3}\ p$ est divisible par $p^2$. Il s'ensuit que $a_{p-2}$ est lui-même divisible par $p^2$.

De $H_{p-1}=\frac{a_{p-2}}{(p-1)!}=\frac{s_{p-1}}{t_{p-1}}$ on déduit la relation : $t_{p-1}\,a_{p-2}=s_{p-1}\,(p-1)!$. Le nombre $p^2$ divise ce nombre entier et est premier avec $(p-1)!$, il divise $s_{p-1}$