

Solution du problème d'arithmétique

d'après Capes 2013

Partie A: Théorème de Lagrange

1. Nous avons, pour $k \in \{1, 2, \dots, n\}$,

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n \cdot (n-1)!}{k \cdot (k-1)! \cdot (n-1-k+1)!} = \frac{n}{k} \cdot \frac{(n-1)!}{(k-1)! \cdot (n-1-k+1)!} = \frac{n}{k} \binom{n-1}{k-1}$$

2. Soit p un entier premier. Alors p divise $p!$. Or, pour tout $k \in \{0, 1, \dots, p\}$, $p! = k! \cdot (p-k)! \cdot \binom{p}{k}$. Enfin, si $1 \leq k \leq p$, alors p ne divise ni $k!$, ni $(p-k)!$: aussi, p est-il premier avec $k! \cdot (p-k)!$. Il s'ensuit par le théorème de Gauss que p divise $\binom{p}{k}$.

Théorème de Gauss Si $a|bc$ et $a \wedge b = 1$, alors $a|c$

Méthode En général, il faut partir d'un membre pour aller à l'autre ici, il est plus simple de reformuler ce que l'on veut obtenir en isolant $(x+1)f(x+1)$, et en effectuant les regroupements / changement d'indice appropriés.

De façon plus formelle, on écrit les coordonnées du polynôme F dans la base $(1, X, X^2, \dots, X^{p-1})$ de $\mathbb{R}_{p-1}[X]$. Pour ce faire, il faut identifier la fonction polynomiale f avec le polynôme $F(X) = \sum_{k=1}^{p-1} (X+k)$

3. (a) Nous avons $f(x) = \prod_{k=1}^{p-1} (x+k)$ d'où $(x+1)f(x+1) = (x+1) \prod_{k=1}^{p-1} (x+1+k) = (x+1) \prod_{k=2}^p (x+k) = \prod_{k=1}^p (x+k) = \prod_{k=1}^{p-1} (x+k) \cdot (x+p) = (x+p)f(x)$. Aussi, nous avons la relation

$$(x+1)f(x+1) = (x+p)f(x)$$

d'où nous déduisons que $pf(x) = (x+1)f(x+1) - xf(x)$

- (b) La fonction f étant une fonction polynomiale de degré $p-1$, on en déduit qu'il existe un p -uplet $(a_0, a_1, \dots, a_{p-1})$ de réels tels que $f(x) = \sum_{k=0}^{p-1} a_k x^{p-1-k}$.
- (c) En considérant le développement du produit $\prod_{k=1}^{p-1} (x+k)$, nous en déduisons que le coefficient dominant de f est 1 et son coefficient constant est $\prod_{k=1}^{p-1} k = (p-1)!$ d'où nous obtenons par identification $a_0 = 1$ et $a_{p-1} = (p-1)!$.
- (d) Calculons $(x+1)f(x+1)$:

$$\begin{aligned} (x+1)f(x+1) &= (x+1) \sum_{k=0}^{p-1} a_k (x+1)^{p-1-k} = \sum_{k=0}^{p-1} a_k (x+1)^{p-k} \\ &= \sum_{k=0}^{p-1} a_k \sum_{j=0}^{p-k} \binom{p-k}{j} x^j \end{aligned}$$

Aussi, en injectant ce résultat dans la formule de la question **A.3.4** nous en déduisons que

$$\begin{aligned} pf(x) &= (x+1)f(x+1) - xf(x) \\ &= \sum_{k=0}^{p-1} a_k \sum_{j=0}^{p-k} \binom{p-k}{j} x^j - \sum_{k=0}^{p-1} a_k x^{p-k} \\ &= \sum_{k=0}^{p-1} a_k \left(\sum_{j=0}^{p-k} \binom{p-k}{j} x^j - x^{p-k} \right) \\ &= \sum_{k=0}^{p-1} a_k \sum_{j=0}^{p-1-k} \binom{p-k}{j} x^j \\ &= \sum_{j=0}^{p-1} \left(\sum_{k=0}^{p-1-j} a_j \binom{p-k}{j} \right) x^j \end{aligned}$$

On en déduit alors que $pf(x) = \sum_{k=0}^{p-1} \left(\sum_{j=0}^k \binom{p-j}{p-1-k} a_j \right) x^{p-1-k}$. Aussi, par identification des coefficients, nous en déduisons que

$$p \cdot a_k = \sum_{j=0}^{p-1} \binom{p-j}{p-1-k} a_j = \sum_{j=0}^k \binom{p-j}{k+1-j} a_j$$

- (e) Pour $k=1$, nous avons $pa_1 = \binom{p}{2}a_0 + \binom{p-1}{1}a_1 = \frac{p(p-1)}{2}a_0 + (p-1)a_1$ donc $a_1 = \frac{p(p-1)}{2}a_0 = \binom{p}{2}a_0$.
Pour $k \in \{2, 3, \dots, p\}$, nous obtenons

$$\begin{aligned} pa_k &= \sum_{j=0}^{k-1} \binom{p-j}{k+1-j} a_j + \binom{p-k}{1} a_k \\ &= \sum_{j=0}^{k-1} \binom{p-j}{k+1-j} a_j + (p-k)a_k \end{aligned}$$

On en déduit alors que

$$ka_k = \sum_{j=0}^{k-1} \binom{p-j}{k+1-j} a_j = \binom{p}{k+1} a_k + \sum_{j=1}^{k-1} \binom{p-j}{k+1-j} a_j$$

Calculs techniques: il faut utiliser le binôme de Newton pour développer $(x+1)^{p-k}$ et terminer en intervertissant les deux sommes: puisque la seconde dépend de l'indice de la première, il faut faire attention. On remarquera que l'une des bornes est quand $j = p-1-k$ soit $k = p-1-j$

Rappelons que $pf(x) = \sum_{k=0}^{p-1} pa_k x^{p-1-k}$; on identifie alors les coefficients de x^{p-1-k} dans les deux membres

- (f) Raisonnons donc par récurrence finie sur l'entier naturel $k \in \{1, 2, \dots, p-2\}$.
 Initialisation: Pour $k = 1$, nous avons $a_1 = \binom{p}{2}$ et donc d'après la question **A.2** nous savons que $p|a_1$ (puisque $p \geq 3$).
 Hérédité: Supposons que p divise $a_1, a_2, \dots, a_{k-1}$. Alors, p divise $\binom{p}{k+1} + \sum_{j=1}^{k-1} \binom{p-j}{k+1-j} a_j$ d'où p divise k . Mais comme $k < p$, $p \wedge k = 1$ et donc par le théorème de Gauss, $p|ka_k$ implique $p|a_k$.

Si p est un nombre premier et $k \in \{1, 2, \dots, p-1\}$, alors $p \wedge k = 1$

Partie B: Théorème de Wilson

- Pour $p = 2$, nous avons $(p-1)! = 1$ d'où comme $1 \equiv -1 \pmod{2}$, il s'ensuit que la formule est vraie pour $p = 2$.
- (a) Nous savons que $a_{p-1} = (p-1)!$ donc nous déduisons de la formule **A.3.5** que, pour $k = p-1$ nous avons

$$(p-1) \cdot (p-1)! = \sum_{j=0}^{p-2} \binom{p-j}{p-1+1-j} a_j = \sum_{j=0}^{p-2} a_j$$

Il s'ensuit alors que $p! = \sum_{j=0}^{p-2} a_j + (p-1)! = 1 + \sum_{j=1}^{p-2} a_j + (p-1)!$.

- (b) Nous savons par **A.2** que si $1 \leq k \leq p-1$, $p| \binom{p}{k}$; aussi, nous en déduisons que $(p-1)! \equiv -1 \pmod{p}$.
- Raisonnons par l'absurde en supposant que p un nombre non premier, donc qu'il existe $d \in \mathbb{N}^*$ un diviseur strict de p (ie. $1 < d < p$). Alors d apparaît dans le produit $(p-1)! = \prod_{k=1}^{p-1} k$ d'où $d|(p-1)!$. De plus, $d|p$ d'où de la relation de congruence $(p-1)! \equiv -1 \pmod{p}$, nous déduisons que $d|-1$, d'où $p \in \{-1, 1\}$ ce qui est absurde ($p > 1$). Aussi, nous démontrons que si $(p-1)! \equiv -1 \pmod{p}$, alors p est un nombre premier, ce qui établit la réciproque du théorème de Wilson.
- (a) Supposons l'existence de deux entiers a et b , avec $a, b \neq 1$, $a \wedge b = 1$ tels que $n = ab$. Aussi, $a < n$ et $b < n$ (car sinon cela implique que a ou b égal 1, ce qui serait absurde). Aussi, $2 \leq a < b \leq n-1$ et donc les nombres a et b apparaissent dans le produit $(n-1)! = \prod_{k=1}^{n-1} k$ d'où nous déduisons que $n|(n-1)!$ et par suite $(n-1)! \equiv 0 \pmod{n}$.
 (b) Soit donc $n = p^\alpha$ avec p premier et $\alpha \geq 2$. Nous avons alors $1 < p < n$ d'où $p, p^2, p^3, \dots, p^{\alpha-1}$ sont des entiers deux à deux différents apparaissant dans le produit $(n-1)! = \prod_{k=1}^{n-1} k!$. Il s'ensuit donc que $p^{1+2+\dots+\alpha-1}$ divise $(n-1)!$, d'où en particulier $p^\alpha|n$. Il s'ensuit alors que $(n-1)! \equiv 0 \pmod{n}$.
 (c) Supposons à présent que $n = p^2$ avec p premier. Aussi, $1 < p < p^2$. Comme $2 \leq p$ et $n > 4$, nous en déduisons que $2p < n$. Aussi, les entiers p et $2p$ apparaissent dans le produit $(n-1)! = \prod_{k=1}^{n-1} k$ d'où $(p \times 2p)|(n-1)!$ ce qui implique que $p^2|(n-1)!$ soit $n|(n-1)!$. Aussi $(n-1)! \equiv 0 \pmod{n}$.

Un entier n non premier est dit composé; il est alors produit de deux entiers naturels strictement compris entre 1 et n

Si n a au moins deux facteurs premiers, alors $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$. On pose $a = p_1^{\alpha_1}$ et $b = \prod_{j=2}^k p_j^{\alpha_j}$ et on a $n = ab$ avec $a \wedge b = 1$

Le fait que $\alpha \geq 3$ implique que $\alpha - 1 \geq 2$: aussi, il y a bien au moins 2 diviseurs p et $p^{\alpha-1}$ d'où leur produit p^α apparaît dans $(n-1)!$

Partie C: Théorème de Wolstenholme

Partie moins classique que les précédentes. A ne faire qu'en seconde / troisième lecture

- Nous avons $H_{n+1} = H_n + \frac{1}{n+1} = \frac{(n+1)s_n + t_n}{(n+1)t_n}$
- Nous obtenons $s_4 = 25 = 5^2$, $s_6 = 49 = 7^2$ et $s_{10} = 7381 = 61 \cdot 121 = 61 \cdot 11^2$.
- Nous avons $f(x) = \prod_{k=1}^{p-1} (x+k) = \sum_{k=0}^{p-1} a_k x^{p-1-k}$. Aussi, par identification des coefficients, nous obtenons que

$$a_{p-2} = \sum_{k=1}^{p-1} \prod_{\substack{j=1 \\ j \neq k}}^{p-1} j = \sum_{k=1}^{p-1} \frac{(p-1)!}{k} = (p-1)! \cdot H_{p-1}$$

Aussi, $H_{p-1} = \frac{a_{p-2}}{(p-1)!}$.

4. Pour $p \geq 3$, p premier, $f(-p) = (-1)^{p-1} \prod_{k=1}^{p-1} (p-k) = (p-1)! = \sum_{k=0}^{p-1} (-1)^k a_k p^{p-1-k}$.
Comme $p-1$ est un nombre pair, il s'ensuit que

$$\begin{aligned} (p-1)! &= p^{p-1} - a_1 p^{p-2} + \dots - a_{p-2} p + a_{p-1} \\ &= p^{p-1} - a_1 p^{p-2} + \dots + a_{p-3} p^2 - a_{p-2} p + (p-1)! \end{aligned}$$

Il s'ensuit alors que $a_{p-2} = p^{p-2} - a_1 p^{p-3} + \dots + a_{p-3} p = p \cdot (p^{p-3} - a_1 p^{p-4} + \dots + a_{p-3})$.

5. Comme tous les coefficients $a_1, a_2, \dots, a_{p-3}$ sont divisibles par p , nous déduisons que $p | (p^{p-3} - a_1 p^{p-4} + \dots + a_{p-3})$. Il s'ensuit donc que $p^2 | a_{p-2}$. Aussi, de $H_{p-1} = \frac{a_{p-2}}{(p-1)!} = \frac{a_{p-2}}{t_{p-1}}$ on déduit $(p-1)! \cdot s_{p-1} = a_{p-2} t_{p-1}$ soit $p^2 | (p-1)! \cdot s_{p-1}$. Or, comme $p^2 \wedge (p-1)! = 1$ nous déduisons du lemme de Gauss que $p^2 | s_{p-1}$ d'où le résultat souhaité.