Lycée Louis-Le-Grand, Paris
MPSI 4 – Mathématiques
A. Troesch

DM n° 16 (je sais compter !) : Arithmétique

Correction du problème 1 – 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 $\mathcal{Q}(2), \dots, \mathcal{Q}(m-1)$ 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 $\frac{2}{3}n < p \leqslant n$:

- $1 \leqslant \frac{n}{p} < \frac{3}{2} < 2$, 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 $\frac{2}{3}n < p \leqslant n$, 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 :

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

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 $n, n-1, \dots, n-k+1$ 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, $n(n-1)\dots(n-k+1)$ possède un diviseur premier (strictement) supérieur à k. Ce diviseur premier ne peut pas être diviseur de $k!$, donc il est encore diviseur de

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

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 $v_p(k!) = \displaystyle\sum_{j=1}^{+\infty} \left\lfloor \frac{k}{p^i} \right\rfloor$, 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 $u^\ell \displaystyle\prod_{i=0}^{n-1} a_i = k!$. Or, les a_i sont des entiers strictement positifs deux à deux distincts, donc $\displaystyle\prod_{i=0}^{n-1} a_i \geqslant k!$. L'égalité précédente impose donc $u = 1$ et $\displaystyle\prod_{i=0}^{n-1} a_i \geqslant k!$, 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
$$a^\ell-b^\ell=(a-b)(a^{\ell-1}+a^{\ell-2}b+\cdots+b^{\ell-1})\geqslant(a-b)\times\ell b^{\ell-1}.$$
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

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

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 $\displaystyle\binom{50}{3} = \frac{50 \times 49 \times 48}{6} = 5^2 \times 2 \times 7^2 \times 2^3 = (5 \times 7 \times 2^2)^2 = 140^2$.

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 $k \geqslant 4$.

Correction du problème 2 – Loi de réciprocité quadratique

Questions préliminaires

1. Puisque p et q sont impairs, $\frac{p-1}{2}$ et $\frac{q-1}{2}$ sont entiers. De plus,

$$\frac{p-1}{2} \equiv 0\ [2] \iff p-1 \equiv 0[4] \iff p \equiv 1[4]$$

Ainsi, $\frac{p-1}{2} \cdot \frac{q-1}{2}$ est impair si et seulement si chacun des deux termes du produit l'est, si et seulement si $p \equiv q \equiv 3[4]$. 0n déduit alors de la loi de réciprocité quadratique que si p et q sont deux entiers premiers impairs distincts,

$$\boxed{\left(\frac{q}{p}\right)_L = \begin{cases} -\left(\frac{p}{q}\right)_L & \text{si } p \equiv q \equiv 3\ [4] \\ \left(\frac{p}{q}\right)_L & \text{sinon.} \end{cases}}$$

2. Soit $a \equiv b\ [p]$, et supposons que a est un résidu quadratique modulo p. Il existe donc $c \in \mathbb{Z}$ tel que $c^2 \equiv a \equiv b\ [p]$, et donc b est un résidu quadratique modulo p également ; et réciproquement. Ainsi, $\boxed{\left(\frac{a}{p}\right)_L = \left(\frac{b}{p}\right)_L}$.

3. On a facilement $1^2 \equiv 1\ [5]$, donc $\boxed{\left(\frac{1}{5}\right)_L = 1}$. C'est d'ailleurs clairement vrai si on remplace 5 par n'importe quel autre nombre premier impair.
Par ailleurs, tout b^2 est congru modulo 5 à r^2, où r est son reste modulo 5. Ainsi, si 2 est résidu quadratique modulo 5, il existe $r \in [\![0,4]\!]$ tel que $r^2 \equiv 2\ [5]$. On vérifie facilement, par calcul de ces 5 carrés, que ce n'est pas le cas. Donc $\boxed{\left(\frac{2}{5}\right)_L = -1}$.

4. On se sert du théorème des résidus quadratiques et des questions 1 et 2 pour trouver les signes et opérer les simplifications :

$$\left(\frac{5}{17}\right)_L = \left(\frac{17}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1,$$

donc $\boxed{\text{5 n'est pas un résidu quadratique modulo 17}}$. De même :

$$\left(\frac{5}{41}\right)_L = \left(\frac{41}{5}\right)_L = \left(\frac{1}{5}\right)_L = 1,$$

$\boxed{\text{5 est un résidu quadratique modulo 41}}$.

Partie I – Quelques propriétés élémentaires du symbole de Legendre

Dans toute cette partie, p désigne un nombre premier impair.

1. Caractérisation des résidus quadratiques

   (a) Soit n un entier premier avec p (c'est-à-dire non divisible par p, celui-ci étant premier). Remarquons d'abord que $y = n^{\frac{p-1}{2}}$ est bien défini, puisque l'exposant est entier. On a alors $y^2 = n^{p-1} \equiv 1$ $[p]$, d'après le théorème de Fermat. Comme le polynôme $X^2 - 1$ de $\mathbb{F}_p[X]$ ne peut pas avoir plus de deux racines, on en déduit que $\boxed{y \equiv 1 \ [p] \text{ ou } y \equiv -1 \ [p]}$.

   (b) Si n est un résidu quadratique premier avec p, on peut écrire $n \equiv a^2$ $[p]$, et donc $n^{\frac{p-1}{2}} \equiv a^{p-1}$ $[p]$. De plus, p ne divise pas a, sinon il diviserait aussi n. Ainsi, on peut utiliser le théorème de Fermat, et on obtient $\boxed{n^{\frac{p-1}{2}} \equiv 1 \ [p].}$

   (c) On remarque d'abord que pour tout $a \in \mathbb{F}_p^*$, l'équation $x^2 = a$ admet soit 0 soit 2 solutions (il ne peut pas y en avoir plus car $X^2 - a$ est un polynôme de degré 2, et s'il y a une solution b, $-b$ est aussi une solution, et distinct de b puisque p est impair). Ainsi, en notant $f : x \mapsto x^2$ de $\mathbb{F}_p^*$ dans lui-même, pour tout a, $|f^{-1}(a)| = 0$ si a n'est pas un résidu quadratique et $|f^{-1}(a)| = 2$ si a est un résidu quadratique. En considérant la partition de $\mathbb{F}_p^*$ associée à cette application, on en déduit que $p - 1$ est partagé en autant de parts de cardinal 2 qu'il y a de résidus quadratiques. Il y a donc $\frac{p-1}{2}$ résidus quadratiques.
   Ainsi, ces résidus quadratiques fournissent $\frac{p-1}{2}$ racines distinctes du polynôme $X^{\frac{p-1}{2}} - 1$ de $\mathbb{F}_p[X]$. Pour des raisons de degré, il ne peut pas y avoir plus de racines. Ainsi un non-résidu quadratique a n'est pas racine de ce polynôme, donc
   $$a^{\frac{p-1}{2}} \not\equiv 1 \quad [p]$$
   On déduit de la question 1(a) que $a^{\frac{p-1}{2}} \equiv -1$ $[p]$.
   Ainsi, par définition du symbole de Legendre, on obtient bien :
   $$\boxed{\left(\frac{n}{p}\right)_L \equiv n^{\frac{p-1}{2}} \ [p] \text{ (formule d'Euler)}}$$

   (d) La multiplicativité du symbole de Legendre en découle de façon immédiate :
   $$\left(\frac{mn}{p}\right)_L \equiv (mn)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}} n^{\frac{n-1}{2}} \equiv \left(\frac{m}{p}\right)_L \left(\frac{n}{p}\right)_L \quad [p]$$
   Les symboles de Legendre prenant leurs valeurs dans $\{-1, 1\}$, et p n'étant pas égal à 2, cette congruence implique l'égalité :
   $$\boxed{\left(\frac{mn}{p}\right)_L = \left(\frac{m}{p}\right)_L \left(\frac{n}{p}\right)_L}.$$

   (e) On peut alors calculer par exemple $\left(\frac{33}{127}\right)_L$:
   $$\left(\frac{33}{127}\right)_L = \left(\frac{11}{127}\right)_L \left(\frac{3}{127}\right)_L = (-1)^2 \left(\frac{127}{11}\right)_L \left(\frac{127}{3}\right)_L = \left(\frac{6}{11}\right)_L \left(\frac{1}{3}\right)_L = \left(\frac{2}{11}\right)_L \left(\frac{3}{11}\right)_L$$
   Or,
   $$\left(\frac{2}{11}\right)_L \equiv 2^5 \equiv 32 \equiv -1 \ [11],$$
   et
   $$\left(\frac{3}{11}\right)_L = -\left(\frac{11}{3}\right)_L = -\left(\frac{2}{3}\right)_L \equiv -2 \equiv 1 \ [3].$$
   Ainsi, comme le symbole de Legendre prend ses valeurs dans $\{-1, 1\}$, on a forcément $\left(\frac{2}{11}\right)_L = -1$ et $\left(\frac{3}{11}\right)_L = 1$. Ce dernier point pouvait aussi se voir directement puisque $3 \equiv 5^2$ $[11]$.

   On obtient donc $\boxed{\left(\frac{33}{127}\right)_L = -1}$.

2. Lemme de Gauss

   Soit m un entier non divisible par p.

   (a) • Pour commencer, m étant premier avce p, m est inversible modulo p (immédiat avec une relation de Bézout). Ainsi, l'application $x \mapsto mx$ est bijective de $\mathbb{F}_p$ dans lui-même, de réciproque $x \mapsto m^{-1}x$.

- On en déduit que les $r_m(n)$ sont deux à deux distincts, pour $n \in [\![1, \frac{p-1}{2}]\!]$. En particulier, $|r_m(n)| \neq |r_m(n')|$ si $n \neq n'$ et $e_m(n) = e_m(n')$.
- Il reste donc à voir ce qui se passe pour n et n' distincts dans $[\![1, \frac{p-1}{2}]\!]$ lorsque $r_m(n)$ et $r_m(n')$ sont de signe opposé. Supposons qu'on ait $|r_m(n)| = |r_m(n')|$, c'est-à-dire $r_m(n) = -r_m(n')$. On a alors $mn \equiv -mn'$ $[p]$, donc
$$m(n+n') \equiv 0 \ [p]$$
Ceci n'est pas possible, puisque $\mathbb{F}_p$ est intègre (m et $n+n'$ étant non nuls modulo p, puisque $n+n' \in [\![2, p-1]\!]$)
- Ainsi, $\boxed{\text{les } |r_n(m)| \text{ sont deux à deux distincts pour } n \in [\![1, \frac{p-1}{2}]\!].}$ De plus, ils sont dans $[\![0, \frac{p-1}{2}]\!]$ par définition, et même dans $[\![1, \frac{p-1}{2}]\!]$, puisque par intégrité, mn n'est pas nul modulo p. On en déduit que l'application $n \mapsto |r_m(n)|$ est injective de $[\![1, \frac{p-1}{2}]\!]$ dans lui-même, et par cardinalité, on en déduit qu'elle est $\boxed{\text{bijective}}$.

(b) Lorsque n parcourt $[\![1, \frac{p-1}{2}]\!]$, les $|r_m(n)| = e_m(n)r_m(n)$ parcourent donc une et une seule fois chaque élément de $[\![1, \frac{p-1}{2}]\!]$. Ainsi,
$$\prod_{n=1}^{\frac{p-1}{2}} e_n(m)r_n(m) = \prod_{n=1}^{\frac{p-1}{2}} n$$
Or,
$$\prod_{n=1}^{\frac{p-1}{2}} r_n(m) \equiv \prod_{n=1}^{\frac{p-1}{2}} mn \equiv m^{\frac{p-1}{2}} \prod_{n=1}^{\frac{p-1}{2}} n \equiv \left(\frac{m}{p}\right)_L \prod_{n=1}^{\frac{p-1}{2}} n \ [p],$$
d'après la question I-1(c). Ainsi,
$$\left(\frac{m}{p}\right)_L \prod_{n=1}^{\frac{p-1}{2}} n \prod_{n=1}^{\frac{p-1}{2}} e_n(m) \equiv \prod_{n=1}^{\frac{p-1}{2}} n \ [p].$$
Par ailleurs, chaque $n \in [\![1, \frac{p-1}{2}]\!]$ étant inversible modulo p, leur produit aussi, et on peut donc simplifier :
$$\left(\frac{m}{p}\right)_L \prod_{n=1}^{\frac{p-1}{2}} e_n(m) \equiv 1[p],$$
et, puisque $\left(\frac{m}{p}\right)_L \in \{-1, 1\}$,
$$\prod_{n=1}^{\frac{p-1}{2}} e_n(m) \equiv \left(\frac{m}{p}\right)_L \ [p],$$
Les deux membres étant égaux soit à 1 soit à -1 et p étant différent de 2, cette congruence est en fait une égalité :
$$\boxed{\prod_{n=1}^{\frac{p-1}{2}} e_n(m) = \left(\frac{m}{p}\right)_L}.$$

3. Caractère quadratique de 2

(a) Pour $n \in [\![1, \frac{p-1}{2}]\!]$, on a $2n \in [\![2, \frac{p-1}{2}]\!]$. Ainsi, $e_n(2) = 1$ si et seulement si $2m \leqslant \frac{p-1}{2}$ si et seulement si $m \leqslant \frac{p-1}{4}$. Ainsi,
$$\left|\left\{n \in [\![1, \frac{p-1}{2}]\!] \mid e_n(2) = 1\right\}\right| = \left\lfloor \frac{p-1}{4} \right\rfloor.$$
Ainsi par complémentarité,
$$\left|\left\{n \in [\![1, \frac{p-1}{2}]\!] \mid e_n(2) = -1\right\}\right| = \frac{p-1}{2} \left\lfloor \frac{p-1}{4} \right\rfloor = \frac{p-1}{2} + \left\lceil -\frac{p-1}{4} \right\rceil,$$
et comme $\frac{p-1}{2}$ est entier,
$$\left|\{n \in [\![1, \frac{p-1}{2}]\!] \mid e_n(2) = -1\}\right| = \left\lceil \frac{p-1}{2} - \frac{p-1}{4} \right\rceil = \left\lceil \frac{p-1}{4} \right\rceil.$$

Ainsi, en comptant les signes dans le produit, on obtient :

$$\boxed{\left(\frac{2}{p}\right)_L = \prod_{n=1}^{\frac{p-1}{2}} e_n(2) = (-1)^{\left\lceil \frac{p-1}{4} \right\rceil}}$$

(b) On écrit $p = 8k + \ell$, avec $\ell \in \{1, 3, 5, 7\}$. On a alors

$$\frac{p-1}{4} = 2k + \frac{\ell - 1}{4},$$

où $\frac{\ell-1}{4}$ prend respectivement les valeurs $0, \frac{1}{2}, 1, \frac{3}{2}$ lorsque ℓ prend les valeurs 1, 3, 5, 7. Ainsi, $\left\lceil \frac{p-1}{4} \right\rceil$ est pair ssi $\ell = 1$ ou $\ell = 7$. Ainsi, on a bien :

$$\boxed{\left(\frac{2}{p}\right)_L = \begin{cases} 1 & \text{si } p \equiv \pm 1\ [8] \\ -1 & \text{si } p \equiv \pm 3 \end{cases}}$$

Par ailleurs, avec les mêmes notations, $p^2 = (8k + \ell)^2 = 64k^2 + 16\ell + \ell^2 \equiv \ell^2$ [16]. Ainsi, si $p \equiv \pm 1$ [8], $p^2 - 1 \equiv 1 - 1 = 0$ [16], donc $\frac{p^2-1}{8}$ est pair. De même, si $p \equiv \pm 3$ [8], alors $p^2 - 1 \equiv 3^2 - 1 \equiv 8[16]$, donc $\frac{p^2-1}{8}$ est impair. On déduit de ce qui précède que :

$$\boxed{\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}}.$$

Partie II – Démonstration calculatoire de la loi de réciprocité quadratique

1. On distingue 2 cas :
   - Si $e_q(k) = 1$, alors $r_q(k) = s_q(k)$, et on a bien l'égalité $e_{q,k} r_q(k) = p \cdot \delta_{-1, e_q(k)} + e_q(k) s_q(k)$.
   - Si $e_q(k) = -1$, on a $r_q(k) + p = s_q(k)$, donc $e_q(k) r_q(k) = -r_q(k) = p - s_q(k) = p + e_q(k) s_q(k) = p \cdot \delta_{-1, e_q(k)} + e_q(k) s_q(k)$.

   Ainsi, dans tous les cas, la formule est valide : $\boxed{e_{q(k)} r_q(k) = p \cdot \delta_{-1, e_q(k)} + e_q(k) s_q(k)}$.

2. Les $e_{q(k)} r_q(k) = |r_q(k)|$ parcourant une et une seule fois les éléments de $[\![1, \frac{p-1}{2}]\!]$, on en déduit que

$$\sum_{k=1}^{\frac{p-1}{2}} e_{q(k)} r_q(k) = \sum_{k=1}^{\frac{p-1}{2}} k = \frac{1}{2} \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} = \frac{p^2 - 1}{8}.$$

   Ainsi, en utilisant la question précédente, on obtient bien :

$$\boxed{\sum_{k=1}^{\frac{p-1}{2}} p \cdot \delta_{-1, e_q(k)} + e_q(k) s_q(k) = \frac{p^2 - 1}{8}}$$

3. On a :

$$\sum_{k=1}^{\frac{p-1}{2}} \mathrm{e}_q(k) \left(kq - p \left\lfloor \frac{kq}{p} \right\rfloor \right) = \sum_{k=1}^{\frac{p-1}{2}} \mathrm{e}_q(k) kq - p \sum_{k=1}^{p-1} \left\lfloor \frac{kq}{p} \right\rfloor.$$

   Ainsi, puisque $\mathrm{e}_q(k) \equiv 1$ [2], on obtient :

$$\sum_{k=1}^{\frac{p-1}{2}} \mathrm{e}_q(k) \left(kq - p \left\lfloor \frac{kq}{p} \right\rfloor \right) \equiv q \sum_{k=1}^{\frac{p-1}{2}} k - pS(q,p) \equiv \boxed{q \frac{p^2 - 1}{8} - pS(q,p)}.$$

4. Or, $\left\lfloor \frac{kq}{p} \right\rfloor$ est le quotient de la division euclidienne de kq par p, donc $kq - p\left\lfloor \frac{kq}{p} \right\rfloor$ est le reste de cette division à savoir $s_q(k)$. On en déduit que

$$\sum_{k=1}^{\frac{p-1}{2}} p\delta_{-1,e_q(k)} + e_q(k)s_q(k) \equiv p\sum_{k=1}^{\frac{p-1}{2}} \delta_{-1,e_q(k)} + q\frac{p^2-1}{8} - pS(q,p) \ [2].$$

Par ailleurs, la somme restante compte les éléments k pour lesquels $-1 = e_q(k)$: il y en a μ. En reprenant le résultat de la question 2, il vient donc :

$$\frac{p^2-1}{8} \equiv \mu p + q\frac{p^2-1}{8} - pS(q,p) \ [2],$$

donc, puisque p est impair, donc congru à 1 modulo 2, ainsi que q,

$$\boxed{\mu \equiv S(q,p) \ [2]}.$$

On a donc

$$\boxed{\left(\frac{q}{p}\right)_L = \prod_{k=1}^{\frac{p-1}{2}} e_q(k) = (-1)^{\mu} = (-1)^{S(q,p)}}.$$

5. Soit $\ell \in [\![1, \frac{q-1}{2}]\!]$. Alors

$$\begin{aligned} \left\lfloor \frac{kq}{p} \right\rfloor = \ell &\iff l \leqslant \frac{kq}{p} < \ell + 1 \\ &\iff \frac{p\ell}{q} \leqslant k < \frac{p(\ell+1)}{q}. \end{aligned}$$

Le nombre de valeurs entières de k réalisant cette inégalité est

$$C_\ell = \left\lceil \frac{(\ell+1)p}{q} \right\rceil - \left\lceil \frac{\ell p}{q} \right\rceil.$$

Puisque $\ell \leqslant \frac{q-1}{2}$,

$$\frac{p(\ell+1)}{q} \leqslant \frac{p(q+1)}{2q} = \frac{pq+p}{2q} < \frac{pq+q}{2} = \frac{p+1}{2}.$$

L'inégalité étant stricte entre des entiers, il vient $\frac{p(\ell+1)}{q} \leqslant \frac{p-1}{2}$, donc toutes les valeurs de k trouvées de la sorte interviennent dans la somme définissant $S(q,p)$.
Par ailleurs, les valeurs de $\left\lfloor \frac{kq}{p} \right\rfloor$ sont bien toutes dans l'intervalle $[\![1, \frac{q-1}{2}]\!]$, puisque

$$\frac{kq}{p} \leqslant \frac{(p-1)q}{2p} \leqslant \frac{q}{2},$$

et en passant à la partie entière,

$$\left\lfloor \frac{kq}{p} \right\rfloor \leqslant \frac{q-1}{2}.$$

Ainsi, en regroupant les termes de la somme $S(q,p)$ suivant leur valeur, on obtient :

$$\boxed{S(q,k) = \sum_{\ell=1}^{\frac{q-1}{2}} \ell C_\ell = \sum_{\ell=1}^{\frac{q-1}{2}} \ell\left(\left\lceil \frac{(\ell+1)p}{q} \right\rceil - \left\lceil \frac{\ell p}{q} \right\rceil\right) = \sum_{\ell=1}^{\frac{q-1}{2}} \ell\left(\left\lfloor \frac{(\ell+1)p}{q} \right\rfloor - \left\lfloor \frac{\ell p}{q} \right\rfloor\right)}.$$

La dernière égalité découle du fait que puisque q est un nombre premier ne divisant ni k, ni $k+1$, ni p, les quantités $\frac{kp}{q}$ et $\frac{(k+1)}{p}$ sont non entières, et donc leur partie entière par excès diffère de leur partie entière par défaut de 1 ; ces 1 se compensent.

6. On en déduit enfin que

$$S(q,p)+S(p,q) = \sum_{\ell=1}^{\frac{q-1}{2}} k\left(\left\lfloor \frac{(k+1)p}{q} \right\rfloor - \left\lfloor \frac{kp}{q} \right\rfloor\right)+\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor = \sum_{\ell=1}^{\frac{q-1}{2}} k\left\lfloor \frac{(k+1)p}{q} \right\rfloor - (k-1)\left\lfloor \frac{kp}{q} \right\rfloor = \frac{q-1}{2}\left\lfloor \frac{(q+1)p}{2q} \right\rfloor$$

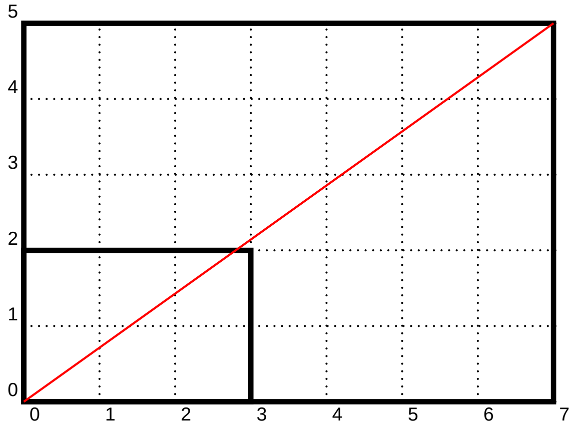

FIGURE 1 – Interprétation géométrique

On a déjà justifié l'inégalité $\dfrac{(q+1)p}{2q} < \dfrac{p+1}{2}$. De plus $\dfrac{(q+1)p}{2q} \geqslant \dfrac{q}{2} \geqslant \dfrac{q-1}{2}$, donc

$$\left\lfloor \frac{(q+1)p}{2q} \right\rfloor = \frac{p-1}{2}.$$

On peut donc en conclure que :

$$\boxed{S(q,p) + S(p,q) = \frac{q-1}{2} \cdot \frac{p-1}{2}.}$$

L'interprétation géométrique consiste à compter les points à coordonnées strictement positives dans le petit rectangle de la figure 1 en les comptant horizontalement s'ils sont au dessus de la diagonale du grand rectangle, et verticalement s'ils sont en-dessous.

7. On a donc

$$\left(\frac{p}{q}\right)_L \times \left(\frac{q}{p}\right)_L = (-1)^{S(p,q)+S(q,p)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Les symboles de Legendre étant leur propre inverse, il vient :

$$\boxed{\left(\frac{q}{p}\right)_L = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)_L}.$$

Démontrer enfin la loi de réciprocité quadratique donnée dans le préambule du problème.

Partie III – Démonstration trigonométrique de la loi de réciprocité quadratique (Eisenstein)

1. On délinéarise $\sin(mx)$:

$$\sin(mx) = \mathrm{Im}(\mathrm{e}^{\mathrm{i}\,mx}) = \mathrm{Im}((\cos(x) + \mathrm{i}\sin(x))^m = \mathrm{Im}\left(\sum_{k=0}^{m} \binom{2n+1}{k} \mathrm{i}^k \cos^{2n+1-k}(x) \sin^k(x)\right).$$

En conservant la partie imaginaire, donc les indices $k = 2\ell + 1$ impairs, il vient :

$$\sin(mx) = \sum_{\ell=1}^{n} (-1)^\ell \binom{2n+1}{2\ell+1} \cos^{2(n-\ell)}(x) \sin^{2\ell+1}(x) = \sum_{\ell=1}^{n} (-1)^\ell \binom{2n+1}{2\ell+1} (1-\sin^2(x))^{n-\ell} \sin^{2\ell+1}(x)$$

Ainsi, en posant $\boxed{P_n = \sum_{\ell=1}^{n} (-1)^\ell \binom{2n+1}{2\ell+1} X^\ell (1-X)^{n-\ell}}$, il vient

$$\boxed{P_n(\sin^2(x)) = \frac{\sin(mx)}{\sin(x)}}.$$

Le coefficient dominant de P_n est (si cette quantité est non nulle) :

$$\sum_{\ell=1}^{n}(-1)^{\ell}(-1)^{n-\ell}\binom{2n+1}{2\ell+1} = (-1)^n\sum_{\ell=1}^{n}\binom{2n+1}{2\ell+1} = \frac{(-1)^n}{2}\sum_{k=0}^{2n+1}\binom{2n+1}{k},$$

puisqu'un ensemble non vide a autant de sous-ensembles de cardinal pair que de cardinal impair, ce qu'on obtient en considérant la bijection $X \mapsto X\triangle\{x\}$, x étant un élément fixé de l'ensemble total E. Ainsi, d'après la formule du binôme,

$$\sum_{\ell=1}^{n}(-1)^{\ell}(-1)^{n-\ell}\binom{2n+1}{2\ell+1} = (-1)^n 2^{2n} = (-4)^n.$$

Ainsi, $\boxed{\text{le coefficient dominant de } P_n \text{ est } (-4)^n = (-4)^{\frac{m-1}{2}}}$.

2. On recherche les racines de P_n. Pour cela, on remarque que si $\sin(mx) = 0$, avec $x \in]0, \frac{\pi}{2}[$, alors $\sin^2(x)$ est racine de P. Or,

$$\sin(mx) = 0 \Longleftrightarrow mx \equiv 0\ [\pi] \Longleftrightarrow x \equiv 0\ [\frac{\pi}{m}]$$

Ainsi, $\sin^2$ étant strictement croissante sur $[0, \frac{\pi}{2}]$, on obtient $n = \frac{m-1}{2}$ racines distinctes de P_n :

$$r_k = \sin^2\left(\frac{k\pi}{m}\right),\ k \in [\![1, n]\!].$$

Comme P_n est de degré n, on a toutes ses racines dans $\mathbb{C}$. Ainsi, on peut factoriser :

$$P_n = (-4)^{\frac{m-1}{2}}\prod_{k=1}^{n}\left(X - \sin^2\left(\frac{k\pi}{m}\right)\right).$$

En évaluant en $\sin^2(x)$, il vient :

$$\boxed{\frac{\sin(mx)}{\sin(x)} = (-4)^{\frac{m-1}{2}}\prod_{j=1}^{\frac{m-1}{2}}\left(\sin^2(x) - \sin^2\frac{2\pi j}{m}\right).}$$

3. On a $qk \equiv r_q(k)\ [p]$, donc $\frac{2\pi}{p}qk \equiv \frac{2\pi}{p}r_q(k)\ [2\pi]$. Ainsi,

$$\sin\left(\frac{2\pi}{p}qk\right) = \sin\left(\frac{2\pi}{p}r_q(k)\right) = \sin\left(\frac{2\pi}{p}e_q(k)|r_q(k)|\right),$$

et par imparité du sinus,

$$\boxed{\sin\left(\frac{2\pi}{p}qk\right) = e_q(k)\sin\left(\frac{2\pi}{p}|r_q(k)|\right)}.$$

4. On utilise le lemme de Gauss :

$$\left(\frac{q}{p}\right)_L = \prod_{k=1}^{\frac{p-1}{2}} e_p(q) = \frac{\displaystyle\prod_{k=1}^{\frac{p-1}{2}}\sin\left(\frac{2\pi}{p}qk\right)}{\displaystyle\prod_{k=1}^{\frac{p-1}{2}}\sin\left(\frac{2\pi}{p}|r_q(k)|\right)}.$$

Or, $k \mapsto |r_q(k)|$ est une bijection de $[\![1, \frac{p-1}{2}]\!]$ dans lui-même, donc

$$\begin{aligned}\left(\frac{q}{p}\right)_L &= \frac{\displaystyle\prod_{k=1}^{\frac{p-1}{2}}\sin\left(\frac{2\pi}{p}qk\right)}{\displaystyle\prod_{k=1}^{\frac{p-1}{2}}\sin\left(\frac{2\pi}{p}k\right)}.\\ &= \prod_{k=1}^{\frac{p-1}{2}}\left((-4)^{\frac{m-1}{2}}\prod_{j=1}^{\frac{m-1}{2}}\left(\sin^2(\frac{2\pi k}{p}) - \sin^2\frac{2\pi j}{q}\right)\right)\\ &= (-4)^{\frac{p-1}{2}\cdot\frac{(q-1)}{2}}\prod_{k=1}^{\frac{p-1}{2}}\prod_{j=1}^{\frac{m-1}{2}}\left(\sin^2(\frac{2\pi k}{p}) - \sin^2\frac{2\pi j}{q}\right)\end{aligned}$$

On peut bien sûr écrire de même

$$\left(\frac{p}{q}\right)_L = (-4)^{\frac{p-1}{2}\cdot\frac{(q-1)}{2}} \prod_{k=1}^{\frac{p-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin^2(\frac{2\pi k}{q}) - \sin^2 \frac{2\pi j}{p} \right),$$

et les deux expressions obtenues ne diffèrent que par le signe de chaque terme du produit. Or, il y a $\frac{p-1}{2} \cdot \frac{q-1}{2}$ termes dans le produit, donc

$$\boxed{\left(\frac{p}{q}\right)_L = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right)_L}.$$

Partie IV – Démonstration combinatoire de la loi de réciprocité quadratique

1. La multiplication par m est une injection de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même, puisque m est inversible (donc régulier) dans $\mathbb{Z}/p\mathbb{Z}$ (du fait que m est premier avec p). Pour des raisons de cardinalité, c'est donc une bijection. Ainsi, en associant à chaque classe de $\mathbb{Z}/p\mathbb{Z}$ son unique représentant dans $[\![0, p-1]\!]$, la multiplication par m induit, après réduction modulo p, une bijection de $[\![0, p-1]\!]$ dans lui-même. Ainsi, $\mu_m \in \mathfrak{S}([\![0, p-1]\!])$.
2. On a clairement, par associativité, $\mu_m \circ \mu_n = \mu_{mn}$, donc, par multiplicativité de la signature :

$$\varepsilon(\mu_{mn}) = \varepsilon(\mu_m)\varepsilon(\mu_n), \qquad \text{soit:} \quad \boxed{\left(\frac{mn}{p}\right)_Z = \left(\frac{m}{p}\right)_Z \left(\frac{n}{p}\right)_Z}.$$

3. Soit m un résidu quadratique modulo m. Il existe donc $n \in \mathbb{Z}$ tel que $n^2 \equiv m \mod p$. On a alors $\mu_m = \mu_{n^2}$, et donc, d'après ce qui précède,

$$\boxed{\left(\frac{m}{p}\right)_Z = \left(\frac{n}{p}\right)_Z^2 = 1},$$

la dernière égalité découlant du fait que le symbole de Zolotarev prend par définition ses valeurs dans $\{-1, 1\}$.
4. Remarquons pour commencer que G est le support d'un cycle de μ_m, vu comme permutation de $\mathbb{Z}/p\mathbb{Z}$: il s'agit du cycle :

$$C = (1 \ m \ m^2 \ \cdots \ m^{r-1})$$

Soit maintenant aG une classe modulo G. Elle est de même cardinal que G, à savoir r, et elle est le support du cycle suivant de μ_m :

$$(a \ am \ am^2 \ \cdots \ am^{r-1}).$$

Ainsi, on obtient autant de cycles à supports disjoints que de classes d'équivalence modulo G (à savoir $\frac{p-1}{r}$). Il reste alors un dernier cycle, de longueur 1, constitué du point fixe 0.
Ainsi, μ_m est bien composée de $\frac{p-1}{r}+1$ cycles à supports disjoints, dont 1 point fixe, les autres étant de longueur r. $\boxed{\text{Le type cyclique est donc } 1^1 r^{\frac{p-1}{r}}}$.
5. La signature d'une permutation σ d'un ensemble de cardinal n étant la parité de $n - C(\sigma)$ où $C(\sigma)$ est le nombre de cycles, on en déduit que

$$\varepsilon(\mu_m) = (-1)^{p - \frac{p-1}{r} + 1} \qquad \text{soit:} \quad \boxed{\varepsilon(\mu_m) = (-1)^{\frac{p-1}{r}}},$$

puisque $p+1$ est pair. On distingue alors 2 cas :
   - Si $\dfrac{p-1}{r}$ est pair, disons $\dfrac{p-1}{r} = 2\ell$, alors

$$\left(\frac{m}{p}\right)_Z = \varepsilon(\mu_m) = (-1)^{\frac{p-1}{r}} = 1.$$

   Par ailleurs,

$$m^{\frac{p-1}{2}} = m^{r\ell} = (m^r)^\ell = 1^\ell = 1 = \left(\frac{m}{p}\right)_Z.$$

- Si $k = \dfrac{p-1}{r}$ est impair, alors $\left(\dfrac{m}{p}\right)_Z = -1$, et d'un autre côté, r étant pair, $\frac{rk}{2}$ est entier, et non divisible par r, sinon, on aurait
$$2r \div rk \qquad \text{puis:} \qquad 2 \div k,$$
ce qui contredit notre hypothèse. Ainsi, $m^{\frac{p-1}{2}} \not\equiv 1\ [p]$ (puisque l'exposant n'est pas multiple de l'ordre). Puisque $m^{\frac{p-1}{2}} \in \{-1, 1\}$ (d'après le théorème de Fermat), on en déduit que $m^{\frac{p-1}{2}} = -1 = \left(\frac{m}{p}\right)_Z$.

Ainsi, dans les deux cas, $\boxed{m^{\frac{p-1}{2}} = -1 = \left(\dfrac{m}{p}\right)_Z.}$

D'après la formule d'Euler (question I-1(c)), on en déduit que
$$\boxed{\left(\frac{m}{p}\right)_Z = \left(\frac{m}{p}\right)_L}$$

6. Comme dans les parties précédentes, q désigne un nombre premier impair distinct de p.
Notons $\tau : x \mapsto x+1$ la permutation circulaire de $\mathbb{Z}/p\mathbb{Z}$ (il s'agit du cycle $(0\ 1\ \cdots\ p-1)$). Alors l'application $\nu : i \mapsto qi + j$ est égale à la composée $\tau^j \circ \mu_q$. Il s'agit donc d'une $\boxed{\text{permutation de } \mathbb{Z}/p\mathbb{Z}}$, en tant que composée de permutations.
On a de plus
$$\varepsilon(\nu) = \varepsilon(\tau)^j \varepsilon(\mu_q).$$
Or, τ est une permutation circulaire, donc un cycle de longueur p. Sa signature est donc $(-1)^{p+1} = 1$, puisque p est impair. On en déduit que
$$\boxed{\varepsilon(\nu) = \varepsilon(\mu_q) = \left(\frac{q}{p}\right)_Z}.$$

7. L'application σ_j est clairement bien définie. Il s'agit d'une permutation, puisqu'on peut facilement défini une réciproque (en utilisant la réciproque de la permutation ν de la question précédente) :
$$(i, j') \mapsto \begin{cases} (\nu^{-1}(i), j') & \text{si } j = j' \\ (i, j') & \text{sinon.} \end{cases}$$
De plus, tout couple (i, j') tel que $j' \neq j$ est point fixe, et si $C = (x_1\ \ldots\ x_k)$ est un cycle de ν définie dans la question précédente, $C_j = ((x_1, j)\ (x_2, j)\ \cdot\ (x_k, j))$ est un cycle de σ_j. La réciproque est vraie aussi. Ainsi, les cycles non triviaux de σ_j sont de même type que ceux de ν. Comme les cycles triviaux (de longueur 1) ont une signature de 1, on en déduit que
$$\boxed{\varepsilon(\sigma_j) = \varepsilon(\nu) = \left(\frac{q}{p}\right)_Z}.$$

8. On peut écrire σ comme une composée :
$$\sigma = \sigma_{q-1} \circ \cdots \circ \sigma_1 \circ \sigma_0.$$
Ainsi,
$$\varepsilon(\sigma) = \prod_{j=0}^{q} \varepsilon(\sigma_j) = \left(\frac{q}{p}\right)_Z^q \qquad \text{soit:} \qquad \boxed{\varepsilon(\sigma) = \left(\frac{q}{p}\right)_Z},$$
la dernière déduction provenant de l'imparité de q.

9. La première partie de la question a été traités dans le cours : l'application π est clairement un morphisme de groupe, et si $\pi(k) = (0, 0)$, alors $p \div k$ et $q \div k$, donc $pq \div k$, puisque p et q sont premiers entre eux. Ainsi, le noyau de π est $\{0\}$, donc π est injective. Pour des raisons de cardinalité, c'est donc une bijection. Ainsi, $\boxed{\pi \text{ est un isomophisme de groupes}}$.
La définition de λ est non ambiguë puisque tout entier s'écrit d'au plus une façon sous la forme $qi + j$, $(i, j) \in \mathbb{Z} \times [\![0, q-1]\!]$ (unicité de la division euclidienne). Elle est exhaustive, par existence de ette division, et du fait que pour $k \in [\![0, pq-1]\!]$, le quotient de la division euclidienne est bien strictement inférieur à p : il existe donc

$i \in [\![0, p-1]\!]$ et $j \in [\![0, q-1]\!]$ tels que $k = qi + j$. Enfin, elle est bien à valeurs dans $[\![0, pq-1]\!]$, puisque pour $i \in [\![0, p-1]\!]$ et $j \in [\![0, q-1]\!]$,

$$0 \leqslant pj + i \leqslant p(q-1) + (p-1) = pq - 1.$$

Ainsi, $\boxed{\lambda \text{ est bien définie.}}$

Par symétrie, $pj + i \mapsto qi + j$ est tout aussi bien définie, et constitue une réciproque de λ, donc λ est bijective. C'est donc une $\boxed{\text{permutation de } [\![0, pq-1]\!]}$.

Enfin,

$$\pi(qi+j) = (qi+j, qi+j) = (qi+j, j) = \sigma(i,j), \qquad \text{donc:} \qquad \pi^{-1} \circ \sigma(i,j) = (qi+j).$$

De même, par symétrie, $\pi^{-1} \circ \tau(i,j) = pj + i$.

De la définition de λ, il vient bien l'égalité :

$$\boxed{\lambda \circ \pi^{-1} \circ \sigma = \pi^{-1} \circ \tau}.$$

10. On a donc

$$\lambda \circ \pi^{-1} \circ \sigma \circ \pi = \pi^{-1} \circ \tau \circ \pi.$$

Or, $\pi^{-1} \circ \sigma \circ \pi$ est une permutation de $\mathbb{Z}/pq\mathbb{Z}$ (ou de façon similaire de $[\![0, pq-1]\!]$), ayant même type cyclique que σ. En effet, si $(x_1 \ \ldots \ x_k)$ est un cycle de $\pi^{-1} \circ \sigma \circ \pi$, alors $(\pi(x_1) \ \ldots \ \pi(x_k))$ est un cycle de σ, et réciproquement (effet de la conjugaison sur les cycles). De même pour τ.

Ainsi, la signature ne dépendant que du type cyclique,

$$\varepsilon(\tau) = \varepsilon(\pi^{-1} \circ \tau \circ \pi) = \varepsilon(\lambda)\varepsilon(\pi^{-1} \circ \sigma \circ \pi) = \varepsilon(\lambda)\varepsilon(\sigma).$$

On détermine alors la signature de λ en comptant les inversions, c'est-à-dire les entiers $n < n'$ tels que $\lambda(n) > \lambda(n')$. On écrit $n = qi + j$ et $n' = q'i + j'$ les divisions euclidiennes de n et n' par q. L'inégalité $n < n'$ se traduit alors par l'inégalité lexicographique $(i,j) < (i',j')$

Par ailleurs, $\lambda(n) = pj + i$ et $\lambda(n') = pj' + i'$. Ainsi, de la même façon, l'inégalité $\lambda(n) > \lambda(n')$ se traduit par l'inégalité lexicographique $(j,i) > (j',i')$.

Il s'agit donc de dénombrer les couples de couples $((i,j),(i',j'))$, tels que $(i,j) < (i',j')$ et $(j',i') < (j,i)$ pour l'ordre lexicographique. On ne peut clairement par avoir $i = i'$, sinon la première inégalité amène $j < j'$, qui est incompatible avec la deuxième. De même, on ne peut pas avoir $j' = j$. Ainsi, on doit avoir $i < i'$ et $j' < j$. Réciproquement, ces conditions donnent bien les inégalités qu'on veut. Par conséquent, un tel couple de couple sera déterminé par le choix d'une première paire $\{i, i'\} \in \mathcal{P}_2([\![0, p-1]\!])$ (i sera alors le plus petit des deux éléments), et d'une deuxième paire $\{j, j'\} \in \mathcal{P}_2([\![0, q-1]\!])$ (j sera alors le plus grand des deux éléments).

Le nombre de couples de ce type est donc $\binom{p}{2}\binom{q}{2} = \frac{p(p-1)}{2} \cdot \frac{q(q-1)}{2}$.

On en déduit que

$$\varepsilon(\lambda) = (-1)^{\frac{p(p-1)}{2} \cdot \frac{q(q-1)}{2}} = ((-1)^{pq})^{\frac{p-1}{2} \cdot \frac{q-1}{2}}, \qquad \text{donc:} \qquad \boxed{\varepsilon(\lambda) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}},$$

puisque pq est impair.

En injectant cela dans l'identité précédente, on obtient bien, d'après les questions IV-5 et IV-8 :

$$\boxed{\left(\frac{p}{q}\right)_L = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)_L}.$$