

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.

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 $(x+1)f(x+1)$:

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 $F(X) = \prod_{k=1}^{p-1} (X+k)$

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

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

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

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

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

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 $k = p-1-j$

- (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

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

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

On en déduit alors que

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

(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 $p|a_k$.

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 apparait 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 apparait dans $(n-1)!$

EC 131 Analyse avancée

1. Techniquement, pour s'assurer que $\ell \in I$, il faut l'hypothèse I fermée (important pour pouvoir appliquer la continuité de f en ℓ)

2. Moralité: Quand f est croissante, (u_n) est monotone et sa monotonie est donnée par le signe de $u_1 - u_0$

1. Supposons donc la suite (u_n) convergente vers le réel ℓ . Alors, comme pour tout entier naturel n , $u_{n+1} = f(u_n)$, par passage à la limite quand n tend vers $+\infty$, on a par continuité de f en ℓ : $f(\ell) = \ell$. Ainsi, **si** la suite (u_n) converge, **alors** c'est vers un point fixe de f sur I .
2. (a) Par croissance de f on a $f(u_0) \geq f(u_1)$ soit $u_2 \geq u_1$. En appliquant $n - 1$ fois la fonction f à cette inégalité, on obtient $u_{n+1} \geq u_n$ d'où la suite (u_n) est croissante.
 (b) On procède de même: en appliquant la fonction $f^n = \underbrace{f \circ f \circ f \circ \dots \circ f}_n$, nous obtenons que $u_n \geq u_{n+1}$ d'où la suite (u_n) est décroissante.
 (c) Lorsque $u_0 = u_1$, l'application de f^n implique que $u_{n+1} = u_n$ d'où la suite (u_n) est constante.
3. (a) Il est aisé de constater que $\forall x \in \mathbb{R}$, $f(x) \geq 0$, donc on restreint l'intervalle d'étude de f à $\mathbb{R}_+$. La fonction f est clairement croissante sur $\mathbb{R}_+$. Aussi, étudions le signe de $u_1 - u_0$. $u_1 - u_0 = f(u_0) - u_0 = \frac{1}{2}(1 + u_0^2 - 2u_0) = \frac{1}{2}(u_0 + 1)^2 > 0$ d'où par **2a.** la suite (u_n) est croissante.
 (b) On résoud alors $f(x) = x$ ce qui donne $\frac{(x-1)^2}{2} = 0$ soit $x = 1$. Ainsi, l'unique point fixe de f est 1. Comme (u_n) est une suite croissante, elle est soit convergente (admet une limite finie) soit divergente vers $+\infty$. Enfin, d'après la question **1.**, nous savons que si la suite (u_n) converge, alors c'est vers un point fixe $\ell = 1$.
 (c) Etudions donc les deux cas $|u_0| > 1$ et $|u_0| \leq 1$ séparément.
 • $|u_0| > 1$: Nous avons donc $u_0^2 > 1$ d'où $u_0^2 + 1 > 1$ et finalement $u_1 > 1$. On constate donc que, par le même raisonnement, nous avons $\forall n \in \mathbb{N}^*$, $u_n > 1$. La suite (u_n) étant croissante, elle ne peut alors pas converger vers 1 d'où elle diverge.
 • $|u_0| \leq 1$. Supposons donc $|u_0| \leq 1$, c'est-à-dire $-1 \leq u_0 \leq 1$. Alors par élévation au carré nous avons $0 \leq u_0^2 \leq 1$ d'où $1 \leq u_0^2 + 1 \leq 2$ et finalement $0 \leq u_1 \leq 1$. En raisonnant par itération, nous obtenons que $\forall n \in \mathbb{N}$, $|u_n| \leq 1$, d'où la suite (u_n) est bornée. Comme elle est croissante et majorée, elle est convergente et d'après la question **1.**, sa limite est nécessairement 1. Aussi dans ce cas, (u_n) est une suite convergente de limite 1.
4. (a) Classiquement, la composée de fonction décroissante est une fonction croissante...
Formellement: Si $a < b$ alors $f(a) > f(b)$ et donc $f \circ f(a) < f \circ f(b)$ d'où $f \circ f$ est croissante.
 (b) Déjà par la question **2** appliquée à $f \circ f$, nous savons que les suites (u_{2n}) et (u_{2n+1}) sont monotones. Supposons $u_0 < u_2$. On en déduit alors que la suite (u_n) est croissante. En appliquant f qui est une fonction décroissante, nous obtenons alors $f(u_0) < f(u_2)$ soit $u_1 > u_3$ et donc la suite (u_{2n+1}) est décroissante. On prouve alors bien dans ce cas ($u_0 < u_2$) que les suites (u_{2n}) et (u_{2n+1}) sont de monotonies contraires. On procède de même dans le cas $u_0 > u_2$.
5. (a) La fonction f définie sur $\mathbb{R}$ par $f : x \mapsto \frac{\pi}{2} \cos^2(x)$ est dérivable et nous avons $f'(x) = -\pi \cos(x) \sin(x)$. Sur $]0, \pi/2[$, les fonctions $\cos$ et $\sin$ étant strictement positives, la fonction f' est strictement négative sur $]0, \pi/2[$. Ainsi, f est-elle strictement décroissante sur $]0, \pi/2[$.
 Enfin, comme $f(0) = \frac{\pi}{2}$ et $f(\pi/2) = 0$, elle réalise une bijection de $I = [0; \pi/2]$ dans lui-même. Aussi, l'intervalle I est stable par f .
 (b) Considérons la fonction g définie sur I par $g(x) = f(x) - x$. g est dérivable et $g'(x) = f'(x) - 1 < 0$. Aussi, la fonction g est-elle strictement décroissante sur I . Ainsi réalise-t-elle une bijection de $[0, \pi/2]$ dans $[g(\pi/2), g(0)] = [-\pi/2; \pi/2]$; aussi ne s'annule-t-elle qu'une unique fois sur I et donc f admet un unique point fixe sur I . Remarquons que $\cos(\pi/4) = \sqrt{2}/2$ d'où $\cos^2(\pi/4) = \frac{1}{2}$ et finalement $f(\pi/4) = \pi/4$ (soit $g(\pi/4) = 0$). Ainsi, $\pi/4$ est l'unique point fixe de f dans I .

Je ne détaille pas: formellement il faut démontrer via une récurrence... ce qui ne présente aucune difficulté

4.a Notation: on a envie d'écrire f^2 au lieu de $f \circ f$: ce n'est pas interdit mais c'est dangereux (confusion avec $f \times f$). Aussi faut-il bien comprendre de quoi l'on parle!

5a Pour pouvoir appliquer le théorème de la bijection, nous devons indiquer la stricte décroissance de la fonction f . Pour l'obtenir le plus simple est de considérer l'intervalle ouvert $]0, \pi/2[$ sur lequel f' est toujours strictement négative

5.b Introduire la fonction $g(x) = f(x) - x$ et étudier son sens de variation! La valeur du point fixe étant donnée, il suffit de vérifier que $f(\pi/4) = \pi/4$ (c'est bien plus simple que de trouver la valeur de x pour laquelle $f(x) = x$)

- (c) Nous avons $u_0 = \pi/3$ donc comme $\cos(\pi/3) = 1/2$ nous avons $f(\pi/3) = \pi/8$. $u_2 = f(u_1) = \frac{\pi}{2} \cos^2(\pi/8) = \frac{\pi}{4}(\cos(\pi/4) + 1) = \frac{\pi}{8}(2 + \sqrt{2})$.
 Finalement $u_2 - u_0 = \frac{\pi}{8}(2 + \sqrt{2}) - \frac{\pi}{3} = \frac{\pi}{24}(6 + 3\sqrt{2} - 8) > 0$. Aussi, la suite (u_{2n}) est croissante et la suite (u_{2n+1}) est décroissante par **4**.

- (d) Nous savons que $u_0 = \pi/3$, (u_{2n}) est croissante, (u_{2n+1}) est décroissante et que la seule limite possible de (u_n) est $\pi/4$.

La fonction $f \circ f$ étant croissante, nous déduisons que la suite (u_{2n}) est croissante, d'où $\forall n \in \mathbb{N}$, $u_{2n} \geq u_0 = \frac{\pi}{3} > \frac{\pi}{4}$. Ainsi, la suite (u_{2n}) ne peut avoir pour limite $\pi/4$. Or, d'après **1**, si (u_n) converge c'est vers $\pi/4$ (cf **5b**). Il s'ensuit donc que (u_n) admet une sous-suite qui ne converge pas vers $\pi/4$ donc (u_n) ne converge pas vers $\pi/4$: elle est donc divergente.

Autre rédaction: Comme la suite (u_{2n+1}) est décroissante et de premier terme $u_1 = \pi/8$, nous avons $\forall n \in \mathbb{N}$, $u_{2n+1} \leq \pi/8 < \pi/4$. Ainsi, cette suite converge vers une limite ℓ' vérifiant $\ell' \leq \frac{\pi}{8} < \frac{\pi}{4}$. Aussi, (u_n) admet deux sous-suites convergentes vers des limites ℓ et ℓ' différentes, donc la suite (u_n) est divergente.

Il faut donc calculer le signe de $u_2 - u_0$ d'où déjà il nous faut calculer u_2
 Rappelons que $\cos(2a) = 2\cos^2(a) - 1$

5d. Raisonnement avec les sous-suites: le comprendre! Notez que les suites (u_{2n}) et (u_{2n+1}) étant monotones et à valeur dans le fermé borné I , elles sont convergentes dans I . Leurs limites doivent être des points fixes de $f \circ f$ (et non f). Il n'est pas du tout nécessaire de calculer ses limites pour conclure à la divergence de la suite (u_n)