Lycée Louis-Le-Grand, Paris
MP2I – Mathématiques
A. Troesch

Pour le 15/03/2024

DM n° 18 : Arithmétique

Corrigé du problème 1 – Nombres de Carmichael

Partie I – Structure du groupe $(\mathbb{Z}/p\mathbb{Z})^*$

1. Soit pour tout $p \in \mathbb{P}$,

$$\alpha_p = \begin{cases} v_p(a) & \text{si } v_p(a) \geqslant v_p(b) \\ 0 & \text{sinon} \end{cases} \qquad \text{et} \qquad \beta_p = \begin{cases} v_p(b) & \text{si } v_p(a) < v_p(b) \\ 0 & \text{sinon} \end{cases}$$

On pose $a' = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b' = \prod_{p\in\mathbb{P}} p^{\beta_p}$. On a alors $\boxed{a' \wedge b' = 1,\ a' \mid a \text{ et } b' \mid b}$. De plus :

$$a'b' = \prod_{p\in\mathbb{P}} p^{\max(v_p(a),v_p(b))} \qquad \text{soit:} \qquad \boxed{a'b' = a \vee b}.$$

On considère alors $\boxed{x' = x^{a/a'} \text{ et } y' = y^{b/b'}}$, qui sont bien d'ordre a' et b' respectivement.

2. Comme G est abélien, on a $(x'y')^{a'b'} = (x'^{a'})^{b'}(y'^{b'})^{a'} = 1$. Ainsi, en notant c l'ordre de $x'y'$, on a $c|a'b'$.
Par ailleurs, $(x'y')^c = 1$, donc $(x')^c = (y')^{-c} \in \langle x\rangle \cap \langle y\rangle$. Notons $H = \langle x'\rangle \cap \langle y'\rangle$. Comme H est un sous-groupe de $\langle x\rangle$ et de $\langle y\rangle$, l'ordre de H divise a' et b'. Puisque a' et b' sont premiers entre eux, $H = \{1\}$; Ainsi, $(x')^c = 1$ et $(y')^c = 1$, de quoi on déduit que $a'|c$ et $b'|c$. Comme a' et b' sont premiers entre eux, $a'b'|c$.
Ainsi, $\boxed{x'y' \text{ est d'ordre } a'b' = a \vee b.}$

3. Soit $\omega(G)$ le ppcm des ordres de tous les éléments de G. En notant $x_1, \dots, x_n$ les éléments de G et $a_1, \dots, a_n$ leurs ordres, on montre sans problème par une récurrence immédiate basée sur la question précédente, que pour tout $k \in [\![1, n]\!]$, il existe un élément d'ordre $a_1 \vee \cdots \vee a_k$.
En particulier, pour $k = n$, $\boxed{\text{il existe un élément } g \in G \text{ d'ordre } \omega(G)}$.
Par définition, pour tout $g \in G$, l'ordre de g divise $\omega(G)$, donc $g^{\omega(G)} = 1$. Donc $\omega(G) \geqslant \min\{k \in \mathbb{N}^* \mid \forall g \in G,\ g^k = 1,\}$.
De plus, l'existence de g d'ordre $\omega(G)$, assure que pour tout $k \in [\![1, \omega(G) - 1]\!]$, $g^k \neq 1$, donc $\omega(G) \leqslant \min\{k \in \mathbb{N}^* \mid \forall g \in G,\ g^k = 1,\}$.
Les deux inégalités amènent : $\boxed{\omega(G) = \min\{k \in \mathbb{N}^* \mid \forall g \in G,\ g^k = 1,\}}$.

4. Tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible (car $\mathbb{F}_p$ est un corps). On rappelle que cela provient d'une relation de Bézout entre k non divisible par p et p : on trouve un inverse de k en réduisant l'égalité $uk + bp = 1$ modulo p.
Ainsi, $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z}\backslash\{0\}$, donc $\boxed{\text{son ordre est } p - 1.}$

5. Soit $P \in \mathbb{F}_p[X]$ le polynôme à coefficients dans $\mathbb{F}_p$ défini par :

$$P(X) = X^{\omega(G)} - 1.$$

Pour tout $\xi \in G$, $x^\xi = 1$, par définition de l'exposant. Donc $P(\xi) = 0$. D'après le point admis plus haut $P(X)$ est divisible par $X - \xi$). Écrivons $P(X) = (X - \xi)Q(X)$.
Soit $\xi' \neq \xi$. On a alors $P(\xi') = 0$, donc $(\xi - \xi')Q(\xi') = 0$. Comme $\xi - \xi' = 0$ et que $\mathbb{F}_p$ est un corps (donc intègre), on en déduit que $Q(\xi') = 0$, et donc qu'on peut factoriser Q par $(X - \xi')$.
En continuant de la sorte (par une récurrence immédiate), on en déduit que $\boxed{P \text{ est divisible par } \prod_{\xi\in G}(X - \xi)}$

6. L'examen des degrés nous assure alors, puisque P n'est pas le polynôme nul, que $\prod_{\xi\in G}(X-\xi) \leqslant \deg(P)$, donc que $\boxed{p-1 \leqslant \omega(G)}$.
   Comme par ailleurs, pour tout $x \in G$, $x^{p-1} = 1$ (d'après Lagrange), on en déduit, d'après la question 3, que $\omega(G) \leqslant p-1$.
   Ainsi, $\boxed{p-1 = \omega(G).}$
7. On déduit alors de la question 3 qu'il existe un élément g d'ordre $p-1$, ce qui équivaut à dire que $G = \langle x \rangle$.
   Ainsi, $\boxed{G \text{ est cyclique d'ordre } p-1.}$

Partie II – Stucture des groupes $(\mathbb{Z}/p^n\mathbb{Z})^*$

1. Il s'agit encore d'une relation de Bézout : $\boxed{k \text{ est inversible modulo } p^n}$ ssi il existe $u \in \mathbb{Z}$ tel que $ku \equiv 1\ [p^n]$, ssi il existe u et v dans $\mathbb{Z}$ tels que $ku + p^n v = 1$, ssi a et p^n sont premiers entre eux, ssi $\boxed{p \text{ ne divise pas } k}$.
2. Le nomrbe de diviseurs de p dans $[\![1, p^n]\!]$ est p^{n-1}, donc, d'après la question précédente, le nombre d'éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$ est $p^n - p^{n-1}$, soit :
   $$\boxed{|(\mathbb{Z}/p^n\mathbb{Z})^*| = \varphi(p^n) = p^{n-1}(p-1)}.$$
3. Soit $a \in \mathbb{Z}$, et $m \in \mathbb{N}^*$. D'après la formule du binôme,
   $$(1+p^m a)^p = \sum_{k=0}^{p} \binom{p}{k} p^{mk} a^k.$$
   Pour tout $k \geqslant 2$, $mk \geqslant 3m \geqslant m+2$ (car $m \geqslant 1$). De plus, pour $k = 2$, $\binom{p}{k}$ est divisible par p (car $k \in [\![1, p-1]\!]$ puisque $p \geqslant 3$ par hypothèse ; plus simplement $\binom{p}{k} = \dfrac{p(p-1)}{2}$, et $p-1$ est pair), et $2m \geqslant m+1$. Ainsi, pour $k = 2$, $\binom{p}{k} p^{mk}$ est divisible par p^{m+2}.
   On en déduit que
   $$\boxed{(1+p^m a)^p \equiv 1 + \binom{p}{1} p^m a \equiv 1 + a p^{m+1}\ [p^{m+2}]}.$$
4. On raisonne par récurrence, en notant pour $m \in \mathbb{N}^*$, $\mathcal{P}(m)$ la propriété :
   $$\forall a \in \mathbb{Z},\quad (1+pa)^{p^m} \equiv 1 + p^{m+1} a\ [p^{m+2}].$$
   - Initialisation : pour $m = 0$, c'est une évidence, puisque $(1+p)^{p^0} = 1 + p$.
   - Hérédité : Soit $m \in \mathbb{N}$. Supposons $\mathcal{P}(m)$. Nous avons alors :
     $$(1+pa)^{p^{m+1}} = ((1+pa)^{p^m})^p.$$
     Or, d'après l'hypothèse de récurrence, il existe $b \in \mathbb{Z}$ tel que $(1+pa)^{p^m} = 1 + p^{m+1}a + p^{m+2}b$. On a donc
     $$(1+pa)^{p^{m+1}} = (1 + p^{m+1}(a+pb))^p.$$
     On applique la question précédente au rang $m+1 \geqslant 1$:
     $$(1+p^{m+1}(a+pb))^p \equiv 1 + p^{m+2}(a+pb)\ [p^{m+3}],$$
     puis :
     $$(1+pa)^{p^{m+1}} \equiv 1 + p^{m+2} a\ [p^{m+3}].$$
     Il s'agit là de $\mathcal{P}(m+1)$.
   - Ainsi, d'après le principe de récurrence, on peut conclure que :
     $$\forall m \in \mathbb{N}^*,\ \forall a \in \mathbb{Z},\ \boxed{(1+pa)^{p^m} \equiv 1 + p^{m+1} a\ [p^{m+2}]}.$$

5. On a, d'après la question précédente (qu'on peut appliquer pour $n-1$ car $n \geqslant 2$),

$$(1+p)^{p^{n-1}} \equiv 1 + p^n \ [p^{n+1}] \qquad \text{donc:} \qquad (1+p)^{p^{n-1}} \equiv 1 \ [p^n].$$

On en déduit que l'ordre a de $1+p$ divise p^{n-1}. Il existe donc $\alpha \in [\![1, n-1]\!]$ tel que $a = p^\alpha$ (α ne peut pas être nul car $1+p \neq 1$ dans $\mathbb{Z}/p^n\mathbb{Z}$). Or, la question précédente amène aussi (au rang $n-2 \geqslant 0$) :

$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \ [p^n] \qquad \text{donc:} \qquad (1+p)^{p^{n-1}} \not\equiv 1 \ [p^n].$$

Ainsi, a ne divise pas p^{n-2}, donc $\alpha > n-2$. On a donc $\alpha = n-1$, et $a = p^{n-1}$.
Ainsi, $\boxed{1+p \text{ est d'ordre } p^{n-1} \text{ dans } (\mathbb{Z}/p^n\mathbb{Z})^*}$.

6. Soit $x \in \mathbb{Z}$ tel que sa classe $\overline{x}$ modulo p soit une racine primitive modulo p. Ainsi, x est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Considérons $\tilde{x}$ la classe de x modulo p^n. Comme x est premier avec p (car $\overline{x}$ est inversible), x est de même premier avec p^n. Donc $\tilde{x} \in (\mathbb{Z}/p^n\mathbb{Z})^*$. L'ordre de ce groupe étant $p^n(p-1)$, l'ordre de $\tilde{x}$ divise $p^n(p-1)$, d'après le théorème de Lagrange. Soit a l'ordre de $\tilde{x}$. Il existe donc $\alpha \in [\![0, n]\!]$ et m divisant $p-1$ tel que $a = p^\alpha m$. On a alors

$$x^{p^\alpha m} \equiv 1 \ [p^n] \qquad \text{donc:} \qquad x^{p^\alpha m} \equiv 1 \ [p].$$

Puisque $\overline{x}$ est d'ordre $p-1$, on en déduit que $p-1$ divise $p^\alpha m$, et étant premiers avec p^α, il divise m. Par conséquent $m = p-1$.
Ainsi, $\tilde{x}$ est d'ordre $p^\alpha(p-1)$, donc $tildex^{p^\alpha}$ est d'ordre $p-1$.
Il existe donc $\boxed{\text{un élément d'ordre } p-1 \text{ dans } (\mathbb{Z}/p^n\mathbb{Z})^*}$.

7. $(\mathbb{Z}/p^n\mathbb{Z})^*$ contient un élément d'ordre $p-1$, et un élément d'ordre p^{n-1}. Par conséquent $p-1$ et p^{n-1} étant premiers entre eux, il découle de la question I-2 que $(\mathbb{Z}/p^n\mathbb{Z})^*$ contient un élément y d'ordre $p^{n-1}(p-1)$. Comme il s'agit là de l'ordre du groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$, on en déduit que y engendre $(\mathbb{Z}/p^n\mathbb{Z})^*$.
Ainsi, $\boxed{(\mathbb{Z}/p^n\mathbb{Z})^* \text{ est cyclique d'ordre } p^{n-1}(p-1)}$.

Partie III – Cas des $(\mathbb{Z}/2^n\mathbb{Z})^*$

1. On suppose $n \geqslant 3$. On note $G = (\mathbb{Z}/2^n\mathbb{Z})^*$, H l'ensemble des classes modulo 2^n des entiers k congrus à 1 modulo 4, et et $K = (\{-1, +1\}, \times)$.

   (a) On a $H \subset G$ car les éléments de H sont représentés par des entiers k impairs, donc premiers avec 2^n, donc inversibles modulo 2^n. De plus :
   - $1 \equiv 1[4]$, donc $\overline{1} \in H$: H contient le neutre de $(\mathbb{Z}/2^n\mathbb{Z})^*$.
   - Soit h et k dans H, représentés par des entiers x et y de $\mathbb{Z}$. On a donc $x \equiv 1 \ [H]$ et $y \equiv 1 \ [4]$, donc $xy \equiv 1 \ [4]$, donc $hk \in H$.
   - Soit $h \in H$ représenté par x. Comme x est impair, donc premier avec 2^n, x est inversible modulo 2^n. Soit $y \in \mathbb{Z}$ un inverse modulo 2^n de x. On a alors $xy \equiv 1[2^n]$ et comme $n \geqslant 3$, $xy \equiv 1 \ [4]$. Or, comme $x \equiv 1 \ [4]$, on a $xy \equiv y \ [4]$, donc $y \equiv 1 \ [4]$. Ainsi, $\overline{y} \in H$. H est donc stable par inversion.

   On en déduit que $\boxed{H \text{ est un sous-groupe de } G}$. Son ordre est clairement $\boxed{2^{n-2}}$.

   (b) Il n'est pas dur de vérifier que K est un groupe (version multiplicative de $\mathbb{Z}/2\mathbb{Z}$).
   On définit φ de $H \times K$ dans G par :

$$\varphi(h, k) = hk.$$

   - Comme h est inversible modulo 2^n ainsi que k (égal à 1 ou -1), il en est de même de hk. Ainsi, φ est bien à valeurs dans G.
   - Soit (h, k) et (h', k') des éléments de $H \times K$. On a alors

$$\varphi((h,k) \cdot (h',k')) = \varphi(hh', kk') = hh'kk' = hkh'k' = \varphi(h,k)\varphi(h',k'),$$

     puisque G est abélien. Ainsi, φ est un morphisme.
   - Soit $(h, k) \in \mathrm{Ker}(\varphi)$. On a donc $hk = 1$ dans $\mathbb{Z}/2^n\mathbb{Z}$. Comme $k = 1$ ou $k = -1$, on en déduit que $h = 1$ ou $h = -1$ dans $\mathbb{Z}/2^n\mathbb{Z}$. Comme $n \geqslant 2$, on peut réduire modulo 4. Comme h soit être représenté par un élément congru à 1 modulo 4, on en déduit qu'on a nécessairement $h = 1$, puis $k = 1$. Ainsi, $\mathrm{Ker}(\varphi) = \{(1, 1)\}$, donc $\boxed{\varphi \text{ est injective.}}$

- G est de cardinal 2^{n-1} (représenté par les entiers impaires de $[\![2, 2^n]\!]$, ainsi que $H \times K$. Ainsi, l'injectivité et l'égalité des cardinaux finis amènent le fait que φ est bijective.
- On en déduit que $\boxed{\varphi \text{ est un isomorphisme}}$.

(c) On montre par récurrence sur $n \geqslant 3$ la propriété

$$\mathcal{P}(n) : \quad 5^{2^{n-3}} \equiv 1 + 2^{n-1} \ [2^n].$$

- Initialisation : Pour $n = 3$, c'est trivial : $5 \equiv 1 + 4 \ [8]$.
- Hérédité : Soit $n \geqslant 3$ tel que $\mathcal{P}(n)$ soit vrai. Il existe alors a tel que

$$5^{2^{n-3}} = 1 + 2^{n-1} + a2^n = 1 + 2^{n-1}(1 + 2a).$$

En élevant au carré et en développant le carré de droite, il vient :

$$5^{2^{n-2}} = 1 + 2^n(1 + 2a) + 2^{2n-2}(1 + 2a)^2.$$

Or, $n \geqslant 3$, donc $2n - 2 \geqslant n + 1$. On en déduit alors que

$$5^{2^{n-2}} \equiv 1 + 2^n \ [2^{n+1}],$$

ce qui est exactement $\mathcal{P}(n + 1)$.

- On déduit du principe de récurrence que

$$\forall n \geqslant 3, \boxed{5^{2^{n-3}} \equiv 1 + 2^{n-1} \ [2^n]}.$$

Comme H est d'ordre 2^{n-2}, le théorème de Lagrange nous affirme que l'ordre de 5 (ou plutôt de sa classe dans H) est une puissance de 2, inférieure à 2^{n-2}. Comme $5^{2^{n-3}} \not\equiv 1 \ [2^n]$ d'après la question précédente, $\boxed{\text{l'ordre de 5 ne peut alors qu'être } 2^{n-2}}$.

(d) On déduit de la question précédente que H est cyclique d'ordre 2^{n-2}, donc isomorphe à $\mathbb{Z}/2^{n-2}\mathbb{Z}$ (remarquez que cet isomorphisme nous fait passer d'une notation multiplicative à une notation additive). On a déjà remarqué que K est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Donc, d'après la question 1(b), $\boxed{(\mathbb{Z}/2^n\mathbb{Z})^* \text{ est isomorphe à } (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})}$

$\boxed{\text{Ce groupe n'est pas cyclique}}$. En effet, pour tout $x = (y, z)$ dans ce produit cartésien,

$$2^{n-2}x = (2^{n-2}y, 2^{n-2}z) = (0, 0),$$

donc il n'existe pas d'élément d'ordre 2^{n-1} (l'ordre maximal ne pouvant excéder 2^{n-2}, égal d'ailleurs à cette valeur).

2. - Cas $n = 1$: le seul élément inversible de $\mathbb{Z}/2\mathbb{Z}$ est 1, donc $\boxed{(\mathbb{Z}/2\mathbb{Z})^* = \{1\}}$ (groupe trivial)
   - Cas $n = 2$: les éléments inversibles de $\mathbb{Z}/4\mathbb{Z}$ sont 1 et 3. Donc $\boxed{(\mathbb{Z}/4\mathbb{Z})^* \text{ est d'ordre 2, donc isomorphe à } \mathbb{Z}/2\mathbb{Z}}$.

Partie IV – Nombres de Carmichael et indicateur de Carmichael

1. - Soit $n \geqslant 2$; Comme $\varphi(n)$ est l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$ (encore Bézout comme en II-1), l'ordre des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ divise $\varphi(n)$ (théorème d'Euler), donc leur ppcm aussi.
     Ainsi pour tout $n \geqslant 2$, $\boxed{\lambda(n) \text{ divise } \varphi(n)}$.
   - Si $\lambda(n) = \varphi(n)$, alors d'après le rappel en début de partie, il existe un élément x d'ordre $\lambda(n)$, donc d'ordre $\varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Pour des raisons de cardinalité, on a alors $(\mathbb{Z}/n\mathbb{Z})^* = \langle x \rangle$, donc $\boxed{(\mathbb{Z}/n\mathbb{Z})^* \text{ est cyclique}}$.
   - Réciproquement, si $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique, il existe un élément d'ordre $\varphi(n)$, donc $\varphi(n)$ divise $\lambda(n)$ par définition. Les deux divisibilités amènent l'égalité $\varphi(n) = \lambda(n)$.
   - Ainsi, $\lambda(n) = \varphi(n)$ si et seulement si $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique.
2. - Si n est premier, alors $\lambda(n) = \varphi(n)$ (car $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique), et $\varphi(n) = n - 1$. Ainsi, $\lambda(n)$ ne divise pas strictement $n - 1$.
   - Supposons alors que $\lambda(n)$ divise strictement $n - 1$. La remarque qui précède permet déjà d'affirmer que n n'est pas premier. De plus, pour tout x premier avec n, $\overline{x}$ est dans $(\mathbb{Z}/n\mathbb{Z})^*$, donc son ordre divise $\lambda(n)$ (définition de $\lambda(n)$), donc aussi $n - 1$, par hypothèse. Ainsi, $\overline{x}^{n-1} = 1$, soit $x^{n-1} \equiv 1 \ [n]$.
     On en déduit que n est un nombre de Carmichael.

- Réciproquement, supposons que n est un nombre de Carmichael. Alors pour tout x premier avec n, $\overline{x}^{n-1} = 1$, donc l'ordre de $\overline{x}$ divise $n-1$. Ceci étant vrai pour tout élément de $(\mathbb{Z}/n\mathbb{Z})^*$, le ppcm des ordres des éléments de ce groupe divise aussi $n-1$, soit $\lambda(n)$ divise $n-1$.
  De plus, on ne peut pas avoir égalité, car cela impliquerait que $\varphi(n) \geqslant n-1$, puis $\varphi(n) = n-1$, donc que tout nombre de $[\![1, n-1]\!]$ est premier avec n, donc que n est premier, ce qui est exclus par définition pour un nombre de Carmichael.
- Ainsi, $\boxed{n \text{ est de Carmichael si et seulement si } \lambda(n) \text{ divise strictement } n-1}$.

3. Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, avec $\alpha_i \geqslant 1$ et $k \geqslant 1$.
   - Le théorème chinois nous permet d'affirmer que
   $$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$
   On montre sans difficulté qu'on a alors :
   $$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*.$$
   - Il existe dans $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ un élément d'ordre $\lambda(p_i^{\alpha_i})$ (question I-3), donc en itérant I-2, il existe dans $(\mathbb{Z}/n\mathbb{Z})^*$ un élément d'ordre $\mu = \lambda(p_1^{\alpha_1}) \vee \lambda(p_2^{\alpha_2}) \vee \cdots \vee \lambda(p_k^{\alpha_k})$. Donc μ divise $\lambda(n)$.
   - Récirproquement, μ est un multiple de chaque $p_i^{\alpha_i}$, donc pour tout $i \in [\![1, k]\!]$, et tout x dans $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, l'ordre de x divise μ, donc $x^\mu = 1$. Ainsi, pour tout $(x_1, \ldots, x_k$ dans $(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*$, on a :
   $$(x_1, \ldots, x_k)^\mu = (x_1^\mu, \ldots, x_k^\mu) = (1, \ldots, 1).$$
   Donc l'ordre de tout élément de $(\mathbb{Z}/n\mathbb{Z})^*$ divise μ, donc $\lambda(n)$ divise μ.
   - On en déduit que
   $$\boxed{\lambda(n) = \mu = \lambda(p_1^{\alpha_1}) \vee \lambda(p_2^{\alpha_2}) \vee \cdots \vee \lambda(p_k^{\alpha_k})}.$$

4. Les parties précédentes nous apprennent que si p est un nombre premier impair, $\lambda(p^\alpha) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$ (car $\mathbb{Z}/p^\alpha\mathbb{Z}$ est cyclique), et que pour $p = 2$, $\lambda(2^\alpha) = 2^{\alpha-2}$ si $\alpha \geqslant 3$, $2^{\alpha-1}$ si $\alpha = 1$ ou $\alpha = 2$ (ce qui correspond aussi à l'expression obtenue pour $p > 2$). Ainsi :
   - si $v_p(2) \leqslant 2$ (donc si 8 ne divise pas n), on a :
   $$\boxed{\lambda(n) = (p_1^{\alpha_1-1}(p_1-1)) \vee (p_2^{\alpha_2-1}(p_2-1) \vee \cdots \vee (p_k^{\alpha_k-1}(p_k-1))}.$$
   - si $v_p(2) \geqslant 3$ (donc si 8 divise n), en stipulant que $p_1 = 2$, on a :
   $$\boxed{\lambda(n) = 2^{\alpha_1-2} \vee (p_2^{\alpha_2-1}(p_2-1)) \vee \cdots \vee (p_k^{\alpha_k-1}(p_k-1))}.$$

5. - Si n est un nombre de Carmichael, il est composé par définition.
     Par ailleurs, $\lambda(n)$ divise $n-1$, donc pour tout $i \in [\![1, p]\!]$, $\lambda_i(p_i^{\alpha_i})$ divise $n-1$, et l'expression de $\lambda_i(p_i^{\alpha_i})$ montre que si $\alpha_i > 1$, alors p_i divise $n-1$ (y compris pour $p = 2$, en distinguant les cas $\alpha = 2$ et $a \geqslant 3$). Or, comme p_i divise n, ceci n'est pas possible. Par conséquent, $\alpha_i \leqslant 1$. Par conséquent, n n'a pas de facteur multiple.
     On a donc pour tout $i \in [\![1, k]\!]$, $\lambda(p_i^{\alpha_i}) = p_i - 1$ (y compris si $p_i = 2$), et $\lambda(p_i^{\alpha_i})$ divise $n-1$, donc $p_i - 1$ divise $n-1$.
   - Réciproquement, si n est composé, sans facteur multiple et si pour tout p facteur premier de n, $p-1$ divise n, alors, en écrivant $n = p_1 \cdot p_k$ avec les p_i premiers deux à deux distincts, on a
   $$\lambda(n) = (p_1 - 1) \vee \cdot \vee (p_k - 1).$$
   Or chacun des $p_i - 1$ divise $n-1$, donc leur pgcd aussi. On en déduit que $\lambda(n)$ divise $n-1$. On a déjà montré qu'on ne peut avoir l'égalité que si n est premier, ce qui est exclus ici. Ainsi, $\lambda(n)$ divise strictement $n-1$.

   Ainsi, $\boxed{n \text{ est de Carmichael ssi tout facteur premier } p \text{ de } n \text{ est simple et vérifie } p-1|n-1}$.

6. On a $561 = 3 \times 11 \times 17$, donc il est composé, sans facteur multiple. De plus on vérifie facilement que 2, 10 et 16 divisent 560, donc n est de Carmichael.

7. La réciproque résulte du fait que si a est premier avec n, il est inversible modulo n, donc on peut simplifier par a.

   Dans le sens direct, si n est de Carmichael, l'égalité est trivialement vérifiée par définition pour les a premiers avec n, et il faut l'obtenir pour les autres valeurs de a. C'est en fait une conséquence du théorème chinois. On écrit $n = p_1 \cdots p_k$ (les p_i étant deux à deux distincts car n est de Carmichael), et on considère $a \in \mathbb{Z}$, et $i \in [\![1, k]\!]$
   - Si $a \wedge p_i = 1$, alors $a^{p_i - 1} \equiv 1\ [p^i]$ d'après Fermat, donc, comme $p_i - 1$ divise $n - 1$, $a^{n-1} \equiv 1\ [p_i]$, puis $a^n \equiv a\ [p_i]$.
   - Si $a \wedge p_i \neq 1$, alors $p_i | a$, donc $a \equiv 0\ |p_1]$, donc $a^n \equiv a \equiv 0\ [p_i]$.

   Par conséquent, pour tout $i \in [\![1, k]\!]$, $a^n \equiv a\ [p_i]$. Les p_i étant des premiers 2 à 2 distincts, ils sont 2 à 2 premiers entre eux, et, sachant que $n = p_1 \cdots p_k$, le théorème chinois permet de conclure que $\boxed{a^n \equiv a\ [n].}$

Corrigé du problème 2 – Postulat de Bertrand, théorème de Sylvester

Partie I – Majoration du produit des premiers nombres premiers

1. Soit $n \in \mathbb{N}^*$. Par symétrie des coefficients binomiaux, $\binom{2n+1}{n} = \binom{2n+1}{n+1}$. Ainsi d'après la formule du binôme,
$$2^{2n+1} = \sum_{k=0}^{2n+1} \binom{2n+1}{k} \geqslant \binom{2n+1}{n} + \binom{2n+1}{n+1} = 2\binom{2n+1}{n}.$$
   Ainsi, $\boxed{\binom{2n+1}{n} \leqslant 2^{2n}}$.

   On pouvait aussi faire une récurrence.

2. • Soit $n \in \mathbb{N}^*$. On a :
$$\binom{2n+1}{n} = \frac{(2n+1)\cdots(n+2)}{n!}.$$
   Soit p un nombre premier tel que $n+1 < p \leqslant 2n+1$. Alors p et un des facteurs du produit $(2n+1)\cdots(n+2)$, donc p divise ce produit. Par ailleurs,
$$v_p(n!) = \sum_{k=1}^{n} v_p(k) = 0,$$
   car $p > n$. Ainsi, p ne divise pas $n!$. On en déduit que p divise $\binom{2n+1}{n}$.

   • Ainsi, pour tout p premier vérifiant $n+1 < p \leqslant 2n+1$, $v_p\left(\binom{2n+1}{n}\right) \geqslant 1$, donc $\boxed{\prod_{\substack{p \in \mathcal{P} \\ n+1<p\leqslant 2n+1}} p \quad \text{divise } \binom{2n+1}{n}}$.

3. Soit, pour tout $m \geqslant 2$, la propriété $\mathcal{Q}(m) : \prod_{\substack{p \in \mathcal{P} \\ p \leqslant m}} p \leqslant 4^{m-1}$
   - Pour $m = 2$, on obtient l'ingalité $2 \leqslant 4^1$, qui est vraie.
   - Soit $m > 2$, et supposons que $\mathcal{Q}(2), \ldots, \mathcal{Q}(m-1)$ sont vrais.
     * Si m n'est pas premier (en particulier si m est pair),
$$\prod_{\substack{p \in \mathcal{P} \\ p \leqslant m}} p = \prod_{\substack{p \in \mathcal{P} \\ p \leqslant m-1}} p \leqslant 4^{m-2} \leqslant 4^{m-1}$$
       d'après l'hypothèse de récurrence.
     * Si m est premier (donc impair), on écrit $m = 2n + 1$ (avec $n \geqslant 1$), et
$$\prod_{\substack{p \in \mathcal{P} \\ p \leqslant m}} p = \prod_{\substack{p \in \mathcal{P} \\ p \leqslant 2n+1}} p = \left(\prod_{\substack{p \in \mathcal{P} \\ p \leqslant n+1}} p\right)\left(\prod_{\substack{p \in \mathcal{P} \\ n+1<p\leqslant 2n+1}} p\right) \leqslant 4^n \binom{2n+1}{n},$$
       d'après l'hypothèse de récurrence (valide car $n \geqslant 1$, donc $2 \leqslant n + 1 < 2n + 1$), et la question précédente (la divisibilité entraînant l'inégalité). On utilise alors la question 1, qui amène :
$$\prod_{\substack{p \in \mathcal{P} \\ p \leqslant m}} p \leqslant 4^n 4^n = 4^{m-1}.$$

Ainsi, on a vérifié $\mathcal{P}(m)$.

- D'après le principe de récurrence forte, on en déduit que pour tout $m \geqslant 2$,

$$\boxed{\prod_{\substack{p\in\mathcal{P}\\ p\leqslant m}} p \leqslant 4^{m-1}}$$

Partie II – Majoration d'un coefficient binomial

Soit $n \in \mathbb{N}^*$.

1. Pour tout $x \geqslant 0$, $\lfloor 2x\rfloor - 2\lfloor x\rfloor \in \mathbb{Z}$. De plus,

$$-1 = 2x - 1 - 2x < \lfloor 2x\rfloor - 2\lfloor x\rfloor < 2x - 2(x-1) = 2.$$

Ainsi, $\boxed{\lfloor 2x\rfloor - 2\lfloor x\rfloor \in \{0,1\}}$.

2. Soit, pour tout $k \geqslant 1$, α_k le nombre de multiples de p^k dans $[\![1, N]\!]$, et β_k le nombre de multiples de p^k qui ne sont pas multiples de p^{k+1}. On a alors :

$$\alpha_k = \left\lfloor \frac{N}{p^k} \right\rfloor \qquad \text{et} \qquad \beta_k = \alpha_k - \alpha_{k+1}.$$

Ainsi,

$$v_p(N!) = \sum_{\ell=1}^{N} v_p(\ell) = \sum_{k\geqslant 1} k\beta_k = \sum_{k\geqslant 1} k(\alpha_k - \alpha_{k+1}).$$

Les termes a_k sont nuls pour k assez grand. Soit K tel que pour tout $k > K$, $a_k = 0$. On a alors :

$$v_p(N!) = \sum_{k=1}^{K} ka_k - \sum_{k=1}^{K+1} ka_{k+1} = \sum_{k=1}^{N} ka_k - \sum_{k=2}^{N} (k-1)a_k = \sum_{k=1}^{N} a_k.$$

On obtient bien la formule de Legendre :

$$\boxed{v_p(N!) = \sum_{k\geqslant 1} \left\lfloor \frac{N}{p^k} \right\rfloor}$$

3. (a) Soit $n \in \mathbb{N}^*$, et p un nombre premier. On a donc :

$$v_p\left(\binom{2n}{n}\right) = v_p((2n)!) - 2v_p(n!) = \sum_{k\geqslant 1} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor.$$

On déduit alors de la question 1 que

$$v_p\left(\binom{2n}{n}\right) \leqslant \sum_{\substack{k\geqslant 1\\ p^k\leqslant 2n}} 1 = \max\{k \in \mathbb{N}^* \mid p^k \leqslant 2n\}.$$

Il en résulte immédiatement que $\boxed{p^{v_p\left(\binom{2n}{n}\right)} \leqslant 2n}$

(b) Si $p > \sqrt{2n}$, $p^2 > 2n$, donc $v_p\left((2n)!\right) \leqslant 1$ (d'après a), donc $\boxed{v_p\left(\binom{2n}{n}\right) \leqslant 1}$.

(c) Si $\dfrac{2}{3}n < p \leqslant n$:

- $1 \leqslant \frac{n}{p} < \frac{3}{2} < 2$, et $2 \leqslant \frac{2n}{p} < 3$, donc $\left\lfloor \frac{n}{p} \right\rfloor = 1$ et $\left\lfloor \frac{2n}{p} \right\rfloor = 2$;
- À condition que $p \geqslant 3$, $p^2 > 2n$, donc pour tout $k > 1$, $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ et $\left\lfloor \frac{2n}{p^k} \right\rfloor = 0$
- Ainsi, pour tout entier premier $p \geqslant 3$ tel que $\dfrac{2}{3}n < p \leqslant n$, la formule de Legendre amène $\boxed{v_p\left(\binom{2n}{n}\right) = 0}$

(on a simplement dit que le facteur p intervient une fois dans un seul des facteurs de $n!$, alors qu'il y a deux facteurs p et $2p$ divisibles par p dans $(2n)!$)

- Si $p=2$, l'inégalité $\frac{2}{3}n < p \leqslant n$ amène $2 \leqslant n < 3$, donc $n=2$, cas qu'on exclut (on considère $n \geqslant 3$, le postulat de bertrand étant trivialement vrai pour $n=1$ et $n=2$).

4. Un facteur premier de $\binom{2n}{n}$ divise nécessairement un des facteurs multiplicatifs de $(2n)!$, donc est inférieur à $2n$. On déduit alors des questions précédentes que :

$$\binom{2n}{n} = \prod_{\substack{p\in\mathcal{P}\\ p\leqslant 2n}} p^{v_p\left(\binom{2n}{n}\right)} \leqslant \left(\prod_{\substack{p\in\mathcal{P}\\ p\leqslant\sqrt{2n}}} 2n\right)\cdot\left(\prod_{\substack{p\in\mathcal{P}\\ \sqrt{2n}<p\leqslant\frac{2}{3}n}} p^1\right)\cdot\left(\prod_{\substack{p\in\mathcal{P}\\ \frac{2}{3}n<p\leqslant n}} p^0\right)\cdot\left(\prod_{\substack{p\in\mathcal{P}\\ n+1\leqslant p\leqslant 2n}} p^1\right)$$

Ainsi, on obtient bien :

$$\boxed{\binom{2n}{n} \leqslant (2n)^{\sqrt{2n}}\left(\prod_{\substack{p\in\mathcal{P}\\ \sqrt{2n}<p\leqslant\frac{2}{3}n}} p\right)\cdot\left(\prod_{\substack{p\in\mathcal{P}\\ n<p\leqslant 2n}} p\right).}$$

Partie III – Démonstration du postulat de Bertrand

1. (a) Soit $k<n$. On a alors

$$\binom{2n}{k+1} = \frac{2n-k}{k+1}\binom{2n}{k}.$$

Or, $2n-k > n \geqslant k+1$, donc $\frac{2n-k}{k+1} > 1$, et comme $\binom{2n}{k} > 0$, on obtient $\boxed{\binom{2n}{k+1} > \binom{2n}{k}}$.

(b) On a alors, par symétrie des coefficients binomiaux, pour tout $k \in [\![0, 2n]\!]$, $\binom{2n}{k} \leqslant \binom{2n}{n}$.

La chaîne précédente d'inégalités étant stricte, on a aussi (puisque $n \geqslant 2 \geqslant 1$), $\binom{2n}{n} > \binom{2n}{0}$, donc $\binom{2n}{n} \geqslant 2 = \binom{2n}{0} + \binom{2n}{n}$. Ainsi, d'après la formule du binôme,

$$2^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k} = \binom{2n}{0} + \binom{2n}{n} + \sum_{k=1}^{2n-1}\binom{2n}{k} \leqslant \binom{2n}{n} + \sum_{k=1}^{2n-1}\binom{2n}{n} = 2n\binom{2n}{n}.$$

Il en résulte que $\boxed{\frac{4^n}{2n} \leqslant \binom{2n}{n}}$.

2. On a donc, d'après les résultats de la partie II, et l'hypothèse sur la non existence d'un nombre premier entre $n+1$ et $2n$:

$$\frac{4^n}{2n} \leqslant \binom{2n}{n} \leqslant (2n)^{\sqrt{2n}}\left(\prod_{\substack{p\in\mathcal{P}\\ \sqrt{2n}<p\leqslant\frac{2}{3}n}} p\right),$$

et d'après la majoration de la partie I :

$$\frac{4^n}{2n} \leqslant (2n)^{\sqrt{2n}}\left(\prod_{\substack{p\in\mathcal{P}\\ p\leqslant\frac{2}{3}n}} p\right) \leqslant (2n)^{\sqrt{2n}}4^{\frac{3}{2}n-1},$$

d'où finalement, $\boxed{\frac{4^n}{2n} \leqslant (2n)^{\sqrt{2n}}4^{\frac{2}{3}n}.}$

3. (a) Soit f la fonction $x \mapsto 2^x - x - 1$. Elle est dérivable, de dérivée $x \mapsto f(x) \leqslant (\ln(2))2^x - 1$. Comme $\ln(2) \geqslant \frac{1}{2}$ (puisque $4 \geqslant \mathrm{e}$), f' est strictement positive sur $[1, +\infty[$. Ainsi, f est strictement croissante sur cet intervalle, et $f(1) = 0$. On en déduit que f est strictement positive sur $]2, +\infty[$. Ainsi, pour tout $a > 1$, $\boxed{a+1 < 2^a}$.

(b) Puisque $\sqrt[6]{2n} > 1$, on a alors :

$$2n = (\sqrt[6]{2n})^6 \leqslant (\sqrt[6]{2n}+1)^6 \leqslant (2^{\sqrt[6]{2n}})^6,$$

d'où le résultat attendu : $\boxed{2n \leqslant 2^{6\sqrt[6]{2n}}}$.

4. On a donc, en reprenant le résultat de la question 2 :

$$2^{2n} \leqslant (2n)^{\sqrt{2n}+1} 4^{\frac{2}{3}n} \leqslant 2^{6\sqrt[6]{n}(\sqrt{2n}+1)} 2^{\frac{4}{3}n} \qquad \text{donc:} \qquad 2^{\frac{2}{3}n} \leqslant 2^{6\sqrt[6]{n}(\sqrt{2n}+1)}.$$

Ainsi, en élevant au cube ($x \mapsto x^3$ étant croissante) :

$$2^{2n} \leqslant 2^{18\sqrt[6]{n}(\sqrt{2n}+1)} = 2^{18(2n)^{\frac{1}{2}+\frac{1}{3}}+18n^{\frac{1}{6}}} = 2^{18(2n)^{\frac{2}{3}}+18n^{\frac{1}{6}}}.$$

Or, pour tout $n \geqslant 50$,

$$\frac{18n^{\frac{1}{6}}}{2(2n)^{\frac{2}{3}}} \leqslant \frac{18}{2 \cdot 2^{\frac{2}{3}}} \cdot \frac{1}{\sqrt{50}} \leqslant \frac{9}{7 \cdot 2^{\frac{2}{3}}}.$$

En élevant au cube, on obtient :

$$\frac{81 \cdot 9}{49 \cdot 7 \cdot 4} < 2 \times \frac{1}{2} = 1,$$

donc $18n^{\frac{1}{6}} < 2(2n)^{\frac{2}{3}}$. Il vient alors :

$$\boxed{2^{2n} < 2^{20(2n)^{\frac{2}{3}}}}.$$

Il en résulte que $2n < 20(2n)^{\frac{2}{3}}$, donc $(2n)^{\frac{1}{3}} < 20$, donc $2n < (20)^3 = 8000$, donc $\boxed{n < 4000}$.

5. Les entiers premiers donnés dans l'énoncé peuvent s'écrire $q_1 < q_2 < \cdots < q_{14}$, et vérifient pour tout $i \in [\![1, 13]\!]$, $q_{i+1} < 2q_i$. Ainsi, étant donné $2 \leqslant n < q_{14} = 4001$, en notant $i = \max\{j \mid q_j \leqslant n\}$, i existe (cet ensemble est non vide, car il contient $i = 1$, et majoré par 14), et $i < 14$ (car $q_{14} > n$). L'entier q_{i+1} existe donc, est premier, et vérifie $q_{i+1} > n$ (par maximalité de i). De plus, $q_{i+1} < 2q_i = 2n$. Donc $q_{i+1} \in [\![n+1, 2n]\!]$.
Ainsi, tout intervalle du type $[\![n+1, 2n]\!]$, pour $n \geqslant 2$, $n \leqslant 4000$, contient un des nombres premiers de la liste donnée dans l'énoncé. Il est trivialement vrai pour $n = 1$ aussi.
$\boxed{\text{Le postulat de Bertrand est donc vrai pour tout entier strictement positif } n \leqslant 4000}$.

6. Par ailleurs, d'après la question précédente, s'il est faux pour une valeur de n, cette valeur vérifie $n < 4000$, ce qui contredit ce qu'on vient d'établir.
Il en résulte que $\boxed{\text{le postulat de Bertrand est vrai pour tout } n \in \mathbb{N}^*}$.

Partie IV – Une conséquence du théorème de Sylvester

1. • Si le postulat de Bertrand est vrai, étant donné $k \in \mathbb{N}^*$, l'intervalle $[\![k+1, 2k]\!]$ contient un nombre premier n. Soit $n = 2k$. L'un des entiers $n, n-1, \ldots, n-k+1$ est donc un nombre premier, donc possède un diviseur premier supérieur ou égal à $n - k + 1 = k + 1$, donc strictement plus grand que k. Ainsi, le théorème de Sylvester est vrai dans le cas $n = 2k$.
   • Si on suppose le théorème de Sylvester dans le cas $n = 2k$, l'un des enters n, $n-1$, $n-k+1 = k+1$ possède un diviseur premier strictement plus grand que k. Ce diviseur premier est aussi plus petit que $n = 2k$. Ainsi, il est dans $[\![k+1, 2k]\!]$. Ainsi, il existe un nombre premier dans $[\![k+1, 2k]\!]$, ce qui est le postulat de Bertrand.
$\boxed{\text{Le postulat de Bertrand est donc équivalent au cas } n = 2k \text{ du théorème de Sylvester}}$.

2. Par symétrie des coefficients binomiaux, l'équation $\binom{n}{k} = m^\ell$ équivaut à l'équation $\binom{n}{n-k} = m^\ell$. Pour $k \in [\![0, n]\!]$ (seul cas intéressant), $\frac{n}{2}$ est supérieur ou égal à l'un des deux entiers k et $k' = n - k$, donc on peut se ramener à une équation $\boxed{\binom{n}{k} = m^\ell, \text{ avec } n \geqslant 2k}$.
On suppose désormais que $n \geqslant 2k$

3. Puisque $n \geqslant 2k$, d'après le théorème de Sylvester, $n(n-1)\ldots(n-k+1)$ possède un diviseur premier (strictement) supérieur à k. Ce diviseur premier ne peut pas être diviseur de $k!$, donc il est encore diviseur de

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

Ainsi, $\boxed{\binom{n}{k} \text{ possède un diviseur premier } p > k}$.

4. Soit n, k dans $\mathbb{N}^*$ tels que $n \geqslant 2k$. Supposons qu'il existe un entier m, et un entier $\ell \geqslant 2$ tels que $\binom{n}{k} = m^\ell$
   (a) • D'après la question précédente, $\binom{n}{k}$ possède un diviseur premier $p > k$.

- Ainsi, p est un diviseur de m^ℓ, et donc, étant premier, c'est un diviseur de m. Il est donc diviseur de m^ℓ de multiplicité au moins ℓ. Ainsi, p^ℓ divise $\binom{n}{k}$.
- Or, p est un diviseur de $n(n-1)\dots n-k+1$. Ainsi, p étant premier il existe, d'après le lemme de Gauss, un entier $i \in [\![0, k-1]\!]$ tel que p divise $n-i$. Par ailleurs, pour tout $j \in [\![0, k-1]\!]$, tel que $i \neq j$, on a

$$1 \leqslant |(n-i)-(n-j)| \leqslant k-1 < p,$$

donc p ne divise aucun autre facteur $n-j$ ($j \neq i$) de $n(n-1)\dots(n-k+1)$.
- Comme p^ℓ divise $\binom{n}{k}$ donc $n(n-1)\dots(n-k+1)$, et que des facteurs de ce produit, seul $n-i$ est divisible par p, on en déduit que $\boxed{n-i \text{ est divisible par } p^\ell}$.

(b) L'entier $n-i$ étant non nul, on en déduit que

$$n \geqslant n-i \geqslant p^\ell \geqslant k^\ell \qquad \text{donc:} \qquad \boxed{n \geqslant k^\ell}.$$

5. (a) Soit $i \in [\![0, k-1]\!]$.
- L'idée est juste de regrouper tous les facteurs premiers de la décomposition de $n-i$ par groupes de ℓ facteurs identiques ; ce qui restera ira dans l'entier a_i. Plus formellement, on définit, pour tout $p \in \mathcal{P}$, $q_{p,i}$ et $r_{p,i}$ le quotient et le reste de la division euclidienne de $v_p(n-i)$ par ℓ, et on définit

$$m_i = \prod_{p\in\mathcal{P}} p^{q_i} \qquad \text{et} \qquad a_i = \prod_{p\in\mathcal{P}} p^{r_i}.$$

Comme les r_i vérifient tous $r_i < \ell$, aucun facteur premier n'apparaît avec une valuation au moins égale à ℓ dans a_i, donc a_i n'est divisible par aucune puissance de ℓ non triviale (si b^ℓ divise a_i, un facteur premier de b apparaît dans la décomposition de a_i avec une multiplicité au moins égale à ℓ) Par ailleurs

$$a_i m_i^\ell = \prod_{p\in\mathcal{P}} p^{q_i\ell+r_i} = p^{v_p(n-i)} = n-i.$$

D'où $\boxed{\text{l'existence des couples } (a_i, m_i)}$.
- Supposons que (a_i, m_i) et (a'_i, m'_i) vérifient tous deux les conditions. Alors $a_i m_i^\ell = a'_i {m'_i}^\ell$. Soit p un nombre premier. Alors

$$v_p(m_i^\ell) = \ell v_p(m_i) \equiv 0\ [\ell].$$

De même, $v_p({m'_i}^\ell) \equiv 0\ [\ell]$ (ces deux valuations sont éventuellement nul). Par conséquent,

$$v_p(a_i) \equiv v_p(a'_i)\ [\ell],$$

et comme $v_p(a_i) < \ell$ ainsi que $v_p(a'_i)$, on a $v_p(a_i) = v_p(a'_i)$. Ceci étant vrai pour tout nombre premier p, on en déduit, a_i et a'_i étant tous deux positifs, que $a_i = a'_i$, puis $m_i^\ell = {m'_i}^\ell$, et $x \mapsto x^\ell$ étant injective sur $\mathbb{R}_+$ ($\ell > 0$), il vient $m_i = m'_i$. D'où $\boxed{\text{l'unicité du couple } (a_i, m_i)}$.

(b) Supposons qu'il existe $i < j$ dans $[\![0, k-1]\!]$ tels que $a_i = a_j$. On a $n-i > n-j$, et comme $a_i = a_j$, cela nécessite $m_i > m_j$, donc $m_i \geqslant m_j + 1$ (m_i et m_j étant entiers) ; On a alors

$$(n-i)-(n-j) = a_j(m_i^\ell - m_j^\ell) \geqslant a_j((m_j+1)^\ell - m_j^\ell).$$

Ainsi, en développant $(m_j+1)^\ell$ à l'aide de la formule du binôme, en simplifiant m_j^ℓ et en ne conservant qu'un terme de ce qui reste (les autres étant positifs), on obtient :

$$(n-i)-(n-j) \geqslant a_j \ell m_j^{\ell-1} \geqslant \ell a_j m_j^{\frac{\ell}{2}} \geqslant \ell\sqrt{a_j m_j^\ell} = \ell\sqrt{n-j},$$

car $\ell \geqslant 2$ et $a_j \geqslant 1$. Ainsi, puisque i et j sont dans $[\![0, k-1]\!]$, que $k \leqslant \frac{n}{2}$, et que $\ell \geqslant \sqrt{2}$:

$$k > (n-i)-(n-j) \geqslant \ell\sqrt{\frac{n}{2}} \geqslant \sqrt{n}.$$

On a alors $k^\ell \geqslant k^2 > n$, ce qui contredit 3(b).
Ainsi, $\boxed{\text{les } a_i,\ i \in [\![0, k-1]\!] \text{ sont deux à deux distincts}}$.

6. (La clé de la preuve, selon Erdös)

(a) Par définition des a_i, et par l'hypothèse faite sur les m_i,

$$\left(\prod_{i=1}^{k-1} m_i\right)^{\ell} \left(\prod_{i=0}^{k-1} a_i\right) = \binom{n}{k} k! = m^{\ell} k!.$$

Soit $d = \left(\prod_{i=1}^{k-1} m_i\right) \wedge m$, et $u = \dfrac{\prod_{i=1}^{k-1} m_i}{d}$ et $v = \dfrac{m}{d}$.

Alors $\boxed{u \text{ et } v \text{ sont premiers entre eux et vérifient } u^{\ell} \prod_{i=0}^{k-1} a_i = v^{\ell} k!}$.

(b) Un diviseur premier p de v est de valuation multiple de ℓ. Comme p ne divise pas u (donc pas non plus u^{ℓ}) et que les a_i ne sont divisibles par aucune puissance non triviale d'ordre ℓ, il existe i et j distincts tels que a_i et a_j soient tous deux divisibles par p. Donc $n-i$ et $n-j$ sont divisibles par p, et distincts. Comme $|(n-i)-(n-j)| < k$, et est divisible par p il en résulte que $p < k$ et *a fortiori* $\boxed{p \leqslant k}$.

(c) On adapte la preuve de la formule de Legendre, en remarquant que par définition, chaque a_i divise $n-i$. Parmi les k termes consécutifs $n, (n-1), \ldots, (n-k+1)$, il y en a au plus $\left\lceil \dfrac{k}{p} \right\rceil$ donc au plus $\left\lfloor \dfrac{k}{p} \right\rfloor + 1$ qui sont divisibles au moins une fois par p. Donc il y a au plus $\left\lfloor \dfrac{k}{p} \right\rfloor + 1$ termes parmi les a_i divisibles au moins une fois par p. De même, il y en a au plus $\left\lfloor \dfrac{k}{p^2} \right\rfloor + 1$ qui sont divisibles deux fois par p, donc qui fournissent un facteur p supplémentaire par rapport à ceux obtenus dans la première étape, puis au plus $\left\lfloor \dfrac{k}{p^2} \right\rfloor + 1$ qui sont divisibles par p^3 etc. On s'arrête à $p^{\ell-1}$, car les a_i ne sont pas divisibles par p^{ℓ}, de par leur définition. Ainsi,

$$\boxed{v_p(a_0 a_1 \ldots a_{k-1}) \leqslant \sum_{i=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right)}$$

Pour ceux qui aiment la formalisation, on peut rédiger à l'aide de fonctions caractéristiques, efficaces ici :

$$v_p(a_0 a_1 \ldots a_{k-1}) = \sum_{i=0}^{k-1} v_p(a_i) = \sum_{i=0}^{k-1} \sum_{j=1}^{+\infty} \mathbb{1}(p^j \mid a_i).$$

Comme les a_i ont au plus $\ell - 1$ facteurs p :

$$v_p(a_0 a_1 \ldots a_{k-1}) = \sum_{i=0}^{k-1} \sum_{j=1}^{\ell-1} \mathbb{1}(p^j \mid a_i) = \sum_{j=1}^{\ell-1} \sum_{i=0}^{k-1} \mathbb{1}(p^j \mid a_i) \leqslant \sum_{j=1}^{\ell-1} \sum_{i=0}^{k-1} \mathbb{1}(p^j \mid n-i).$$

On en déduit alors que

$$v_p(a_0 a_1 \ldots a_{k-1}) = \sum_{j=1}^{\ell-1} \left| \{ i \in [\![0, k-1]\!] \text{ tq } p^j \mid n-i \} \right|.$$

On déduit alors des arguments donnés en début de question que

$$\boxed{v_p(a_0 a_1 \ldots a_{k-1}) \leqslant \sum_{j=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right)}$$

(d) Or, d'après la formule de Legendre $v_p(k!) = \sum_{j=1}^{+\infty} \left\lfloor \dfrac{k}{p^i} \right\rfloor$, et, puisque u et v sont premiers entre eux, p ne divise

pas u. Ainsi,

$$\begin{aligned} v_p(v^\ell) &= v_p(a_0 \dots a_{k-1}) - v_p(k!) \\ &\leqslant \sum_{j=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right) - \sum_{j=1}^{+\infty} \left\lfloor \frac{k}{p^i} \right\rfloor \\ &\leqslant \sum_{j=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right) - \sum_{j=1}^{\ell-1} \left\lfloor \frac{k}{p^i} \right\rfloor \\ &= \ell - 1. \end{aligned}$$

Ainsi, $\boxed{v_p(v^\ell) \leqslant \ell - 1}$

Les diviseurs premiers p de v ont donc tous une multiplicité strictement plus petite que ℓ dans v^ℓ. Or leur multiplicité dans v^ℓ est un multiple de ℓ, elle est donc nécessairement nulle. Par conséquent, p n'est pas diviseur de v^ℓ donc pas non plus de v, d'où une contradiction.

On en déduit que v ne peut pas avoir de diviseur premier, donc que $\boxed{v = 1}$.

(e) On a alors $u^\ell \prod_{i=0}^{n-1} a_i = k!$. Or, les a_i sont des entiers strictement positifs deux à deux distincts, donc $\prod_{i=0}^{n-1} a_i \geqslant k!$. L'égalité précédente impose donc $u = 1$ et $\prod_{i=0}^{n-1} a_i \geqslant k!$, ce qui n'est possible que si les a_i sont les éléments de $[\![1, k]\!]$ dans un certain ordre (ils doivent être le plus petit possible globalement, tout en étant deux à deux distincts). Cela signifie bien que $\sigma : i \mapsto a_i$ est définie de $[\![0, k-1]\!]$ dans $[\![1, k]\!]$, et étant injective d'un ensemble vers un ensemble de même cardinal fini, $\boxed{\sigma \text{ est une bijection}}$.

7. Soit $\ell = 2$. Alors, si $k \geqslant 4$, soit $i = \tau(4)$, donc $a_i = 4 = 2^2$. Cela contredit le fait que les a_i ne contiennent pas de carré. Donc $\boxed{\binom{n}{k} \text{ n'est pas un carré.}}$

8. On suppose $\ell \geqslant 3$, et $k \geqslant 4$. Soit $i_1 = \tau(1)$, $i_2 = \tau(2)$ et $i_4 = \tau(4)$.

(a) On suit l'indication donnée : soit $b = n - i_2$, $x = b - (n - i_1)$ et $y = n - i_4 - b$. Si on suppose que $(n - i_2)^2 = (n - i_1)(n - i_4)$, on a alors :

$$b^2 = (b - x)(b + y) = b^2 + b(y - x) - xy, \qquad \text{donc:} \qquad b(y - x) = xy.$$

De là on obtient (j'admets que ce n'était pas évident à trouver) :

$$|xy| = |b||y - x| \geqslant |b| = n - i_2 > n - k \geqslant k^\ell - k.$$

La première inégalité résulte du fait qu'on ne peut pas avoir $y = x$, sinon $xy = 0$, puis $x = y = 0$, puis $i_1 = i_2 = i_3$, ce qui contredit l'injectivité de τ. Comme $k > 1$, on a

$$|xy| \geqslant k^\ell - 2k + 1 \geqslant k^2 - 2k + 1 = (k - 1)^2.$$

Par ailleurs, i_1, i_2 et i_4 étant dans $[\![0, k-1]\!]$,

$$|x| = |i_1 - i_2| \leqslant k - 1 \qquad \text{et} \qquad |y| = |i_4 - i_2| \leqslant k - 1,$$

d'où $(k-1)^2 \geqslant |xy|$, et en mettant tout bout-à-bout, $|xy| > |xy|$, d'où une contradiction.

Conclusion : $\boxed{(n - i_2)^2 \neq (n - i_1)(n - i_4)}$

(b) Puisque par définition de τ, $a_{i_1} = 1$, $a_{i_2} = 2$ et $a_{i_4} = 4$, cette propriété se réexprime ainsi :

$$(2m_{i_2}^\ell)^2 \neq m_1^\ell 4 m_2^\ell \qquad \text{donc:} \qquad m_{i_2}^\ell \neq (m_{i_1} m_{i_4})^\ell \qquad \text{donc:} \qquad \boxed{m_{i_2} \neq m_{i_1} m_{i_4}}.$$

(c) On suppose $m_{i_2}^2 > m_{i_1} m_{i_4}$.

i. On a alors

$$(n - i_2)^2 - (n - i_1)(n - i_4) = 4(m_{i_2}^{2\ell} - (m_{i_1} m_{i_4})^\ell).$$

Or, si a et b sont deux réels tels que $a > b$, alors

$$a^\ell - b^\ell = (a - b)(a^{\ell-1} + a^{\ell-2} b + \dots + b^{\ell-1}) \geqslant (a - b) \times \ell b^{\ell-1}.$$

Ainsi, on obtient ici :

$$(n-i_2)^2-(n-i_1)(n-i_4)>4\ell(m_{i_2}^2-m_{i_1}m_{i_4})(m_{i_1}m_{i_4})^{\ell-1}.$$

Comme $m_{i_2}^2-m_{i_1}m_{i_4}$ est un entier strictement positif, il est au moins égal à 1, d'où :

$$\boxed{(n-i_2)^2-(n-i_1)(n-i_4)>4\ell(m_{i_1}m_{i_4})^{\ell-1}}.$$

Par ailleurs, soit $i=\max(i_1,i_4)$, on a alors :

$$(n-i_1)(n-i_4)>(n-i)^2$$

l'inégalité étant stricte car $i_1\neq i_4$. Par suite,

$$(n-i_2)^2-(n-i_1)(n-i_4)<(n-i_2)^2-(n-i)^2=(2n-i_2-i)(i-i_2).$$

Comme i et i_2 sont dans $[\![0,k-1]\!]$, $i-i_2<k-1$. La positivité de $2n-i_2-i$ amène alors

$$(n-i_2)^2-(n-i_1)(n-i_4)<(k-1)(2n-i_2-i)\qquad\text{puis:}\qquad\boxed{(n-i_2)^2-(n-i_1)(n-i_4)<2n(k-1)}$$

ii. On a alors :

$$2(k-1)m_{i_1}m_{i_4}>4\ell(m_{i_1}m_{i_4})^{\ell}=\ell(n-i_1)(n-i_4),$$

d'où finalement, $\boxed{2(k-1)m_{i_1}m_{i_4}>\ell(n-k+1)^2}$.

Par ailleurs, comme $n\geqslant k^\ell$, $\ell\geqslant 3$ et $k\geqslant 4$, $n\geqslant k\times 4^2$, et on obtient très largement $n>6k$, donc $k<\frac{n}{6}$. Ainsi

$$(n-k+1)^2>(n-k)^2=n^2-2kn+k^2>n^2-2kn>n^2-\frac{n^2}{3},$$

d'où enfin

$$\ell(n-k+1)^2>\frac{2}{3}\ell n^2\geqslant\frac{2}{3}\times 3n^2=2n^2.$$

Ainsi $\boxed{\ell(n-k+1)^2>2n^2}$.

iii. En simplifiant l'inégalité de la question précédente, il vient $(k-1)m_{i_1}m_{i_4}>n$. Or $k-1<k$ et par définition, $m_{i_1}^\ell\leqslant m-i_1\leqslant n$, donc $m_{i_1}\leqslant n^{\frac{1}{\ell}}$, et de même pour m_{i_4}. Il en résulte que

$$n<kn^{\frac{2}{\ell}}\qquad\text{puis:}\qquad\boxed{n<kn^{\frac{2}{3}}}.$$

(d) En élevant l'inégalité obtenue au cube, il vient alors $n<k^3$, ce qui contredit $n\geqslant k^\ell$ et $\ell\geqslant 3$. Ainsi, l'hypothèse initiale (le fait que $\binom{n}{k}$ est égal à m^ℓ) est fausse.

Donc, si $m_{i_2}^2>m_{i_1}m_{i_4}$, sous les hypothèses $\ell\geqslant 3$ et $k\geqslant 4$, $\boxed{\binom{n}{k}\text{ n'est pas une puissance d'ordre }\ell}$.

(e) Les inégalités se font à peu près de la même façon (mais dans l'autre sens) lorsque $m_{i_2}^2<m_{i_1}m_{i_4}$. Je vous laisse mettre l'argument en place. Cela termine la preuve.

9. (a) Soit, pour tout n dans $\mathbb{N}$, la propriété $\mathcal{P}(n)$: $\binom{u_n}{2}$ est un carré parfait.

- Pour $n=0$, on a $\binom{u_0}{2}=\binom{9}{2}=36=6^2$, donc $\mathcal{P}(0)$ est vrai.
- Soit $n\in\mathbb{N}$. Supposons que $\mathcal{P}(n)$ est vrai. Alors

$$\binom{u_{n+1}}{2}=\frac{u_{n+1}(u_{n+1}-1)}{2}=\frac{(2u_n-1)^2((2u_n-1)^2-1)}{2}=\frac{(2u_n-1)^2(2u_n(2u_n-2))}{2}=2^2(2u_n-1)^2\binom{u_n}{2},$$

et par l'hypothèse de récurrence, $\binom{u_{n+1}}{2}$ est un carré parfait.

Par conséquent, $\mathcal{P}(0)$ est vraie, et pour tout n dans $\mathbb{N}$, $\mathcal{P}(n)$ entraîne $\mathcal{P}(n+1)$. D'après le principe de récurrence, $\mathcal{P}(n)$ est vraie pour tout n dans $\mathbb{N}$.

Conclusion : $\boxed{\text{pour tout } n\in\mathbb{N},\ \binom{u_n}{2}\text{ est un carré parfait}}$.

(b) Tout u_n ($n\in\mathbb{N}$) est solution de l'équation $\binom{n}{2}=m^2$. La suite (u_n) étant clairement strictement croissante, cela donne une $\boxed{\text{infinité de solutions}}$ à cette équation.

(c) On a $\binom{50}{3} = \dfrac{50 \times 49 \times 48}{6} = 5^2 \times 2 \times 7^2 \times 2^3 = (5 \times 7 \times 2^2)^2 = 140^2$.

Ainsi, $\boxed{\binom{50}{3} \text{ est un carré parfait}}$.

On s'est servi de l'hypothèse $k \geqslant 4$ pour pouvoir définir $\tau(1)$, $\tau(2)$ et $\tau(4)$: pour que $\tau(4)$ soit bien défini, il et nécessaire d'avoir cette hypothèse $k \geqslant 4$.