Agrégation interne de mathématiques

2023 - Composition 1

Éléments de correction proposés par G. Dupont
http://maths-concours.fr/

Version du 12 avril 2023

Vrai-Faux

1. **Les affirmations suivantes sont-elles vraies ou fausses ? On justifiera soigneusement les réponses.**

   (a) **Affirmation : «Pour tout nombre premier p et pour tout entier naturel n non nul, l'anneau $(\mathbb{Z}/p^n\mathbb{Z}, +, \cdot)$ est un corps.**

   Faux. Par exemple, $p = 2$ et $n = 2$, $(\mathbb{Z}/4Z, +, \cdot)$ n'est pas un corps car il n'est pas intègre. En effet, $\overline{2}\times\overline{2} = \overline{4} = \overline{0}$ alors que $\overline{2} \neq \overline{0}$.

   (b) **Affirmation : «Si p est un nombre premier impair, alors la classe de 2 engendre le groupe multiplicatif des éléments inversibles de l'anneau $(\mathbb{Z}/p^n\mathbb{Z}, +, \cdot)$»**

   Faux. Par exemple, $p = 7$ et $n = 2$, alors le groupe multiplicatif de $(\mathbb{Z}/49Z, +, \cdot)$ comporte $\varphi(49) = 7^2 - 7 = 42$ éléments mais $\overline{2}$ est d'ordre multiplicatif 21 dans $\mathbb{Z}/49\mathbb{Z}$ donc il engendre un sous-groupe d'indice 2 dans le groupe multiplicatif.

   (c) **Affirmation : «Le groupe multiplicatif de $(\mathbb{Z}/9\mathbb{Z}, +, \cdot)$ est cyclique.»**

   Vrai. Le groupe multiplicatif de $(\mathbb{Z}/9Z, +, \cdot)$ comporte $\varphi(9) = 3^2 - 3 = 6$ éléments et $\overline{2}$ est d'ordre 6 dans ce groupe.

   (d) **Si a est un entier relatif, alors on note $\overline{a}$ la classe de a dans $\mathbb{Z}/5\mathbb{Z}$.**

   Étant donnés quatre entiers relatifs a, b, c et d, on note M la matrice de $\mathcal{M}_2(\mathbb{Z})$ définie par $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et on note $\overline{M}$ la matrice de $\mathcal{M}_2(\mathbb{Z}/5\mathbb{Z})$ définie par $\overline{M} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$.

   Affirmation : « Si $M \in \mathrm{GL}_2(\mathbb{R})$, alors $\overline{M} \in \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$.»

   Faux. Il suffit de considérer la matrice $M = 5I_2 \in \mathrm{GL}_2(\mathbb{R})$, dont la réduction $\overline{M}$ modulo 5 est la matrice nulle. Plus généralement, le déterminant étant polynômial en les entrées de M et la réduction $a \mapsto \overline{a}$ étant un morphisme d'anneaux de $\mathbb{Z}$ vers $\mathbb{Z}/5\mathbb{Z}$, toute matrice M dont le déterminant est un multiple non nul de 5 sera inversible alors que $\overline{M}$ ne le sera pas.

   (e) **Soient K et L deux corps commutatifs.**

   Affirmation : « Un morphisme d'anneaux $\mu : K \longrightarrow L$ est toujours injectif.»

   Vrai. Puisque μ induit un morphisme de groupes additifs, on sait que μ est injectif si, et seulement si, $\ker(\mu) = \{0_K\}$. Le noyau d'un morphisme d'anneaux étant un idéal de l'anneau de départ, $\ker(\mu)$ est un idéal de K. Mais K étant un corps, il ne possède que deux idéaux : $\{0_K\}$ et K lui-même. Or $\ker(\mu) \neq K$ car $\mu(1_K) = 1_L \neq 0_L$ de sorte que $\ker(\mu) = \{0_K\}$.

Exercice 1

Soit p un nombre premier. On désigne par $\mathbb{K}$ le corps $\mathbb{Z}/p\mathbb{Z}$.

2. **Soit E un $\mathbb{K}$-espace vectoriel et soit k un entier strictement positif. Notons $(x_1, \dots, x_{k+1})$ une famille constituée de $k+1$ vecteurs de E telle que la famille $(x_1, \dots, x_k)$ est libre.**
   Montrer que la famille de vecteurs $(x_1, \dots, x_{k+1})$ est libre si, et seulement si, le vecteur x_{k+1} n'est pas combinaison linéaire des vecteurs $x_1, \dots, x_k$.
   Soit $(\lambda_1, \dots, \lambda_{k+1}) \in \mathbb{K}^{k+1}$ telle que $\sum_{i=1}^{k+1} \lambda_i x_i = 0_E$. On a donc :
   $$\lambda_{k+1} x_{k+1} = -\sum_{i=1}^{k} \lambda_i x_i. \tag{1}$$
   Supposons que x_{k+1} n'est pas combinaison linéaire des vecteurs $x_1, \dots, x_k$. Si $\lambda_{k+1} \neq 0$, on obtient :
   $$x_{k+1} = \sum_{i=1}^{k} \left(-\frac{\lambda_i}{\lambda_{k+1}}\right) x_i \in \mathrm{Vect}(x_1, \dots, x_k),$$
   une contradiction. Ainsi, $\lambda_{k+1} = 0$ et donc l'égalité (1) devient $\sum_{i=1}^{k} \lambda_i x_i = 0_E$. La famille $(x_1, \dots, x_k)$ étant libre, il vient $\lambda_1 = \cdots = \lambda_k = 0$ et donc, tous les λ_i sont nuls, pour $i \in [\![0, k+1]\!]$, ce qui prouve la liberté de $(x_1, \dots, x_{k+1})$.
   Réciproquement, si x_{k+1} est combinaison linéaire de $x_1, \dots, x_k$, alors il existe $\lambda_1, \dots, \lambda_k$ des scalaires tels que
   $$x_{k+1} = \sum_{i=1}^{k} \lambda_i x_i$$
   ou encore
   $$\sum_{i=1}^{k} \lambda_i x_i - 1 \times x_{k+1} = 0_E,$$
   ce qui fournit une combinaison linéaire nulle non triviale de $x_1, \dots, x_{k+1}$, la famille $(x_1, \dots, x_{k+1})$ est donc liée.

3. **Soient n et k deux entiers strictement positifs vérifiant la relation $k \leq n$.**
   Montrer par récurrence que le nombre de familles libres constituées de k vecteurs de $\mathbb{K}^n$ vaut $(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})$.
   On fait la preuve par récurrence finie sur $k \in [\![1, n]\!]$.
   <u>Initialisation :</u> Pour $k = 1$, une famille composée d'un vecteur est libre si et seulement si ce vecteur est non nul. $\mathbb{K}$ possédant p éléments, $\mathbb{K}^n$ possède p^n vecteurs dont un seul est nul, on a donc $p^n - 1$ choix.
   <u>Hérédité :</u> Soit $k \in [\![1, n-1]\!]$ tel que la propriété est vérifiée. D'après la question **2**, choisir une famille libre de $k+1$ vecteurs $(x_1, \dots, x_{k+1})$ revient à choisir une famille libre $(x_1, \dots, x_k)$ puis un vecteur $x_{k+1} \in \mathbb{K}^n \setminus \mathrm{Vect}(x_1, \dots, x_k)$. Par hypothèse de récurrence, on a $(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})$ choix pour $(x_1, \dots, x_k)$ puis, $\mathrm{Vect}(x_1, \dots, x_k)$ étant un $\mathbb{K}$-espace vectoriel de dimension k, il est isomorphe à $\mathbb{K}^p$ et contient donc p^k vecteurs. Ainsi, on a $p^n - p^k$ choix pour x_{k+1}. Par principe multiplicatif, on a donc $(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})(p^n - p^k)$ choix au total, ce qui prouve l'hérédité.

4. **Soit n un entier strictement positif. Déterminer le cardinal de $\mathrm{GL}_n(\mathbb{K})$.**
   Soit $M \in \mathcal{M}_n(\mathbb{K})$ dont on note $C_1, \dots, C_n$ les colonnes. On sait que
   $$M \in \mathrm{GL}_n(\mathbb{K}) \iff \mathrm{rg}(M) = n \iff \mathrm{rg}(C_1, \dots, C_n) = n \iff (C_1, \dots, C_n) \text{ est libre.}$$
   Ainsi, choisir une matrice de $\mathrm{GL}_n(\mathbb{K})$ revient à choisir une famille libre de n vecteurs de $\mathbb{K}^n$. D'après la question **3**, on a $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ tels choix. Autrement dit :

$$\boxed{\mathrm{card}(\mathrm{GL}_n(\mathbb{K})) = \prod_{j=0}^{n-1}(p^n - p^j).}$$

Exercice 2

5. **Soit n un entier naturel. On note $\mathcal{D}_n$ l'ensemble des entiers naturels qui divisent n. On souhaite montrer que pour tout entier n strictement positif on a l'égalité $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.**

   On pose $f(n) = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

   (a) **Soit p un nombre premier. Pour tout entier i, calculer $\varphi(p^i)$. En déduire la valeur de $f(p^k)$ pour tout entier k strictement positif.**
   Soit $i \in \mathbb{N}^*$. p étant un nombre premier, les seuls entiers de $[\![1, p^i]\!]$ qui ne sont pas premiers avec p^i sont ceux qui sont divisibles par p. L'application $k \mapsto pk$ induisant une bijection de $[\![1, p^{i-1}]\!]$ vers l'ensemble des multiples de p dans $[\![1, p^i]\!]$, il y a p^{i-1} nombres nombres premiers avec p^i dans $[\![1, p^i]\!]$ et donc :

$$\boxed{\forall i \in \mathbb{N}^*, \quad \varphi(p^i) = p^i - p^{i-1}.}$$

   Et, par définition, on a $\varphi(1) = 1$.
   Soit $k \in \mathbb{N}^*$. Puisque p est premier, on a :

$$\mathcal{D}_{p^k} = \left\{ p^i \,\middle|\, i \in [\![0, k]\!] \right\}$$

   donc

$$f(p^k) = \sum_{i=0}^{k} \varphi(p^i) = 1 + \sum_{i=1}^{k} (p^i - p^{i-1}) = 1 + (p^k - 1) = p^k.$$

   On a ainsi :

$$\boxed{\forall k \in \mathbb{N}^*, \quad f(p^k) = p^k.}$$

   (b) **Soient m_1 et m_2 deux entiers naturels premiers entre eux. Montrer que l'application :**

$$P : \left\{ \begin{array}{ccc} \mathcal{D}_{m_1} \times \mathcal{D}_{m_2} & \longrightarrow & \mathcal{D}_{m_1 m_2} \\ (d_1, d_2) & \mapsto & d_1 d_2 \end{array} \right.$$

   est bien définie et bijective.
   Notons $m_1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition en facteurs premiers de m_1 et $m_2 = p_{r+1}^{\alpha_{r+1}} \cdots p_s^{\alpha_s}$ celle de m_2. Puisque m_1 et m_2 sont premiers entre eux, les p_i sont deux à deux distincts.
   Soit $(d_1, d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$. On peut donc écrire

$$d_1 = p_1^{\beta_1} \cdots p_r^{\beta_r} \quad \text{et} \quad d_2 = p_{r+1}^{\beta_{r+1}} \cdots p_s^{\beta_s}$$

   où, pour tout $i \in [\![1, s]\!], \beta_i \in [\![0, \alpha_i]\!]$.
   Alors on a :

$$d_1 d_2 = p_1^{\beta_1} \cdots p_s^{\beta_s} | p_1^{\alpha_1} \cdots p_s^{\alpha_s} = m_1 m_2$$

   donc l'application est bien définie, et l'unicité de la décomposition en facteurs premiers implique l'injectivité.
   Pour la surjectivité, il suffit d'observer qu'un diviseur d de $m_1 m_2$ s'écrit $d = p_1^{\beta_1} \cdots p_s^{\beta_s}$ avec, pour tout $i \in [\![1, s]\!], \beta_i \in [\![0, \alpha_i]\!]$. Si on pose $d_1 = p_1^{\beta_1} \cdots p_r^{\beta_r}$ et $d_2 = p_{r+1}^{\beta_{r+1}} \cdots p_s^{\beta_s}$, alors $d = d_1 d_2 = P(d_1, d_2)$.
   Ainsi,

$$P : \left\{ \begin{array}{ccc} \mathcal{D}_{m_1} \times \mathcal{D}_{m_2} & \longrightarrow & \mathcal{D}_{m_1 m_2} \\ (d_1, d_2) & \mapsto & d_1 d_2 \end{array} \right.$$

   est bijective.

   (c) **En déduire que lorsque m_1 et m_2 sont deux entiers naturels premiers entre eux, on a la relation $f(m_1 m_2) = f(m_1) f(m_2)$.**

On a

$$f(m_1m_2) = \sum_{d \in \mathcal{D}_{m_1m_2}} \varphi(d) = \sum_{(d_1,d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}} \varphi(d_1d_2)$$

mais, d'après le théorème des restes chinois, si d_1 et d_2 sont premiers entre eux (ce qui est le cas quand $(d_1, d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$), on a $\varphi(d_1d_2) = \varphi(d_1)\varphi(d_2)$ donc :

$$\sum_{(d_1,d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}} \varphi(d_1d_2) = \sum_{\substack{d_1 \in \mathcal{D}_{m_1} \\ d_2 \in \mathcal{D}_{m_2}}} \varphi(d_1)\varphi(d_2) = \left(\sum_{d_1 \in \mathcal{D}_{m_1}} \varphi(d_1)\right)\left(\sum_{d_2 \in \mathcal{D}_{m_2}} \varphi(d_2)\right) = f(m_1)f(m_2).$$

On a donc bien, pour m_1 et m_2 premiers entre eux :

$$\boxed{f(m_1m_2) = f(m_1)f(m_2).}$$

(d) Montrer que pour tout entier n strictement positif on a l'égalité $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

On le montre par récurrence sur le nombre r de facteurs premiers distincts de n.
Initialisation : Si n possède un unique facteur premier, alors $n = p^k$ et le résultat a été établi à la question **5.a**.
Hérédité : Soit $r \in \mathbb{N}^*$ tel que la propriété soit vraie pour les entiers admettant exactement n facteurs premiers distincts. Considérons alors un entier de la forme :

$$n = \underbrace{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}_{=m_1} \underbrace{p_{r+1}^{\alpha_{r+1}}}_{=m_2}.$$

Alors m_1 et m_2 sont premiers entre eux et donc, d'après **5.c**, on a

$$f(n) = f(m_1)f(m_2)$$

mais, par hypothèse de récurrence $f(m_1) = m_1$ et, d'après **5.a**, on a $f(m_2) = m_2$ donc

$$f(n) = m_1m_2 = n,$$

d'où l'hérédité.
Ainsi, on a démontré :

$$\boxed{\forall n \in \mathbb{N}^*, \quad \sum_{d \in \mathcal{D}_n} \varphi(d) = n.}$$

6. Soit $(\mathbb{K}, +, \cdot)$ un corps de cardinal fini égal à $c + 1$. On a $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ et on souhaite montrer que le groupe $(\mathbb{K}^*, \cdot)$ de cardinal c est cyclique.
Pour tout entier d de $\mathcal{D}_c$, on note $N(d)$ le nombre d'éléments de $(\mathbb{K}^*, \cdot)$ qui sont d'ordre d.

(a) Déterminer la valeur de $\sum_{d \in \mathcal{D}_c} N(d)$.

Pour tout entier d, on note Ω_d l'ensemble des éléments d'ordre d dans $(\mathbb{K}^*, \cdot)$. Le groupe $(\mathbb{K}^*, \cdot)$ étant d'ordre c, il suit du théorème de Lagrange que l'ordre de chaque élément de $\mathbb{K}^*$ est un diviseur de c. En partitionnant les éléments de $\mathbb{K}^*$ par leur ordre, on obtient :

$$\mathbb{K}^* = \bigsqcup_{d \in \mathcal{D}_c} \Omega_d.$$

En passant au cardinal, on obtient :

$$\boxed{c = \sum_{d \in \mathcal{D}_c} N(d).}$$

(b) Soit d un élément de $\mathcal{D}_c$.

i. **On suppose qu'il existe un élément x d'ordre d dans $\mathbb{K}^*$ et on note H le sous-groupe de $(\mathbb{K}^*, \cdot)$ engendré par x. En introduisant un polynôme judicieux, montrer que tout élément d'ordre d de $\mathbb{K}^*$ est dans H.**

Considérons le polynôme $P = X^d - 1 \in \mathbb{K}[X]$. Puisque $\mathbb{K}$ est un corps, P admet au plus d racines dans $\mathbb{K}$. D'autre part, $H = \langle x \rangle$ est cyclique d'ordre d donc, d'après le théorème de Lagrange, tout élément y de H a un ordre qui divise d. En particulier, $y^d = 1$ et donc H est inclus dans l'ensemble des racines de P. Par cardinalité, H est égal à l'ensemble des racines de P. Tout élément d'ordre p étant racine de P, il est donc dans H.

Avec les notations introduites à la question précédente, on a donc :

$$\boxed{\forall x \in \Omega_d, \quad \Omega_d \subset \langle x \rangle\,.}$$

ii. **Montrer que pour tout entier d de $\mathcal{D}_d$, on a l'égalité $N(d) \leq \varphi(d)$.**

Soit $x \in \Omega_d$ et $H = \langle x \rangle$. D'après la question précédente, H étant cyclique d'ordre d, l'application

$$\psi : \begin{cases} H & \longrightarrow & \mathbb{Z}/d\mathbb{Z} \\ x^k & \longmapsto & \overline{k} \end{cases}$$

est un isomorphisme de groupes. Les éléments d'ordre d dans H étant les x^k avec $k \wedge d = 1$, ils correspondent sous ψ à des éléments inversibles de l'anneau $\mathbb{Z}/d\mathbb{Z}$. L'ensemble Ω_d des éléments d'ordre d dans $\mathbb{K}^*$ étant un sous-ensemble de H, ψ induit une application injective de Ω_d vers $(\mathbb{Z}/d\mathbb{Z})^*$ et donc

$$N(d) = \mathrm{card}(\Omega_d) \leq \mathrm{card}\,(\mathbb{Z}/d\mathbb{Z})^* = \varphi(d).$$

(c) Montrer que pour tout entier d de $\mathcal{D}_c$, on a l'égalité $N(d) = \varphi(d)$. En déduire que $(\mathbb{K}^*, \cdot)$ est un groupe cyclique.

D'après **6.a** et **5.d**, on a :

$$c = \sum_{d \in \mathcal{D}_c} N(d) \quad \text{et} \quad c = \sum_{d \in \mathcal{D}_c} \varphi(d).$$

Par d'ailleurs, d'après **6.b**, pour tout $d \in \mathcal{D}_c$, on a $N(d) \leq \varphi(d)$. Ainsi, on a :

$$c = \sum_{d \in \mathcal{D}_c} N(d) \leq \sum_{d \in \mathcal{D}_c} \varphi(d) = c$$

et donc, pour tout $d \in \mathcal{D}_c$, $N(d) = \varphi(d)$.

En particulier, on a $N(c) = \varphi(c) \geq 1$ donc il existe au moins un élément d'ordre c dans $\mathbb{K}^*$. En particulier :

$$\boxed{(\mathbb{K}^*, \cdot) \text{ est cyclique.}}$$

Problème

Dans tout le problème, p désigne un nombre premier.

I. Valuation et valeur absolue p adiques

I.A. Définition de la valuation

7. **Soit n un entier relatif non nul. Montrer qu'il existe un unique entier k tel que p^k divise n et p^{k+1} ne divise pas n.**
   Soit $n \in \mathbb{N}^*$. On pose :
   $$V_p(n) = \left\{k \in \mathbb{N} \;\middle|\; p^k \text{ divise } n\right\}.$$
   C'est une partie non vide de $\mathbb{R}$ car elle contient 0, et elle est majorée car la suite $(p^k)_{k\in\mathbb{N}}$ tend vers l'infini quand k tend vers l'infini de sorte que p^k est supérieur à n, et ne peut donc le diviser, à partir d'un certain rang.
   Ainsi, $V_p(n)$ admet une borne supérieure. Par ailleurs, $V_p(n)$ étant inclus dans $\mathbb{N}$, c'est un sous-ensemble discret de $\mathbb{R}$ et cette borne supérieure est un maximum.
   $$\boxed{\text{L'entier } v_p(n) = \max V_p(n) \text{ vérifie les conditions requises.}}$$
   L'unique entier k ainsi défini est appelé valuation p-adique de n et on le note $v_p(n)$.

8. **Soient a et b deux entiers relatifs non nuls. Montrer l'égalité $v_p(ab) = v_p(a) + v_p(b)$.**
   On commence par observer que, pour tout entier n tel que $|n| \geq 2$, la décomposition en facteurs premiers de n s'écrit
   $$|n| = \prod_{q\in\mathcal{P}} q^{v_q(n)},$$
   où $\mathcal{P}$ désigne l'ensemble des nombres premiers. En outre, cette écriture est encore valide pour $|n| = 1$.
   Alors, pour tout couple (a, b) d'entiers relatifs non nuls, on a :
   $$|ab| = \prod_{q\in\mathcal{P}} q^{v_q(ab)}$$
   mais
   $$|ab| = |a| \times |b| = \left(\prod_{q\in\mathcal{P}} q^{v_q(n)}\right)\left(\prod_{q\in\mathcal{P}} q^{v_q(n)}\right) = \prod_{q\in\mathcal{P}} q^{v_q(a)+v_q(b)}.$$
   Par unicité de la décomposition en facteurs premiers, on peut identifier les exposants de p dans ces deux décompositions et il vient :
   $$\boxed{v_p(ab) = v_p(a) + v_p(b).}$$

9. **En déduire que, si a, b, c et d sont des entiers relatifs non nuls qui vérifient la relation $\dfrac{a}{b} = \dfrac{c}{d}$, alors $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.**
   On a
   $$\begin{aligned} \frac{a}{b} = \frac{c}{d} &\Rightarrow ad = bc \\ &\Rightarrow v_p(ad) = v_p(bc) \\ &\Rightarrow v_p(a) + v_p(d) = v_p(b) + v_p(c) \\ &\Rightarrow v_p(a) - v_p(b) = v_p(c) - v_p(d). \end{aligned}$$
   Étant donné un nombre rationnel non nul r, si a et b sont deux entiers relatifs non nuls tels que $r = \dfrac{a}{b}$, alors l'entier $v_p(r) = v_p(a) - v_p(b)$ est appelé valuation p-adique de r.

10. Montrer que si r et s sont deux nombres rationnels non nuls, alors on a l'égalité

$$v_p(rs) = v_p(r) + v_p(s).$$

On pose $r = \dfrac{a}{b}$ et $s = \dfrac{a'}{b'}$ avec a, b, a', b' entiers non nuls. Alors on a $rs = \dfrac{aa'}{bb'}$ et donc :

$$\begin{aligned} v_p(rs) &= v_p(aa') - v_p(bb') \\ &= v_p(a) + v_p(a') - (v_p(b) + v_p(b')) \\ &= v_p(a) - v_p(b) + v_p(a') - v_p(b') \\ &= v_p(r) + v_p(s). \end{aligned}$$

On a donc bien :

$$\boxed{\forall (r,s) \in (\mathbb{Q}^*)^2, \quad v_p(rs) = v_p(r) + v_p(s).}$$

11. Montrer que si r et s sont deux nombres rationnels non nuls tels que $r \neq s$, alors on a l'inégalité

$$v_p(r-s) \geq \min(v_p(r), v_p(s)).$$

Si r ou s est nul, le résultat est trivial. On suppose donc que r et s sont non nuls.
On observe d'abord que le résultat est vrai pour les entiers. En effet, si m et n sont deux entiers naturels non nuls, on $p^{v_p(n)}$ divise n et $p^{v_p(m)}$ divise m de sorte que $p^{\min(v_p(m), v_p(n))}$ divise $m - n$ et donc $v_p(m-n) \geq \min(v_p(m), v_p(n))$.
Supposons maintenant que $r = \dfrac{a}{b}$ et $s = \dfrac{a'}{b'}$ avec a, b, a', b' des entiers non nuls. Alors :

$$r - s = \frac{a}{b} - \frac{a'}{b'} = \frac{ab' - a'b}{bb'}$$

de sorte que

$$\begin{aligned} v_p(r-s) &= v_p(ab' - a'b) - v_p(bb') \\ &\geq \min(v_p(ab'), v_p(a'b)) - (v_p(b) + v_p(b')) \\ &= \min(v_p(a) + v_p(b'), v_p(a') + v_p(b)) - (v_p(b) + v_p(b')) \\ &= \min(v_p(a) - v_p(b), v_p(a') - v_p(b')) \\ &= \min(v_p(r), v_p(s)). \end{aligned}$$

On a donc bien :

$$\boxed{\forall (r,s) \in (\mathbb{Q}^*)^2, \quad v_p(r-s) \geq \min(v_p(r), v_p(s)).}$$

Par convention, on pose $v_p(0) = +\infty$. Ceci permet de définir une application $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\}$.

12. En prenant soin de préciser les inégalités et les règles de calcul dans $\mathbb{Z} \cup \{+\infty\}$, vérifier que les résultats des questions 10. et 11. restent valables lorsque r et s sont deux nombres rationnels.

Pour la question 10 :
Si r et s sont nuls, on a $rs = 0$, ce qui, avec la convention

$$(+\infty) + (+\infty) = +\infty,$$

prolonge le résultat trouvé à la question 10.
Si l'un des deux seulement est, on a $rs = 0$, ce qui, avec la convention

$$\forall m \in \mathbb{Z}, \quad m + (+\infty) = +\infty,$$

prolonge bien le résultat trouvé à la question 10.
Pour la question 11 :
Si r et s sont nuls, on a $r - s = 0$, ce qui, avec la convention

$$\min(+\infty, +\infty) = +\infty$$

prolonge le résultat trouvé à la question 11.
Si r est non nul et s nul, on a $r - s = r$, ce qui, avec la convention

$$\forall m \in \mathbb{Z}, \min(m, +\infty) = m$$

prolonge le résultat trouvé à la question 11.
Enfin, si r est nul et s non nul, on a $v_p(r - s) = v_p(s - r)$ et on est ramené au cas précédent.

$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\}$ vérifie les relations des questions **10.** et **11.**

I.B. Étude de $v_p(n!)$

Soit n un entier naturel non nul.

13. Étant donné un entier naturel k, on note E_k l'ensemble des entiers $i \in [\![1, n]\!]$ tels que $v_p(i) \geq k$. Décrire les éléments de E_k puis déterminer le cardinal de E_k.

Pour tout $k \in \mathbb{N}$, les éléments de E_k sont les entiers de $[\![1, n]\!]$ qui sont divisibles par p^k. Ces nombres s'écrivant $p^k d$ avec d tel que $1 \leq d \leq \dfrac{n}{p^k}$, on obtient :

$$\boxed{\operatorname{card}(E_k) = \left\lfloor \frac{n}{p^k} \right\rfloor.}$$

14. Pour un entier i fixé dans $[\![1, n]\!]$, déterminer le nombre d'entiers k tels que $i \in E_k$. En déduire la formule :

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Pour tout $i \in \mathbb{N}$, on a :

$$v_p(i) = \operatorname{card}\left\{k \in \mathbb{N}^* \mid k \leq v_p(i)\right\}$$

donc

$$\begin{aligned}
v_p(n!) &= v_p\left(\prod_{i=1}^{n} i\right) \\
&= \sum_{i=1}^{n} v_p(i) \\
&= \sum_{i=1}^{n} \operatorname{card}\left\{k \in \mathbb{N}^* \mid k \leq v_p(i)\right\} \\
&= \operatorname{card}\left\{(i, k) \in [\![1, n]\!] \times \mathbb{N}^* \mid k \leq v_p(i)\right\} \\
&= \sum_{k \in \mathbb{N}^*} \left\{i \in [\![1, n]\!] \mid k \leq v_p(i)\right\} \\
&= \sum_{k \in \mathbb{N}^*} \operatorname{card}(E_k) \\
&= \sum_{k \in \mathbb{N}^*} \left\lfloor \frac{n}{p^k} \right\rfloor,
\end{aligned}$$

les interversions de sommes étant justifiées par le fait que l'on manipule des familles de réels positifs.
On a donc bien :

$$\boxed{v_p(n!) = \sum_{k\in\mathbb{N}^*} \left\lfloor \frac{n}{p^k} \right\rfloor.}$$

15. Application : En utilisant la formule de la question 14., déterminer le nombre de zéros à la fin de l'écriture décimale de 100 !.

Le nombre de zéros à la fin de l'écriture décimale d'un entier n est égal à l'entier d maximal tel que 10^d divise n.
Puisque $10 = 2 \times 5$, ceci revient à déterminer $\min(v_2(n), v_5(n))$.
D'après ce qui précède, on a :

$$v_2(100!) = \sum_{k\in\mathbb{N}^*} \left\lfloor \frac{100}{2^k} \right\rfloor = \sum_{k=1}^{6} \left\lfloor \frac{100}{2^k} \right\rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

et

$$v_5(100!) = \sum_{k\in\mathbb{N}^*} \left\lfloor \frac{100}{5^k} \right\rfloor = \sum_{k=1}^{2} \left\lfloor \frac{100}{5^k} \right\rfloor = 20 + 4 = 24$$

de sorte que $\min(v_2(100!), v_5(100!)) = 24$.
En conclusion :

$$\boxed{\text{Il y a 24 zéros à la fin de l'écriture décimale de 100!.}}$$

Remarque : On peut vérifier expérimentalement ce résultat avec la fonction suivante :

```python
def nb_zeros(N):
    k = 1
    while N%10**k ==0:
        k +=1
    return k-1
```

Alors, on a obtenu dans la console :

```
In: import math

In: nb_zeros(math.factorial(100))
Out: 24
```

16. Montrer que pour tout entier n strictement positif on a la majoration suivante :

$$v_p(n!) \leq \frac{n}{p-1}.$$

D'après la question **14.**, on a :

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \\ &\leq \sum_{k=1}^{+\infty} \frac{n}{p^k} \\ &= \frac{n}{p} \sum_{k=0}^{+\infty} \left(\frac{1}{p}\right)^k \\ &= \frac{n}{p} \times \frac{1}{1-\frac{1}{p}} \end{aligned}$$

$$= \frac{n}{p-1}.$$

On a donc bien :

$$\boxed{v_p(n!) \leq \frac{n}{p-1}.}$$

0.0.A. I.C. Une caractérisation des puissances de 2.

Soit n un entier naturel non nul. Il se décompose de manière unique en une somme

$$n = \sum_{i=0}^{q} u_i 2^i$$

où $q \in \mathbb{N}$, $(u_0, \ldots, u_q) \in \{0,1\}^{q+1}$ et $u_q \neq 0$. On définit alors

$$s(n) = \sum_{i=0}^{q} u_i.$$

17. Pour tout entier k strictement positif, montrer que l'on a la relation $v_2(k+1) = s(k) - s(k+1) + 1$.

Dans ce corrigé, nous noterons

$$k = (u_q u_{q-1} \cdots u_1 u_0)_2 = \sum_{i=0}^{q} u_i 2^i.$$

Si k est pair, alors $u_0 = 0$ et donc

$$k = (u_q u_{q-1} \cdots u_1 0)_2 \quad \text{et} \quad k+1 = (u_q u_{q-1} \cdots u_1 1)_2$$

de sorte que $s(k) - s(k+1) = -1$. D'autre part, k étant pair, $k+1$ est impair et donc $v_2(k+1) = 0$. On a donc bien

$$v_2(k+1) = s(k) - s(k+1) + 1.$$

Si tous les u_i sont égaux à 1 alors

$$k = (\underbrace{11 \cdots 11}_{q+1 \text{ chiffres}})_2 \quad \text{et} \quad k+1 = (\underbrace{100 \cdots 00}_{q+2 \text{ chiffres}})_2$$

donc

$$s(k) - s(k+1) = (q+1) - 1 = q.$$

D'autre part, $k+1 = 2^{q+1}$ de sorte que $v_2(k+1) = q+1$ et on a bien

$$v_2(k+1) = s(k) - s(k+1) + 1.$$

Sinon, on pose

$$a = \min \{k \in [\![0, n]\!] \mid u_a = 0\}$$

qui est bien défini, de sorte que

$$k = (u_q \cdots u_{a+1} 0 \underbrace{1 \cdots 1}_{a-1 \text{ chiffres}}) \quad \text{et} \quad k+1 = (u_q \cdots u_{a+1} 1 \underbrace{0 \cdots 0}_{a-1 \text{ chiffres}})$$

de sorte que

$$s(k) - s(k+1) + 1 = a - 1 + 1 = a.$$

D'autre part, on a bien $v_2(k+1) = a$ et donc, dans tous les cas :

$$\boxed{\forall k \in \mathbb{N}^*, \quad v_2(k+1) = s(k) - s(k+1) + 1.}$$

18. En déduire une expression de $v_2(n!)$ en fonction de n et de $s(n)$. On a :

$$\begin{aligned}
v_2(n!) &= \sum_{k=1}^{n} v_2(k) \\
&= \sum_{k=1}^{n-1} v_2(k+1) \quad \text{car } v_2(1) = 0 \\
&= \sum_{k=1}^{n-1} (s(k) - s(k+1) + 1) \quad \text{d'après } \mathbf{17.} \\
&= (n-1) + \underbrace{s(1)}_{=1} - s(n) \quad \text{par télescopage} \\
&= n - s(n).
\end{aligned}$$

19. Si n est une puissance de 2, montrer que pour tout entier $k \in [\![1, n-1]\!]$, le coefficient binomial $\binom{n}{k}$ est pair.

Soit $k \in [\![1, n-1]\!]$. On a :

$$\begin{aligned}
v_2\left(\binom{n}{k}\right) &= v_2(n!) - v_2(k!) - v_2((n-k)!) \\
&= n - s(n) - k + s(k) - (n-k) + s(n-k) \\
&= s(k) + s(n-k) - s(n).
\end{aligned}$$

Mais si n est une puissance de 2, alors $s(n) = 1$ et, comme $s(k) \geq 1$ et $s(n-k) \geq 1$, il vient $v_2\left(\binom{n}{k}\right) \geq 1$, c'est-à-dire que $\binom{n}{k}$ est pair.

20. Montrer que si pour tout entier $k \in [\![1, n-1]\!]$, le coefficient binomial $\binom{n}{k}$ est pair, alors n est une puissance de 2.

Si n n'est pas une puissance de 2, alors il existe $a \in [\![1, q-1]\!]$ tel que $u_a = 1$. On peut alors écrire

$$n = (\underbrace{u_q \cdots u_{a+1}}_{q-a-1 \text{ chiffres}} \, 1 \, \underbrace{u_{a-1} \cdots u_0}_{a \text{ chiffres}})_2$$

avec $u_q \neq 0$, de sorte que si on pose

$$k = (\underbrace{0 \cdots 0}_{q-a-1 \text{ chiffres}} \; 1 u_{a-1} \cdots u_0)_2 \in [\![1, n-1]\!]$$

alors

$$n - k = (u_q \cdots u_{a+1} 0 \underbrace{0 \cdots 0}_{a \text{ chiffres}})_2 \in [\![1, n-1]\!].$$

Or, d'après la question précédente, on a :

$$v_2\left(\binom{n}{k}\right) = s(k) + s(n-k) - s(n) = 0$$

et donc $\binom{n}{k}$ est impair.

On a donc établi :

$$\boxed{n \text{ est une puissance de 2 si, et seulement si, } \binom{n}{k} \text{ est pair pour tout } k \in [\![1, n-1]\!].}$$

On peut le vérifier expérimentalement sur un triangle de Pascal, où l'on ne fait afficher que les restes modulo 2 :

1 :	1	1																			
2 :	1	0	1																		
3 :	1	1	1	1																	
4 :	1	0	0	0	1																
5 :	1	1	0	0	1	1															
6 :	1	0	1	0	1	0	1														
7 :	1	1	1	1	1	1	1	1													
8 :	1	0	0	0	0	0	0	0	1												
9 :	1	1	0	0	0	0	0	0	1	1											
10 :	1	0	1	0	0	0	0	0	1	0	1										
11 :	1	1	1	1	0	0	0	0	1	1	1	1									
12 :	1	0	0	0	1	0	0	0	1	0	0	0	1								
13 :	1	1	0	0	1	1	0	0	1	1	0	0	1	1							
14 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1						
15 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					
16 :	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1				
17 :	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1			
18 :	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1		
19 :	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	
20 :	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1

C'est d'ailleurs l'occasion de rappeler que cette réduction modulo 2 du triangle de Pascal fait apparaître un triangle de Sierpinski, voir par exemple https://blogdemaths.wordpress.com/2013/07/16/sierpinski-et-pascal-sont-dans-un-triangle/

I.D. Valeur absolue p-adique

On définit l'application $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_+$ par $|0|_p = 0$ et, pour tout nombre rationnel x non nul, $|x|_p = \dfrac{1}{p^{v_p(x)}}$. Cette application est appelée valeur absolue p-adique.

21. Montrer que pour tout couple (x, y) de nombres rationnels on a :

$$|xy|_p = |x|_p\,|y|_p \qquad |x-y|_p \leq \max(|x|_p\,, |y|_p) \quad \textbf{et} \quad |x+y|_p \leq |x|_p + |y|_p\,.$$

Si x ou y est nul, les relations sont évidentes. On suppose donc que x et y sont non nuls. On a alors :

$$\begin{aligned}
|xy|_p &= \frac{1}{p^{v_p(xy)}} \\
&= \frac{1}{p^{v_p(x)+v_p(y)}} \qquad \text{d'après } \mathbf{10.} \\
&= \frac{1}{p^{v_p(x)}} \times \frac{1}{p^{v_p(y)}} \\
&= |x|_p\,|y|_p\,,
\end{aligned}$$

$$\begin{aligned}
|x-y|_p &= \frac{1}{p^{v_p(x-y)}} \\
&\leq \frac{1}{p^{\min(v_p(x),v_p(y))}} \qquad \text{d'après } \mathbf{11.} \\
&= \max\left(\frac{1}{p^{v_p(x)}}, \frac{1}{p^{v_p(y)}}\right) \\
&= \max(|x|_p\,, |y|_p)
\end{aligned}$$

et, après avoir observé la parité de la valeur absolue p-adique, il vient :

$$\begin{aligned}
|x+y|_p &= |x-(-y)|_p \\
&\leq \max(|x|_p\,, |-y|_p) \quad \text{d'après ce qui précède} \\
&= \max(|x|_p\,, |y|_p) \quad \text{par parité} \\
&\leq |x|_p + |y|_p\,.
\end{aligned}$$

On a donc bien :

$$\boxed{\forall (x,y)\in\mathbb{Q}^2,\quad |xy|_p = |x|_p\,|y|_p \quad |x-y|_p \leq \max(|x|_p\,,|y|_p) \quad \text{et} \quad |x+y|_p \leq |x|_p + |y|_p\,.}$$

22. Soit d_p l'application

$$d_p : \left\{ \begin{array}{ccc} \mathbb{Q}^2 & \longrightarrow & \mathbb{R}_+ \\ (x,y) & \mapsto & |x-y|_p\,. \end{array} \right.$$

Montrer que pour tout triplet (x,y,z) de nombres rationnels on a l'inégalité suivante

$$d_p(x,z) \leq \max(d_p(x,y), d_p(y,z)).$$

Montrer que d_p est une distance sur $\mathbb{Q}$.
Soit $(x,y,z)\in\mathbb{Q}^3$. On a :

$$\begin{aligned}
d_p(x,z) &= |x-z|_p \\
&= |(x-y)+(z-y)| \\
&\leq \max(|x-y|_p\,, |z-y|_p) \quad \text{d'après}\mathbf{21.} \\
&\leq \max(|x-y|_p\,, |y-z|_p) \quad \text{par parité} \\
&= \max(d_p(x,y), d_p(y,z)),
\end{aligned}$$

ce qui prouve la première relation.
Montrons que d_p est une distance sur $\mathbb{Q}^2$:

— d_p est bien définie sur $\mathbb{Q}^2$ et à valeurs positives,
— d_p est symétrique par parité de la valeur absolue p-adique,
— Soit $(x,y)\in\mathbb{Q}^2$ tel que $x\neq y$. Alors

$$d_p(x,y) = |x-y|_p = \frac{1}{p^{v_p(x-y)}} \neq 0$$

et $d_p(x,x) = |0|_p = 0$ donc d_p vérifie l'axiome de séparation.
— Enfin, pour tout $(x,y,z)\in\mathbb{Q}^3$, on a :

$$d_p(x,z) = |x-z|_p = |x-y+y-z|_p \leq |x-y|_p + |y-z|_p = d_p(x,y) + d_p(y,z)$$

donc d_p vérifie l'inégalité triangulaire.

En conclusion :

$$\boxed{d_p \text{ définit une distance sur } \mathbb{Q}^2.}$$

23. Étudier la convergence de la suite $(p^n)_{n\geq 0}$ dans l'espace métrique $(\mathbb{Q}, d_p)$. Pour tout $n\in\mathbb{N}$, on a :

$$d_p(p^n,0) = |p^n|_p = \frac{1}{p^n} \xrightarrow[n\to+\infty]{} 0$$

donc

$$\boxed{\text{la suite } (p^n)_{n\in\mathbb{N}} \text{ converge vers } 0 \text{ dans } (\mathbb{Q}, d_p).}$$

II. Les entiers p-adiques

II.A. Définition de $\mathbb{Z}_p$

On note $\mathbb{Z}_p$ l'ensemble des suites $(a_n)_{n\geq 0}$ d'entiers naturels qui vérifient :

— **pour tout entier naturel n, on a $a_n \in [\![0, p^{n+1}-1]\!]$,**

— **pour tous les couples d'entiers naturels n et m tels que $m \geq n$, on a $a_m \equiv a_n\ [p^{n+1}]$.**

24. Soit $(a_n)_{n\geq 0}$ une suite d'entiers naturels telle que pour tout $n \in \mathbb{N}$, on a $a_n \in [\![0, p^{n+1}-1]\!]$. Montrer que la suite $(a_n)_{n\geq 0}$ est dans $\mathbb{Z}_p$ si, et seulement si

$$\forall n \in \mathbb{N}, \quad a_{n+1} \equiv a_n\ [p^{n+1}].$$

La condition est évidemment nécessaire car il suffit de prendre $m = n+1$ dans la seconde condition définissant $\mathbb{Z}_p$. Réciproquement, si $(a_n)_{n\geq 0}$ vérifie

$$\forall n \in \mathbb{N}, \quad a_{n+1} \equiv a_n\ [p^{n+1}]$$

alors pour tout $n \in \mathbb{N}$, on a :

$$a_{n+2} \equiv a_{n+1}\ [p^{n+2}] \quad \text{et} \quad a_{n+1} \equiv a_n\ [p^{n+1}]$$

donc

$$p^{n+2} | a_{n+2} - a_{n+1} \quad \text{et} \quad p^{n+1} | a_{n+1} - a_n$$

mais $p^{n+1} | p^{n+2}$ donc

$$p^{n+1} | (a_{n+2} - a_{n+1}) + (a_{n+1} - a_n) = a_{n+2} - a_n$$

et donc $a_{n+2} \equiv a_n\ [p^{n+1}]$.
Par récurrence sur k, on montre ainsi que, pour tout $k \in \mathbb{N}^*$, on a $a_{n+k} \equiv a_n\ [p^{n+1}]$, ce qui prouve que $(a_n)_{n\geq 0} \in \mathbb{Z}_p$.

25. Soit $a = (a_n)_{n\geq 0}$ un élément de $\mathbb{Z}_p$. Étant donné un entier n fixé, on décompose a_{n+1} en la somme $a_{n+1} = \sum_{i=0}^{n+1} u_i p^i$ où les u_i sont des entiers compris entre 0 et $p-1$.

Montrer que a_n se décompose en la somme $\sum_{i=0}^{n} u_i p^i$.

En base p, a_n se décompose sous la forme $a_n = \sum_{i=0}^{n} v_i p^i$ où les v_i sont des entiers compris entre 0 et $p-1$. Puisque la suite (a_n) est dans $\mathbb{Z}_p$, p^{n+1} divise $a_{n+1} - a_n$ pour tout entier naturel n mais

$$a_{n+1} - a_n = u_{n+1} p^{n+1} + \sum_{i=0}^{n} (u_i - v_i) p^i.$$

Or

$$\left| \sum_{i=0}^{n} (u_i - v_i) p^i \right| \leq \sum_{i=0}^{n} |u_i - v_i|\, p^i \leq \sum_{i=0}^{n} (p-1) p^i = p^{n+1} - 1$$

et donc

$$\sum_{i=0}^{n} (u_i - v_i) p^i = 0.$$

Par unicité de la décomposition en base p, on a $u_i = v_i$ pour tout $i \in [\![0, n]\!]$ et donc on a bien :

$$\boxed{a_n = \sum_{i=0}^{n} u_i p^i.}$$

À tout élément $(a_n)_{n\geq 0}$ de $\mathbb{Z}_p$ on associe une unique suite $(u_i)_{i\geq 0}$ d'éléments de $[\![0, p-1]\!]$ telle que pour tout entier n on a l'égalité $a_n = \sum_{i=0}^{n} u_i p^i$.

26. **Soit $a = (a_n)_{n\geq 0}$ un élément de $\mathbb{Z}_p$ dont les termes ne sont pas tous nuls. Montrer qu'il existe un unique entier naturel k vérifiant les relations suivantes :**

— **$v_p(a_n) = +\infty$ si $n < k$,**
— **$v_p(a_n) = k$ si $n \geq k$.**

La suite (a_n) n'étant pas identiquement nulle, on peut considérer :

$$k = \min \{i \in \mathbb{N} \mid a_i \neq 0\}.$$

Alors, pour tout $n \in \mathbb{N}$:

— si $n < k$, alors $a_n = 0$ et donc $v_p(a_n) = +\infty$,
— si $n \geq k$, alors $a_n \equiv \underbrace{a_k}_{\neq 0}\ [p^{k+1}]$ donc p^{k+1} ne divise pas a_n. D'autre part, $p^{k+1}|a_n - a_k$ et donc $p^k|a_n - a_k$ mais $a_k \equiv \underbrace{a_{k-1}}_{=0}\ [p^k]$ donc p^k divise a_k et, par somme, p^k divise a_n. On a donc bien $v_p(a_n) = k$.

Cet entier k est noté $\tilde{v}_p(a)$. Par convention, on pose $\tilde{v}_p(0) = +\infty$ où 0 est la suite de $\mathbb{Z}_p$ dont tous les termes sont nuls.

27. **Soit $x \in \mathbb{Z}$ et $a = (a_n)_{n\geq 0}$ la suite d'entiers telle que, pour tout entier n, le terme a_n est le reste de la division euclidienne de x par p^{n+1}. Montrer que la suite a est un élément de $\mathbb{Z}_p$.**

Pour tout $n \in \mathbb{N}$, on a les divisions euclidiennes :

$$x = p^{n+1} q_n + a_n$$
$$x = p^{n+2} q_{n+1} + a_{n+1}$$

de sorte que $a_n \in [\![0, p^{n+1} - 1]\!]$ et

$$a_{n+1} - a_n = p^{n+2} q_{n+1} - p^{n+1} q_n = p^{n+1}(p q_{n+1} - q_n) \equiv 0\ [p^{n+1}]$$

et donc $a_{n+1} \equiv a_n\ [p^{n+1}]$.

$$\boxed{\text{la suite } (a_n)_{\geq 0} \text{ ainsi construite est dans } \mathbb{Z}_p.}$$

Cette suite sera notée $\theta(x)$ et on notera θ l'application $\theta : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ ainsi définie.

28. **Dans cette question uniquement, fixons $p = 5$. Déterminer les éléments $\theta(7)$ et $\theta(-7)$ de $\mathbb{Z}_5$.**

Pour 7 : On a la division euclidienne de 7 par 5 :

$$7 = 5^1 \times 1 + 2$$

donc $a_0 = 2$. D'autre part, pour tout $n \geq 1$, on a $5^{n+1} \geq 7$ donc la division euclidienne de 7 par 5^{n+1} est :

$$7 = 5^{n+1} \times 0 + 7$$

de sorte que

$$\boxed{\theta(7) = (2, 7, 7, 7, \cdots) \in \mathbb{Z}_5.}$$

Pour -7 : On a les divisions euclidiennes :

$$-7 = 5^1 \times (-2) + 3 \qquad \text{donc } a_0 = 3$$

$$-7 = 5^2 \times (-1) + 18 \qquad \text{donc } a_1 = 18$$
$$-7 = 5^3 \times (-1) + 118 \qquad \text{donc } a_2 = 118$$

et, plus généralement, on observe que :

$$\forall k \geq 1, \quad -7 = 5^{k+1} \times (-1) + \underbrace{(5^{k+1} - 7)}_{\in [\![0, 5^{k+1}-1]\!]}$$

de sorte que $a_k = 5^{k+1} - 7$. Ainsi :

$$\boxed{\theta(-7) = (3, 5^2 - 7, 5^3 - 7, \cdots, 5^k - 7, \cdots) \in \mathbb{Z}_5.}$$

29. Montrer que θ est une application injective. Soient x et y entiers tels que $\theta(x) = \theta(y)$. Alors, pour tout $i \in \mathbb{Z}$, x et y ont le même reste modulo p^{i+1}. Mais alors, x et y ont la même écriture en base p et donc $x = y$.
Ainsi :

$$\boxed{\theta \text{ est injective.}}$$

30. Soit $\alpha = (\alpha_n)_{n\geq 0}$ la suite définie par $\alpha_n = \sum_{i=0}^{n} p^i$ pour tout entier positif n. Vérifier que la suite α est un élément de $\mathbb{Z}_p$. Montrer qu'il n'existe pas d'entier relatif x tel que $\theta(x) = \alpha$.
Pour tout $n \in \mathbb{N}$, α_n est un entier positif et :

$$\alpha_n = \sum_{i=0}^{n} p^i = \frac{p^{n+1} - 1}{p - 1} \leq p^{n+1} - 1$$

D'autre part, $\alpha_{n+1} = p^{n+1} + \alpha_n$ de sorte que $\alpha_{n+1} \equiv \alpha_n\ [p^{n+1}]$. Ainsi, la suite α est bien dans $\mathbb{Z}_p$.
Supposons qu'il existe x entier tel que $\theta(x) = \alpha$. Alors l'écriture en base p de x est $(\cdots, 1, 1, 1)_p$ de sorte que $x = \sum_{i\in\mathbb{N}} p^i = +\infty$, une absurdité.

31. Vérifier que pour tout entier relatif x, on a la relation $\tilde{v}_p(\theta(x)) = v_p(x)$.
Soit $x \in \mathbb{Z}$. On pose $\theta(x) = (a_n)_{n\geq 0} \in \mathbb{Z}_p$.
Notons $k = \tilde{v}_p(\theta(x))$ de sorte que :

$$\begin{cases} v_p(a_n) = +\infty & \text{si} \quad n < k \\ v_p(a_n) = k & \text{si} \quad n \geq k. \end{cases}$$

- Si $n < k$, on a donc $a_n = 0$ et donc $p^{n+1} | x$. En particulier, pour $n = k - 1$, on obtient $p^k | x$.
- Si $n \geq k$, $v_p(a_n) = k$ donc $a_n \neq 0$ et donc p^{n+1} ne divise pas k. En particulier, pour $n = k$, p^{k+1} ne divise pas k.

On a donc bien :

$$\boxed{\forall x \in \mathbb{Z}, \quad \tilde{v}_p(\theta(x)) = v_p(x).}$$

Les deux questions précédentes montrent que θ est une application injective de $\mathbb{Z}$ dans $\mathbb{Z}_p$ et que l'application $\tilde{v}_p$ prolonge l'application v_p à tous les éléments de $\mathbb{Z}_p$ via cette injection. Dans la suite du problème, l'application $\tilde{v}_p$ sera notée v_p.

II.B. Structure d'anneau

32. Soient $a = (a_n)_{n\geq 0}$ et $b = (b_n)_{n\geq 0}$ deux éléments de $\mathbb{Z}_p$. Pour tout entier n, on note c_n le reste de la division euclidienne de $a_n + b_n$ par p^{n+1}. Montrer que la suite $c = (c_n)_{n\geq 0}$ est un élément de $\mathbb{Z}_p$.

Pour tout $n \in \mathbb{N}$, on a $c_n \in [\![0, p^{n+1} - 1]\!]$ car c_n est un reste de division euclidienne par p^{n+1}. D'autre part, $a_{n+1} \equiv a_n\ [p^{n+1}]$, $b_{n+1} \equiv b_n\ [p^{n+1}]$ donc

$$\begin{aligned} c_{n+1} &\equiv a_{n+1} + b_{n+1}\ [p^{n+1}] \\ &\equiv a_n + b_n\ [p^{n+1}] \\ &\equiv c_n\ [p^{n+1}] \end{aligned}$$

donc on a bien :

$$\boxed{c \in \mathbb{Z}_p.}$$

On note cette suite $a + b$ ce qui munit $\mathbb{Z}_p$ d'une loi de composition interne notée $+$.

33. Déterminer un élément neutre, que l'on notera 0, pour la loi $+$. Étant donné un élément $a = (a_n)_{n\geq 0}$ de $\mathbb{Z}_p$, expliciter un élément $b = (b_n)_{n\geq 0}$ de $\mathbb{Z}_p$ tel que $a + b = 0$.
Montrer que $(\mathbb{Z}_p, +)$ est un groupe commutatif.
Posons $z = (z_n)_{n\geq 0}$ où, pour tout $n \in \mathbb{N}$, $z_n = 0$. Alors, pour tout $n \in \mathbb{N}$, on a $z_n \in [\![0, p^{n+1} - 1]\!]$ et $z_{n+1} = 0 \equiv 0\ [p^{n+1}] \equiv z_n\ [p^{n+1}]$ donc $z \in \mathbb{Z}_p$. On note 0 cette suite de $\mathbb{Z}_p$, neutre pour la loi $+$.
Soit $a = (a_n)_{n\geq 0}$. Pour tout $n \in \mathbb{N}$, on pose :

$$b_n = \begin{cases} 0 & \text{si} \quad a_n = 0 \\ p^{n+1} - a_n & \text{si} \quad a_n \neq 0 \end{cases}$$

alors $b_n \in [\![0, p^{n+1} - 1]\!]$ et

$$b_{n+1} \equiv -a_{n+1}\ [p^{n+1}] \equiv -a_n\ [p^{n+1}] \equiv b_n\ [p^{n+1}]$$

de sorte que $b = (b_n)_{n\geq 0} \in \mathbb{Z}_p$ et $a + b = 0$.
On a déjà établi que $+$ définit une loi de composition interne sur $\mathbb{Z}_p$ admettant un élément neutre et pour laquelle tout élément est symétrisable. Il reste à observer que la loi $+$ est associative et commutative, ce qui suit des propriétés de l'addition dans $\mathbb{Z}$.
En conclusion :

$$\boxed{(\mathbb{Z}_p, +) \text{ est un groupe commutatif.}}$$

34. Soient $a = (a_n)_{n\geq 0}$ et $b = (b_n)_{n\geq 0}$ deux éléments de $\mathbb{Z}_p$. Pour tout entier n, on note d_n le reste de la division euclidienne de $a_n b_n$ par p^{n+1}.
On admet que la suite $(d_n)_{n\geq 0}$ ainsi définie est dans $\mathbb{Z}_p$ et elle est notée $d = a \cdot b$. On admet également que $\cdot$ est une loi de composition interne qui permet de munir $(\mathbb{Z}_p, +)$ d'une structure d'anneau commutatif.
Déterminer l'élément neutre de la multiplication dans $(\mathbb{Z}_p, \cdot)$.
On pose $e = (e_n)_{n\geq 0}$ où, pour tout $n \in \mathbb{N}$, $e_n = 1$.
On a alors, pour tout $n \in \mathbb{N}$, $e_n \in [\![0, p^{n+1} - 1]\!]$ et $e_{n+1} = e_n$ donc $e_{n+1} \equiv e_n\ [p^{n+1}]$ de sorte que $e \in \mathbb{Z}_p$. Enfin, pour tout $a = (a_n)_{n\geq 0} \in \mathbb{Z}_p$, on a $a \cdot e = (a_n)_{n\geq 0}$ donc :

$$\boxed{e = (1, 1, \cdots) \text{ est neutre pour la multiplication.}}$$

35. Montrer que $(\mathbb{Z}_p, +)$ est un anneau intègre.
Note : Ici, il est clair qu'un argument direct m'a échappé vu que je passe par des résultats qui se retrouvent aux questions 37 à 39. Ca ne crée pas de boucle logique car on les établit dans cette réponse, mais il est clair que le sujet nous guide vers un autre chemin.
Soit $a = (a_n)_{n\geq 0} \in \mathbb{Z}_p$. On commence par observer que $a \in (\mathbb{Z}_p)^*$ si, et seulement si, $a_0 \neq 0$. Évidemment, si $a_0 = 0$, a n'est pas inversible car il n'existe pas d'entier b_0 tel que $a_0 b_0 \equiv 1\ [p]$. Réciproquement, supposons $a_0 = 0$. On construit alors les termes de $b = (b_n)_{n\geq 0}$ par récurrence.

Puisque p est premier et a_0 est non nul dans $[\![0, p-1]\!]$, a_0 est premier avec p et donc, il existe (u, v) tels que $a_0u + pv = 1$. En prenant b_0 pour b_0 le reste de la division euclidienne de u par p, on a bien $b_0 \in [\![0, p-1]\!]$ tel que $a_0b_0 \equiv 1\ [p]$.
Supposons maintenant que $(b_0, \cdots, b_{n-1})$ sont construits, avec n un entier naturel non nul. Alors pour tout $k \in [\![0, n-1]\!]$, on a $a_kb_k \equiv 1\ [p^{k+1}]$ et, comme $a \in \mathbb{Z}_p$, on a :

$$a_n \equiv \underbrace{a_0}_{\neq 0}\ [p]$$

donc $p \wedge a_n = 1$ et donc $a_n \wedge p^{n+1} = 1$. Alors, comme ci-dessus, il existe $b_n \in [\![0, p^{n+1}-1]\!]$ tel que $a_nb_n \equiv 1\ [p^{n+1}]$.
On a alors :

$$\underbrace{a_n}_{\equiv a_{n-1}\ [p^n]} b_n \equiv a_{n-1}b_{n-1}\ [p^n]$$

et a_n est premier avec p^n donc inversible modulo p^n et donc

$$b_n \equiv b_{n-1}\ [p^n]$$

de sorte que $b \in \mathbb{Z}_p$.
Alors, pour tout a non nul dans $\mathbb{Z}_p$, on considère l'entier m minimal tel que $a_m \neq 0$. Alors $a_{m-1} \equiv 0\ [p^m]$ et donc, pour tout $k \geq m$, $a_k \equiv 0\ [p^m]$.
On pose alors pour tout $k \geq m$, en posant $k = m + \ell$, on pose

$$u_\ell = \frac{a_{m+\ell}}{p^m}$$

de sorte que $u_{\ell+1} \equiv u_\ell\ [p^{\ell+1}]$ et $u_0 \neq 0$. Ainsi, u est inversible dans $\mathbb{Z}_p$ et on a $a = \theta(p^m)u$.
Considérons alors $b \in \mathbb{Z}_p$ non nul. On peut l'écrire $b = \theta(p^{m'})u'$ avec m' entier et u' non nul. L'application θ est multiplicative (rédaction détaillée à la question 37 ci-après), on a :

$$a \cdot b = \theta(p^{m+m'})uu' \neq 0$$

et donc, après un long détour (dont nous allons bénéficier ensuite), on a bien montré :

$$\boxed{(\mathbb{Z}_p, +, \cdot) \text{ est intègre.}}$$

De manière utile pour la suite, on remarque que quand on a écrit $a = \theta(p^m)u$, on a $m = v_p(a)$ de sorte que tout élément non nul s'écrit $a = \theta(p^{v_p(a)})u$, avec u inversible et donc de valuation p-adique nulle.

36. Montrer que si $a = (a_n)_{n\geq 0}$ et $b = (b_n)_{n\geq 0}$ sont deux éléments de $\mathbb{Z}_p$ non nuls, alors on a les relations

$$v_p(a \cdot b) = v_p(a) + v_p(b) \quad \textbf{et} \quad v_p(a - b) \geq \min(v_p(a), v_p(b)).$$

Si a et b sont non nuls, il suit de la dernière partie de la réponse précédente que l'on peut écrire

$$a = \theta(p^{v_p(a)})u \quad \text{et} \quad b = \theta(p^{v_p(b)})v$$

avec u et v inversibles dans $\mathbb{Z}_p$.
Alors $a \cdot b = \theta(p^{v_p(a \cdot b)})w$, avec w inversible et

$$a \cdot b = \theta(p^{v_p(a)})\theta(p^{v_p(b)})v = \theta(p^{v_p(a)+v_p(b)})uv.$$

Les valuations de u, v et w étant nulles, on a bien :

$$\boxed{v_p(a \cdot b) = v_p(a) + v_p(b).}$$

D'autre part,
$$v_p(a-b) = \min\left\{k \in \mathbb{N} \,\middle|\, a_k - b_k \not\equiv 0\ [p^{k+1}]\right\}$$
mais, pour tout $k < \min(v_p(a), v_p(b))$, on a $a_k \equiv 0\ [p^{k+1}]$ et $b_k \equiv 0\ [p^{k+1}]$ donc $a_k - b_k \equiv 0\ [p^{k+1}]$ de sorte que :
$$\boxed{v_p(a-b) \geq \min(v_p(a), v_p(b)).}$$

37. Montrer que l'application θ définie dans la question 27. est un morphisme injectif d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}_p$.

On sait déjà que $\theta : \mathbb{Z} \longrightarrow \mathbb{Z}^p$ est injective.
Soit $(x, y) \in \mathbb{Z}^2$. On pose $\theta(x) = (a_n)_{n\geq 0}$ et $\theta(y) = (b_n)_{n\geq 0}$. Alors, pour tout $n \in \mathbb{N}$, on a les divisions euclidiennes :
$$x = q_a p^{n+1} + a_n \quad \text{et} \quad x = q_b p^{n+1} + b_n$$
donc
$$x + y = (q_a + q_b)p^{n+1} + (a_n + b_n) \quad \text{et} \quad xy = (q_a q_b p^{n+1} + q_a b_n + q_b a_n)p^{n+1} + a_n b_n$$
donc
$$x + y \equiv a_n + b_n\ [p^{n+1}] \quad \text{et} \quad xy \equiv a_n b_n\ [p^{n+1}]$$
de sorte que
$$\theta(x+y) = \theta(x) + \theta(y) \quad \text{et} \quad \theta(xy) = \theta(x)\theta(y).$$
Enfin, pour tout $n \in \mathbb{N}$, on a :
$$1 = 0 \times p^{n+1} + 1$$
donc $\theta(1) = (1, 1, \cdots) = e$.
En conclusion :
$$\boxed{\theta : \mathbb{Z} \longrightarrow \mathbb{Z}_p \text{ est un morphisme d'anneaux injectif.}}$$

À l'aide de ce morphisme injectif, on identifie $\mathbb{Z}$ au sous-anneau $\theta(\mathbb{Z})$ de $\mathbb{Z}_p$.

38. Soit $a = (a_n)_{n\geq 0}$ un élément de $\mathbb{Z}_p$. Montrer que a est inversible dans $\mathbb{Z}_p$ si le terme a_0 est non nul.

Fait à la question 35.

39. Soit $a = (a_n)_{n\geq 0}$ un élément de $\mathbb{Z}_p$. Montrer qu'étant donné un entier k, on a $v_p(a) \geq k$ si et seulement s'il existe une suite $b = (b_n)_{n\geq 0}$ de $\mathbb{Z}_p$ telle que $a = \theta(p^k) \cdot b$.

Fait à la question 35.

40. Déterminer les idéaux de $\mathbb{Z}_p$.

Soit I un idéal non nul de $\mathbb{Z}_p$. S'il existe $a \in I$ tel que $a_0 \neq 0$, alors $a \in \mathbb{Z}_p^*$ et donc $I = \mathbb{Z}_p$. Supposons donc que I ne contient aucun élément inversible et posons
$$k = \min_{a\in I} v_p(a)$$
qui est donc un entier supérieur ou égal à 1. Pour tout $a \in I$, il suit de la question **39.** qu'il existe u inversible tel que $a = \theta(p^{v_p(a)})u$ et donc $a \in \theta(p^k) \cdot \theta(p^{v_p(a)-k})u \in \theta(p^k) \cdot \mathbb{Z}_p$. On a donc $I \subset \theta(p^k)\mathbb{Z}_p$.
Réciproquement, considérons $a \in I$ tel que $v_p(a) = k$ de sorte que $a = \theta(p^k)u$, avec u inversible dans $\mathbb{Z}_p$. Alors
$$\forall b \in \mathbb{Z}_p, \quad \theta(p^k)b = \underbrace{\theta(p^k)u}_{=a\in I} \cdot \underbrace{u^{-1}b}_{\in\mathbb{Z}_p} \in I.$$
Ainsi, $I = \theta(p^k) \cdot \mathbb{Z}_p$.
En outre, pour tout $k \in \mathbb{N}^*$, $\theta(p^k) \cdot \mathbb{Z}_p$ est un idéal (principal).
En conclusion :
$$\boxed{\text{les idéaux non triviaux de } \mathbb{Z}_p \text{ sont les } \theta(p^k) \cdot \mathbb{Z}_p.}$$

On a ainsi démontré que $\mathbb{Z}_p$ est un anneau principal.

Soit $E = \mathbb{Z}_p \times (\mathbb{Z}_p \setminus \{0\})$ et $\mathcal{R}$ la relation d'équivalence définie sur E par :

$$(a, b)\,\mathcal{R}\,(c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

Le corps des fractions de l'anneau intègre $\mathbb{Z}_p$ est l'ensemble quotient, noté $\mathbb{Q}_p$, des classes d'équivalence notées $\overline{(a, b)}$ de couples d'éléments de $\mathbb{Z}_p \times (\mathbb{Z}_p \setminus \{0\})$ pour la relation d'équivalence $\mathcal{R}$. Il est muni des lois de composition internes induites par celles définies sur $\mathbb{Z}_p$, c'est un corps commutatif. En associant à un élément a de $\mathbb{Z}_p$ la classe de $(a, 1)$ dans $\mathbb{Q}_p$, on identifie $\mathbb{Z}_p$ à un sous-anneau de $\mathbb{Q}_p$.

41. Montrer que l'application

$$\theta : \begin{cases} \mathbb{Q} & \longrightarrow & \mathbb{Q}_p \\ \dfrac{a}{b} & \mapsto & \overline{(\theta(a), \theta(b))} \end{cases}$$

est bien définie. Montrer ensuite qu'il s'agit d'un morphisme injectif de corps.

Soient $(a, b), (c, d)$ des éléments de E. On a :

$$\begin{aligned} \frac{a}{b} = \frac{c}{d} &\Rightarrow ad = bc \\ &\Rightarrow \theta(ad) = \theta(bc) \\ &\Rightarrow \theta(a)\theta(d) = \theta(b)\theta(c) \quad \text{d'après } \mathbf{37.} \\ &\Rightarrow (\theta(a), \theta(b))\,\mathcal{R}\,(\theta(c), \theta(d)) \\ &\Rightarrow \overline{(\theta(a), \theta(b))} = \overline{(\theta(c), \theta(d))}. \end{aligned}$$

θ étant un morphisme d'anneaux $\mathbb{Z} \longrightarrow \mathbb{Z}_p$ d'après **37.**, compatible avec le passage aux fractions d'après la discussion précédente, il induit un morphisme d'anneaux entre les corps de fractions correspondants, et donc un morphisme d'anneaux $\mathbb{Q} \longrightarrow \mathbb{Q}_p$.

$\mathbb{Q}$ étant un corps, ce morphisme est injectif d'après la question **1.e.**

À l'aide de ce morphisme, on identifie $\mathbb{Q}$ au sous-corps $\theta(\mathbb{Q})$ de $\mathbb{Q}_p$

42. Montrer que, pour $((a, b), (c, d)) \in E^2$ tels que $(a, b)\,\mathcal{R}\,(c, d)$, on a $v_p(a) - v_p(b) = v_p(c) - v_p(d)$. Soit $((a, b), (c, d)) \in E^2$. On a :

$$\begin{aligned} (a, b)\,\mathcal{R}\,(c, d) &\Rightarrow ad = bc \\ &\Rightarrow v_p(ad) = v_p(bc) \\ &\Rightarrow v_p(a) + v_p(d) = v_p(b) + v_p(c) \quad \text{d'après } \mathbf{36.} \\ &\Rightarrow v_p(a) - v_p(b) = +v_p(c) - v_p(d). \end{aligned}$$

Cette valeur commune est appelée valuation p-adique de la classe de (a, b) dans $\mathbb{Q}_p$. On la note $v_p((a, b))$.

43. Soit $x \in \mathbb{Q}_p$. Montrer que $x \in \mathbb{Z}_p$ si et seulement si $v_p(x) \geq 0$.

Si $x \in \mathbb{Z}_p$, on a $v_p(x) \geq 0$ par définition de la valuation p-adique d'un entier.

Réciproquement, soit $x \in \mathbb{Q}_p$. On pose $x = \overline{(\theta(a), \theta(b))}$. On a alors :

$$v_p(x) = v_p(a) - v_p(b).$$

Ainsi, si $v_p(x) \geq 0$, on a $v_p(a) \geq v_p(b)$. Posons D'après la question **39.**, on peut écrire $a = \theta(p^{v_p(a)})a'$ et $b = \theta(p^{v_p(b)})b'$ avec $v_p(a') = v_p(b') = 0$. Alors

$$\overline{(\theta(a), \theta(b))} = \overline{(\theta(p^{v_p(a)})a', \theta(p^{v_p(b)})b')} = \overline{(\theta(p^{v_p(a)-v_p(b)})a', b')} = \overline{(\theta(p^{v_p(a)-v_p(b)})a'(b')^{-1}, 1)} \in \mathbb{Z}_p.$$

On admet que la valuation p-adique sur $\mathbb{Q}_p$ vérifie les propriétés de la valuation dans $\mathbb{Z}$ démontrées dans la partie I. Cela permet de définie, comme dans I.D., la valeur absolue p-adique et la distance p-adique notée d_p sur $\mathbb{Q}_p$.

On se place désormais dans l'espace métrique $(\mathbb{Q}_p, d_p)$. On admettra que les opérations algébriques sur les limites des suites dans cet espace sont valides.

II.C. Topologie dans $\mathbb{Q}_p$

44. Soit $a = (a_n)_{n\geq 0}$ un élément de $\mathbb{Z}_p$. Comme dans la question 25., on lui associe une suite $u = (u_n)_{n\geq 0}$ qui est constituée d'entiers compris entre 0 et $p-1$, telle que, pour tout entier n, on a $a_n = \sum_{i=0}^{n} u_i p^i$.

Montrer que pour tout entier k supérieur ou égal à $n+1$ on a l'inégalité $v_p(a_{-}a_{k+1}) \geq n+1$. En déduire que la suite $(\theta(a_n))_{n\geq 0}$ converge vers a dans $\mathbb{Z}_p$.

Soit $n \in \mathbb{N}$. Soit $k \geq n+1$. On a

$$a_k - a_{n+1} = \sum_{i=0}^{k} u_i p^i - \sum_{i=0}^{n+1} u_i p^i = \begin{cases} \displaystyle\sum_{i=n+2}^{k} u_i p^i & \text{si} \quad k > n+1 \\ 0 & \text{si} \quad k = n+1 \end{cases}$$

donc

$$v_p(a_k - a_{n+1}) = \begin{cases} n+2 & \text{si} \quad k > n+1 \\ +\infty & \text{si} \quad k = n+1. \end{cases}$$

On a donc bien :

$$\boxed{\forall k \geq n+1, \quad v_p(a_k - a_{n+1}) \geq n+1.}$$

On a

$$|\theta(a_n) - a| = \frac{1}{p^{v_p(\theta(a_n)-a}}$$

mais, en passant à la limite dans l'inégalité précédente, on a $v_p(\theta(a_n) - a) \geq n+1$ donc

$$|\theta(a_n) - a| \leq \frac{1}{p^{n+1}} \xrightarrow[n\to+\infty]{} 0$$

de sorte que

$$\boxed{\theta(a_n) \xrightarrow[n\to+\infty]{} a.}$$

On écrira alors $a = \sum_{i=0}^{+\infty} u_i p^i$.

45. Montrer que $\theta(\mathbb{Z})$ est dense dans $\mathbb{Z}_p$.

Soit $a \in \mathbb{Z}_p$ que l'on écrit $a = \sum_{i=0}^{+\infty} u_i p^i$. On a alors :

$$a = \sum_{i=0}^{+\infty} u_i p^i = \lim_{n\to+\infty} \sum_{i=0}^{n} u_i p^i = \lim_{n\to+\infty} \underbrace{\theta(a_n)}_{\in\theta(\mathbb{Z})}$$

donc

$$\boxed{\overline{\theta(\mathbb{Z})} = \mathbb{Z}_p.}$$

46. Soit a un élément de $\mathbb{Z}_p$ que l'on écrit $a = \sum_{i=0}^{+\infty} u_i p^i$. Soit ℓ un entier. Montrer que $v_p(a) \geq \ell$ si, et seulement si, pour tout $i \in [\![0, \ell-1]\!]$, on a $u_i = 0$.

Par l'absurde, supposons qu'il existe $i_0 [\![0, \ell - 1]\!]$ tel que $u_{i_0} \neq 0$. Puisque $\theta(\mathbb{Z})$ est dense dans $\mathbb{Z}_p$, pour tout $\epsilon > 0$, avec les notations précédentes, il existe un entier N à partir duquel $|a - \theta(a_n)|_p \leq \epsilon$ mais $|\theta(a_n)| = \dfrac{1}{p^{i_0}} > \dfrac{1}{p^\ell}$ donc, avec $\epsilon = \dfrac{1}{3}\left|\dfrac{1}{p^\ell} - \dfrac{1}{p^{i_0}}\right|$, on obtient une contradiction.

Réciproquement, si $u_i = 0$ pour tout $i \in [\![0, \ell - 1]\!]$, alors, pour tout $N \in \mathbb{N}$, on a $|\theta(a_N)|_p \leq \dfrac{1}{p^\ell}$ et donc, par passage à la limite, $|a|_p \leq \dfrac{1}{p^\ell}$ et donc $v_p(a) \geq \ell$.

47. Soit $(a^{(k)})_{k\geq 0}$ une suite de Cauchy de $\mathbb{Z}_p$. D'après la question 44., on a :

$$\forall k \geq 0, \quad a^{(k)} = \sum_{i=0}^{+\infty} u_i^{(k)} p^i$$

où les termes $u_i^{(k)}$ sont des entiers compris entre 0 et $p - 1$.

(a) Montrer que pour tout entier positif i, la suite $(u_i^{(k)})_{k\geq 0}$ est stationnaire.

Soit $i \in \mathbb{N}$. Pour tout $\epsilon > 0$, il existe un entier n tel que, pour tout $k \geq 0$, on a $\left|a^{(n+k)} - a^{(n)}\right|_p \leq \epsilon$ et donc $v_p(a^{(n+k)} - a^{(n)}) \geq -\log_p(\epsilon)$. Puisque $-\log_p(\epsilon) \xrightarrow[\epsilon\to 0]{} +\infty$, on peut choisir ϵ tel que $-\log_p(\epsilon) > i$ de sorte que :

$$\forall k \geq 0, \quad \left|u_i^{(n+k)} - u_i^{(n)}\right| = 0$$

et donc $(u_i^{(k)})_{k\geq 0}$ est stationnaire.

(b) En déduire que la suite $(a^{(k)})_{k\geq 0}$ converge dans $\mathbb{Z}_p$.

Pour tout $i \in \mathbb{N}$, on pose $u_i = \lim\limits_{n\to+\infty} u_i^{(n)}$ et, pour tout $n \in \mathbb{N}$, on pose $a_n = \sum\limits_{i=0}^{n} u_i p^i$ de sorte que

$$\theta(a_n) \xrightarrow[n\to+\infty]{} a = \sum_{i=0}^{+\infty} u_i p^i.$$

Montrons que $a^{(k)} \xrightarrow[k\to+\infty]{} a$. Soit $\epsilon > 0$ et ℓ entier tel que $\dfrac{1}{p^\ell} \leq \epsilon$. D'après la question **47.a.**, il existe un entier n_0 tel que pour tout $i \in [\![0, \ell - 1]\!]$ et pour tout $k \geq n_0$, on a $u_i^{(k)} = u_i$. Mais alors, pour tout $k \geq n_0$, on a :

$$\left|a - a^{(k)}\right|_p = |a - \theta(a_k)|_p \leq \frac{1}{p^\ell} \leq \epsilon.$$

Autrement dit $a^{(k)} \xrightarrow[k\to+\infty]{} a$.
En conclusion, on a montré :

$$\boxed{\mathbb{Z}_p \text{ est complet.}}$$

On vient de montrer que $\mathbb{Z}_p$ est complet et on admet que $\mathbb{Q}_p$ est complet.

48. Soit $(x_k)_{k\geq 0}$ une suite d'éléments de $\mathbb{Q}_p$.

Pour $n \in \mathbb{N}$, on pose $S_n = \sum\limits_{k=0}^{n} x_k$.

Montrer que la suite $(S_n)_{n\geq 0}$ converge dans $\mathbb{Q}_p$ si et seulement si la suite réelle $(|x_k|)_{k\geq 0}$ converge vers 0 (c'est-à-dire si et seulement si la suite $(x_k)_{k\geq 0}$ converge vers 0 dans $\mathbb{Q}_p$).

Si $(S_n)_{n\geq 0}$ admet une limite S dans $\mathbb{Q}_p$, alors pour tout $n \in \mathbb{N}^*$, on a :

$$x_n = S_n - S_{n-1} \xrightarrow[n\to+\infty]{} S - S = 0.$$

Réciproquement, si $|x_n|_p \xrightarrow[n\to+\infty]{} 0$ alors pour tout $\epsilon > 0$, il existe $n_0 \in \mathbb{N}$ tel que pour $n \geq n_0$, on $|x_n| \leq \epsilon$, c'est-à-dire $v_p(x_n) \geq -\log_p(\epsilon)$. Mais alors, pour tout $k > n_0$, on a

$$\left|S_{n_0+k} - S_{n_0}\right| = \left|\sum_{k=n_0+1}^{n_0+k} x_k\right|_p \underset{\mathbf{21.}}{\leq} \max_{k\geq n_0+1} |x_k|_p \leq \epsilon$$

donc $(S_n)_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\mathbb{Q}_p$, qui est complet, donc elle converge.
Ainsi,

$$\boxed{(S_n)_{n\in\mathbb{N}} \text{ converge} \iff |x_n|_p \xrightarrow[n\to+\infty]{} 0.}$$

Par conséquent, dans $\mathbb{Q}_p$, une série est convergente si et seulement si ton terme général tend vers 0.

III. Termes nuls d'une suite récurrente linéaire

Soient d un entier naturel non nul et $a = (a_0, \ldots, a_{d-1}) \in \mathbb{Z}^d$ tel que $a_0 \neq 0$.
On s'intéresse à l'ensemble $\mathcal{R}_a$ des suites $u = (u_n)_{n\geq 0}$ définies par $(u_0, \ldots, u_{d-1}) \in \mathbb{Z}^d$ vérifiant la relation de récurrence :

$$\forall n \in \mathbb{N}, u_{n+d} = a_0 u_n + a_1 u_{n+1} + \cdots + a_{d-1} u_{n+d-1}.$$

Pour $u \in \mathcal{R}_a$, on notera

$$Z(u) = \{n \in \mathbb{N} \mid u_n = 0\}.$$

Étant donnés une suite u de $\mathcal{R}_a$ et un entier positif n, on pose $U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix}$.

49. Déterminer une matrice A de $\mathcal{M}_d(\mathbb{Z})$ (indépendante de u) telle que, pour tout entier positif n, on ait $U_n = A^n U_0$. En déduire qu'il existe $X \in \mathcal{M}_{d,1}(\mathbb{Z})$ tel que, pour tout $n \in \mathbb{N}$, $u_n = X^T A^n U_0$.

On considère la matrice :

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & \cdots & a_{d-1} \end{pmatrix}$$

de sorte que, pour tout $n \in \mathbb{N}$, on a :

$$U_{n+1} = AU_n$$

et donc

$$U_n = A^n U_0.$$

Puisque u_n est sur la première coordonnées de U_n, il suffit d'effectuer le produit scalaire avec le premier vecteur de la base canonique pour obtenir sa valeur ; on pose donc $X = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ et on a bien :

$$\boxed{\forall n \in \mathbb{N}, \quad u_n = X^T A^n U_0.}$$

50. Montrer que la matrice A est inversible.

Il faut comprendre que la matrice, définie dans $\mathcal{M}_d(\mathbb{Z})$, est ici vue comme une matrice de $\mathcal{M}_d(\mathbb{R})$. L'énoncé n'est pas très précis sur ce point mais si on se réfère au préambule et au programme du concours qui se restreint aux matrices à coefficients dans un corps, il n'y a pas vraiment de doute possible.

La matrice A est la matrice compagnon du polynôme

$$P(X) = X^d - a_{d-1}X^{d-1} - \cdots - a_1 X - a_0$$

donc

$$\chi_A = P$$

de sorte que

$$\det(A) = \chi(A) = 0 = P(0) = -a_0 \neq 0.$$

Ainsi, on a bien :

$$\boxed{A \in \mathrm{GL}_n(\mathbb{R}).}$$

51. On note $\overline{A}$ la matrice de $\mathcal{M}_d(\mathbb{Z}/p\mathbb{Z})$ obtenue à partir de A en réduisant chacun de ses coefficients modulo p. Montrer que l'on peut choisir un nombre premier impair p tel que la matrice $\overline{A}$ soit dans $\mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z})$.

La projection canonique $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ étant un morphisme d'anneaux et le déterminant étant polynômial en les coefficients de la matrice, on a

$$\det(\overline{A}) = \overline{\det(A)} = -\overline{a_0}$$

mais a_0 admet un nombre fini de diviseurs premiers alors qu'il existe une infinité de nombres premiers impairs. Il existe donc p premier impair tel que p ne divise pas a_0 et alors $\det(\overline{A}) \neq 0$ de sorte que $\overline{A}$ est inversible dans $\mathcal{M}_d(\mathbb{Z}/p\mathbb{Z})$.

On fixe désormais un tel p jusqu'à la fin de la partie III.

52. En déduire qu'il existe un entier strictement positif k et une matrice B de $\mathcal{M}_d(\mathbb{Z})$ tels que $A^k = I_d + pB$.

$\mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z})$ est un groupe fini donc $\overline{A}$ est d'ordre fini dans ce groupe. Ainsi, il existe $k \geq 1$ tel que $\overline{A}^k = \overline{I_d}$ mais $\overline{A}^k = \overline{A^k}$. Autrement dit,

$$\boxed{\exists k \in \mathbb{N}^*,\ \exists B \in \mathcal{M}_d(\mathbb{Z}),\quad A^k = I_d + pB.}$$

53. Soit $(f_j)_{j\geq 0}$ une suite de fonctions de $\mathbb{Z}$ dans $\mathbb{Z}$. Montrer que, pour tout entier n et pour tout entier j, la suite $\left(p^j \dfrac{f_j(n)}{j!}\right)_{n\geq 0}$ appartient à $\mathbb{Z}_p$.

Là, je dois avouer que je ne comprends pas la question : n est fixé mais varie dans la suite, et toutes mes tentatives de correction mènent à des impasses. Cela vient probablement de moi mais quoiqu'il en soit, je passe mon tour pour la fin de cette partie.

54. Montrer que, pour tout entier naturel n, la série $S(n) = \sum_j p^j \dfrac{f_j(n)}{j!}$ converge dans $\mathbb{Q}_p$, puis qu'elle converge dans $\mathbb{Z}_p$.

En suspens.

On admet que si $S(n)$ s'annule pour une infinité de valeurs de n, alors $S(n)$ est nulle sur tout entier n dans $\mathbb{N}$.

55. Soient un entier k et une matrice B de $\mathcal{M}_d(\mathbb{Z})$ tels que l'on ait $A^k = I_d + pB$. Montrer que, si u est une suite appartenant à $\mathcal{R}_a$ et r est un entier compris entre 0 et $k-1$, alors l'ensemble

$$Z_r(u) = \{n \in \mathbb{N} \mid u_{kn+r} = 0\}$$

est soit fini, soit égal à $\mathbb{N}$.

En suspens.

IV. Exponentielle p-adique et application

IV.A. Définition de l'exponentielle

56. Soit x un élément de $\mathbb{Q}_p$. Montrer que, si $v_p(x) > \dfrac{1}{p-1}$, alors la série $\sum_{n \geq 0} \dfrac{x^n}{n!}$ converge.

On a, pour tout $n \in \mathbb{N}$:

$$\begin{aligned} v_p\left(\frac{x^n}{n!}\right) &= v_p(x^n) - v_p(n!) \\ &\geq n v_p(x) - \frac{n}{p-1} \quad \text{(d'après } \mathbf{16.}\text{)} \\ &\geq n\left(\underbrace{v_p(x) - \frac{1}{p-1}}_{>0}\right) \xrightarrow[n \to +\infty]{} +\infty \end{aligned}$$

donc

$$\left|\frac{x^n}{n!}\right|_p = \frac{1}{p^{v_p\left(\frac{x^n}{n!}\right)}} \xrightarrow[n \to +\infty]{} 0$$

et donc, d'après **48.**

$$\boxed{\sum_{n \geq 0} \frac{x^n}{n!} \text{ converge.}}$$

On note alors $e_p(x) = \displaystyle\sum_{n=0}^{+\infty} \frac{x^n}{n!}$ sa somme qui est appelée exponentielle p-adique de x.

57. Montrer que, si x et y sont deux éléments de $\mathbb{Q}_p$ tels que $v_p(x) > \dfrac{1}{p-1}$ et $v_p(y) > \dfrac{1}{p-1}$, alors $e_p(x+y)$ est défini et vérifie la relation $e_p(x+y) = e_p(x)e_p(y)$.

On a $v_p(x+y) \geq \min(v_p(x), v_p(y)) > \dfrac{1}{p-1}$ donc $e_p(x+y)$ existe et, par convergence absolue établie à la question précédente, on a :

$$\begin{aligned} e_p(x)e_p(y) &= \left(\sum_{n=0}^{+\infty} \frac{x^n}{n!}\right)\left(\sum_{m=0}^{+\infty} \frac{x^m}{m!}\right) \\ &= \sum_{N=0}^{+\infty}\left(\sum_{m+n=N} \frac{1}{n!m!} x^n y^m\right) \\ &= \sum_{N=0}^{+\infty} \frac{1}{N!}\left(\sum_{n=0}^{N} \frac{N}{n!(N-n)!} x^n y^{N-n}\right) \\ &= \sum_{N=0}^{+\infty} \frac{1}{N!}\left(\sum_{n=0}^{N} \binom{N}{n} x^n y^{N-n}\right) \\ &= \sum_{N=0}^{+\infty} \frac{(x+y)^N}{N!} \\ &= e_p(x+y). \end{aligned}$$

On a donc bien :

$$\boxed{e_p(x+y) = e_p(x)e_p(y).}$$

58. Soit t un élément de $\mathbb{Q}_p$ tel que $|t|_p < 1$. Montrer que la série $\sum_{n\geq 1}(-1)^{n+1}\dfrac{t^n}{n!}$ converge. On note $\ell_p(1+t)$ sa somme.

On a
$$v_p\left((-1)^{n+1}\frac{t^n}{n!}\right) = v_p((-1)^{n+1}) + v_p(t^n) - v_p(n) = nv_p(t) - v_p(n)$$
mais, pour tout entier n, on a
$$v_p(n) \leq \log_p(n)$$
et $|t|_p < 1$ donc $v_p(t) > 1$ de sorte que $nv_p(t) > n$. Ainsi,
$$v_p\left((-1)^{n+1}\frac{t^n}{n!}\right) \geq n - \log_p(n) \xrightarrow[n\to+\infty]{} +\infty$$
et donc
$$\left|(-1)^{n+1}\frac{t^n}{n!}\right|_p \xrightarrow[n\to+\infty]{} 0.$$
Il suit alors de **48** que
$$\boxed{\sum_{n\geq 1}(-1)^{n+1}\frac{t^n}{n!} \text{ converge.}}$$

IV.B. Inversibles de $\mathbb{Z}/p^n\mathbb{Z}$.

Cette dernière partie a l'air sympa mais j'ai déjà passé trop de temps sur ce sujet. To be continued ?