ISM MP, Mathématiques
Année 2025/2026

Feuille d'exercices n°85

Exercice 1 (*)

Résoudre :

1. $5x \equiv 3\ [7]$ 2. $2x \equiv 5\ [6]$ 3. $x^2 \equiv 1\ [8]$ 4. $x^2 \equiv -1\ [9]$

Corrigé : 1. On a $5 \times 3 \equiv 1\ [7]$ d'où

$$\boxed{x \equiv 2\ [7]}$$

2. On a $$2x \equiv 5\ [6] \iff \exists k \in \mathbb{Z} \quad | \quad 2x + 6k = 5$$

ce qui est absurde puisque 2 ne divise pas 5. Ainsi

$$\boxed{\text{L'équation n'admet pas de solutions.}}$$

3. Pour $x \in \mathbb{Z}$ solution, on a nécessairement $\bar{x} \in \mathrm{U}(\mathbb{Z}/8\mathbb{Z})$. On se concentre donc sur les carrés de $\mathrm{U}(\mathbb{Z}/8\mathbb{Z})$ et on trouve

$$\bar{1}^2 = \bar{1} \qquad \bar{3}^2 = \bar{1} \qquad \bar{5}^2 = \bar{1} \qquad \bar{7}^2 = \bar{1}$$

Ainsi $$\boxed{x^2 \equiv 1\ [8] \iff x \in \mathrm{U}(\mathbb{Z}/8\mathbb{Z})}$$

4. Soit $x \in \mathbb{Z}$ solution. On a $x^4 \equiv 1\ [9]$, *i.e.* $x \times x^3 \equiv 1\ [9]$ d'où $\bar{x} \in \mathrm{U}(\mathbb{Z}/9\mathbb{Z})$. On liste les carrés non nuls de $\mathrm{U}(\mathbb{Z}/9\mathbb{Z})$:

$$\bar{1}^2 = \bar{1} \qquad \bar{2}^2 = \bar{4} \qquad \bar{4}^2 = -\bar{2} \qquad \bar{5}^2 = -\bar{2} \qquad \bar{7}^2 = \bar{4} \qquad \bar{8}^2 = \bar{1}$$

On constate que $-\bar{1}$ n'est pas un carré de $\mathbb{Z}/9\mathbb{Z}$ et par conséquent

$$\boxed{\text{L'équation n'admet pas de solution.}}$$

Exercice 2 (*)

Un corps $(\mathbb{K}, \times, +)$ est dit *algébriquement clos* si tout polynôme à coefficients dans $\mathbb{K}$ de degré supérieur ou égal à un admet une racine dans $\mathbb{K}$. Soit p premier. Le corps $\mathbb{F}_p$ est-il algébriquement clos ?

Corrigé : On considère $\mathrm{P} = \bar{1} + \prod_{k=0}^{p-1} (\mathrm{X} - \bar{k})$. Le polynôme P ne s'annule en aucun point de $\mathbb{F}_p$ et par conséquent

$$\boxed{\text{Le corps } \mathbb{F}_p \text{ n'est pas algébriquement clos.}}$$

Exercice 3 (*)

Résoudre dans $\mathbb{Z}/37\mathbb{Z}$ le système $$\begin{cases} \bar{6}x + \bar{7}y = \bar{0} \\ \bar{6}x - \bar{7}y = \overline{30} \end{cases}$$

Corrigé : L'entier 37 étant premier, on a dans le corps $\mathbb{F}_{37}$

$$\begin{cases}\bar{6}x+\bar{7}y=\bar{0}\\ \bar{6}x-\bar{7}y=\bar{30}\end{cases}\iff\begin{cases}\overline{12}x=\overline{30}\\ \overline{14}y=-\overline{30}\end{cases}$$

En effet, l'implication directe s'obtient en effectuant L_1+L_2, L_1-L_2 et l'implication directe avec $\bar{2}^{-1}(L_1'+L_2')$, $\bar{2}^{-1}(L_1'-L_2')$. Sans difficulté, on a

$$\overline{12}x=\overline{30}\iff -3\times\overline{12}x=-3\times\overline{30}\iff x=\overline{21}$$

Pour résoudre $\overline{14}y=-\overline{30}$, c'est moins évident. On utilise l'algorithme d'Euclide. On a

$$37=14\times2+9\qquad14=9\times1+5\qquad9=5\times1+4\qquad5=4\times1+1$$

d'où $\quad1=5-4\times1\qquad4=9-5\times1\qquad5=14-9\times1\quad$ et $\quad9=37-14\times2$

et

$$1=(14-9\times1)-(9-5\times1)\times1=(14-(37-14\times2))-(37-14\times2-(14-(37-14\times2)\times1)\times1$$

d'où

$$1=-3\times37+8\times14$$

Ainsi

$$\overline{14}y=-\overline{30}\iff\overline{14}y=\bar{7}\iff8\times\overline{14}y=8\times\bar{7}\iff\overline{y}=\overline{19}$$

On conclut

$$\boxed{\begin{cases}\bar{6}x+\bar{7}y=\bar{0}\\ \bar{6}x-\bar{7}y=\overline{30}\end{cases}\iff(x,y)=(\overline{21},\overline{19})}$$

Exercice 4 (*)

Soient m et n deux entiers non nuls non premiers entre eux. Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ sont-ils isomorphes ?

Corrigé : Soit $(\widehat{x},\dot{y})\in\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. On a $(m\vee n)(\widehat{x},\dot{y})=(\widehat{0},\dot{0})$ avec $m\vee n<mn$ puisque $(m\vee n)(m\wedge n)=mn$. Alors, aucun élément de $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ n'est d'ordre mn alors que le groupe $(\mathbb{Z}/mn\mathbb{Z},+)$ est cyclique et admet un tel élément. On conclut

$$\boxed{\text{Les anneaux } \mathbb{Z}/mn\mathbb{Z} \text{ et } \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} \text{ ne sont pas isomorphes.}}$$

Variante : Soit $\varphi:\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ un morphisme d'anneaux. On a $\varphi(\bar{1})=(\widehat{1},\dot{1})$ et

$$\forall k\in\mathbb{Z}\qquad\varphi(\bar{k})=\varphi(k\bar{1})=k\varphi(\bar{1})=k(\widehat{1},\dot{1})=(\widehat{k},\dot{k})$$

Par conséquent

$$\varphi(\overline{m\vee n})=(\widehat{0},\dot{0})\quad\text{et}\quad\overline{m\vee n}\neq\bar{0}$$

puisqu'on a $m\vee n\in[\![\,1\,;\,mn-1\,]\!]$. On retrouve le fait qu'un tel morphisme d'anneaux (qui est unique) n'est pas bijectif.

Exercice 5 (**)

Montrer que

$$\forall n\in\mathbb{N}\qquad13\text{ divise }2^{2^{8n+6}}+10$$

Corrigé : On remarque que $4^n\equiv4\ [12]$ pour tout n entier non nul. Puis

$$2^{8n+6}\equiv4^{4n+3}\equiv4\ [12]$$

Ainsi, d'après le petit théorème de Fermat, il vient

$$2^{2^{8n+6}}+10\equiv2^{4^{4n+3}}+10\equiv2^4+10\equiv26\ [13]$$

On conclut

$$\boxed{\forall n\in\mathbb{N}\qquad13\text{ divise }2^{2^{8n+6}}+10}$$

Exercice 6 (**)

Existe-il n entier non nul tel que l'écriture en base 10 de n^{2026} commence (au sens des puissances de 10 croissantes) par 2026 ?

Corrigé : Soit n entier non nul tel que $n^{2024} \equiv 2024\ [10000]$. On dispose de $k \in \mathbb{Z}$ tel que

$$n^{2024} = 2^3 \times 253 + 2^4 \times 5^4 \times k = 2\left(2^2 \times 253 + 2^3 \times 5^4 \times k\right)$$

On en déduit $2|n^{2024}$ d'où $2|n$. Ainsi, il existe m entier non nul tel que $n = 2m$. Par suite, on a

$$2\left(2^{2020}m^{2024} - 5^4 k\right) = 253$$

ce qui est absurde. On conclut

$$\boxed{\text{Il n'existe pas d'entier } n \text{ non nul tel que } n^{2024} \equiv 2024\ [10000].}$$

Exercice 7 (**)

Pour n entier non nul, on note $\tau(n)$ le nombre de diviseurs de n.

1. Déterminer une expression de $\tau(n)$ pour $n \geqslant 2$.
2. Montrer que si m et n sont deux entiers premiers entre eux, alors $\tau(mn) = \tau(m)\tau(n)$.

Corrigé : 1. Soit n entier $\geqslant 2$. Notons $\mathcal{D}_n$ l'ensemble des diviseurs de n. Pour $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls, on a

$$\mathcal{D}_n = \left\{ \prod_{i=1}^{r} p_i^{\beta_i}, \forall i \in [\![1\,;\, r]\!] \quad \beta_i \in [\![0\,;\, \alpha_i]\!] \right\}$$

Ainsi

$$\boxed{\forall n \geqslant 2 \qquad \tau(n) = \prod_{i=1}^{r} \operatorname{Card}[\![0\,;\, \alpha_i]\!] = \prod_{i=1}^{r} (\alpha_i + 1)}$$

Remarque : On peut aussi écrire

$$\forall n \in \mathbb{N}^* \qquad \tau(n) = \prod_{p \in \mathcal{P}} (1 + v_p(n))$$

2. Soient m et n des entiers premiers entre eux. Ils n'ont aucun facteur premier en commun. On peut donc écrire $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $n = \prod_{i=r+1}^{q} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls. Par suite

$$\boxed{\tau(mn) = \prod_{i=1}^{q} (\alpha_i + 1) = \prod_{i=1}^{r} (\alpha_i + 1) \times \prod_{i=r+1}^{q} (\alpha_i + 1) = \tau(m)\tau(n)}$$

Exercice 8 (**)

Soient a et p des entiers supérieurs à 2.
Montrer que si $a^p - 1$ est premier, alors $a = 2$ et p est premier.

Corrigé : Supposons $p = q\ell$ avec q et ℓ des entiers $\geqslant 2$. D'après l'identité de Bernoulli, il vient

$$a^p - 1 = (a^q)^\ell - 1 = (a^q - 1)\sum_{k=0}^{\ell-1} a^{qk}$$

ce qui contredit la primalité de $a^p - 1$. on en déduit que p est premier. Puis, on factorise

$$a^p - 1 = (a-1)\sum_{k=0}^{p-1} a^k$$

On a $a - 1 < a^p - 1$ et comme $a^p - 1$ est premier, il s'ensuit $a - 1 = 1$ et on conclut

$$\boxed{a^p - 1 \text{ premier} \quad \Longrightarrow \quad a = 2 \quad \text{et} \quad p \text{ premier}}$$

Remarque : Les nombres premiers de la forme $2^p - 1$ sont appelés *nombres premiers de Mersenne.*

Exercice 9 (**)

Soit p un nombre premier supérieur à 4. Montrer que $p^2 - 1$ est divisible par 24.

Corrigé : Notons $p = 2q + 1$ puisque p est impair. On a

$$p^2 - 1 = (p-1)(p+1) = 4q(q+1)$$

Comme $q(q+1)$ est un produit de deux entiers consécutifs, il est pair d'où $8|p^2-1$. Puis, comme $(p-1)p(p+1)$ est un produit de trois entiers consécutifs, alors $3|(p-1)p(p+1)$ et comme p est premier supérieur à 4, alors $3 \wedge p = 1$. Ainsi, d'après le lemme de Gauss, il vient $3|(p-1)(p+1)$ et comme $3 \wedge 8 = 1$, on conclut

$$\boxed{24|p^2-1}$$

Variante : On peut raisonner par congruence. Dans $\mathbb{Z}/8\mathbb{Z}$, on a $\bar{p} \in \{\pm\bar{1}, \pm\bar{3}\}$ d'où $\bar{p}^2 = \bar{1}$ et dans $\mathbb{Z}/3\mathbb{Z}$, on a $\widehat{p} = \pm\widehat{1}$ d'où $\widehat{p}^2 = \widehat{1}$. Pour $p^2 - 1$ divisible par 8, on peut aussi observer $p \equiv \pm 1\ [4]$ d'où $p = \pm 1 + 4k$ puis $p^2 = 1 + 8k(\pm 1 + 2k)$ avec k entier.

Exercice 10 (**)

Déterminer les nilpotents de $\mathbb{Z}/n\mathbb{Z}$ avec n entier $\geqslant 2$.

Corrigé : On a $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls. Soit $x \in \mathbb{Z}$ tel que $\bar{x}$ est un nilpotent de $\mathbb{Z}/n\mathbb{Z}$, *i.e.* il existe N entier non nul tel que

$$x^{\mathrm{N}} \equiv 0\ [n]$$

Par suite $$\forall i \in [\![\, 1\,;\, r\,]\!] \qquad p_i | x$$

et les p_i étant premiers distincts, on en déduit

$$x \in \left(\prod_{i=1}^{r} p_i\right)\mathbb{Z}$$

Réciproquement, soit $x \in \left(\prod_{i=1}^{r} p_i\right)\mathbb{Z}$. Avec $\alpha = \underset{i \in [\![\, 1\,;\, n\,]\!]}{\mathrm{Max}}\, \alpha_i$, on a $n|x^\alpha$ d'où $x^\alpha \equiv 0\ [n]$ ce qui prouve que $\bar{x}$ est nilpotent. On conclut

$$\boxed{\text{L'ensemble des nilpotents de } \mathbb{Z}/n\mathbb{Z} \text{ est l'idéal } \left(\prod_{i=1}^{r} p_i\right)\mathbb{Z}/n\mathbb{Z}.}$$

Exercice 11 (**)

Soit n entier non nul. Déterminer $\sum_{d|n}\varphi(d)$.

Corrigé : On a $$[\![1\,;\,n]\!] = \bigsqcup_{d|n}\{k \in [\![1\,;\,n]\!] \mid k\wedge n = d\}$$

Par ailleurs, pour $d|n$, on a

$$k\wedge n = d \iff \exists!(k',n') \in \mathbb{Z}^2 \quad | \quad k = k'd \qquad n = n'd \quad \text{et} \quad k'\wedge n' = 1$$

Comme n est entier non nul, alors n' l'est également. Ainsi, on peut mettre en bijection $k \in [\![1\,;\,n]\!]$ vérifiant $k\wedge n = d$ avec $k' \in [\![1\,;\,n']\!]$ vérifiant $k'\wedge n' = 1$. Il s'ensuit

$$\text{Card}\,\{k \in [\![1\,;\,n]\!] \mid k\wedge n = d\} = \text{Card}\,\{k' \in [\![1\,;\,n']\!] \mid k'\wedge n' = 1\} = \varphi(n')$$

Comme il s'agit d'union disjointe, on obtient

$$\text{Card}\,[\![1\,;\,n]\!] = \sum_{d|n}\varphi\left(\frac{n}{d}\right)$$

et comme l'application $d \mapsto \dfrac{n}{d}$ réalise une permutation de l'ensemble des diviseurs de n (involutive), on conclut

$$\boxed{\forall n \in \mathbb{N}^* \qquad \sum_{d|n}\varphi(d) = n}$$

Variante : Notons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls. L'ensemble $\mathcal{D}_n$ des diviseurs de n est

$$\mathcal{D}_n = \left\{\prod_{i=1}^{r} p_i^{\beta_i}, \forall i \in [\![1\,;\,r]\!] \quad \beta_i \in [\![0\,;\,\alpha_i]\!]\right\}$$

Par suite, on a $$\sum_{d|n}\varphi(d) = \sum_{(\beta_i)_{i\in[\![1\,;\,r]\!]} \in \prod_{i=1}^{r}[\![0\,;\,\alpha_i]\!]} \varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)$$

D'après le caractère multiplicatif de la fonction φ puis séparations des variables, il vient

$$\sum_{d|n}\varphi(d) = \sum_{(\beta_i)_{i\in[\![1\,;\,r]\!]} \in \prod_{i=1}^{r}[\![0\,;\,\alpha_i]\!]} \prod_{i=1}^{r}\varphi\left(p_i^{\beta_i}\right) = \prod_{i=1}^{r}\sum_{\beta_i=0}^{\alpha_i}\varphi(p_i^{\beta_i}) = \prod_{i=1}^{r}\left(1 + \sum_{\beta_i=1}^{\alpha_i}\left[p_i^{\beta_i} - p_i^{\beta_i-1}\right]\right)$$

Par téléscopage, on retrouve $$\boxed{\sum_{d|n}\varphi(d) = \prod_{i=1}^{r} p_i^{\alpha_i} = n}$$

Exercice 12 (**)

1. Soit $\mathrm{P} = \sum_{k=0}^{n} a_k \mathrm{X}^k \in \mathbb{Z}[\mathrm{X}]$ avec $a_0 \neq 0$ et $a_n \neq 0$. On suppose que P admet une racine rationnelle $r = \dfrac{p}{q}$ écrite sous forme irréductible. Montrer

$$p|a_0 \quad \text{et} \quad q|a_n$$

2. Le polynôme $\mathrm{P} = \mathrm{X}^3 + 3\mathrm{X} - 1$ est-il irréductible dans $\mathbb{Q}[\mathrm{X}]$?

Corrigé : 1. On a $\quad \mathrm{P}(r)=0 \iff \sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k = 0 \iff \sum_{k=0}^{n} a_k p^k q^{n-k} = 0$

Ainsi $\qquad a_0 q^n = -p\sum_{k=1}^{n} a_k p^{k-1} q^{n-k} \quad \text{et} \quad a_n p^n = -q\sum_{k=0}^{n-1} a_k p^k q^{n-1-k}$

On a $p \wedge q = 1$ d'où $p \wedge q^n = 1$ et $q \wedge p^n = 1$. Ainsi, d'après le théorème de Gauss, on conclut

$$\boxed{p|a_0 \quad \text{et} \quad q|a_n}$$

2. Si P n'est pas irréductible, il admet nécessairement un diviseur dans $\mathbb{Q}[\mathrm{X}]$ de degré égal à 1 ce qui implique que P admet une racine rationnelle. D'après le critère précédemment établi, si on dispose d'une racine rationnelle $r = p/q$ avec $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$, alors $p| - 1$ et $q|1$ d'où $r = \pm 1$. Or, ni 1, ni -1 n'est racine de P. On conclut

$$\boxed{\text{Le polynôme P est irréductible dans } \mathbb{Q}[\mathrm{X}].}$$

Exercice 13 (**)

Résoudre

1. $x^2 + x + \bar{7} = \bar{0}$ dans $\mathbb{Z}/13\mathbb{Z}$;
2. $x^2 - \bar{4}x + \bar{3} = \bar{0}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Corrigé : 1. Dans $\mathbb{Z}/13\mathbb{Z}$, on a

$$x^2 + x + \bar{7} = \bar{0} \iff x^2 + x - \bar{6} = \bar{0} \iff (x+\bar{3})(x-\bar{2}) = \bar{0}$$

Par intégrité, on conclut

$$\boxed{\text{Dans } \mathbb{Z}/13\mathbb{Z}, \text{ on a } x^2 + x + \bar{7} = \bar{0} \iff x \in \{-\bar{3}, \bar{2}\}}$$

Remarque : Comme on est dans un corps, on peut tout à fait procéder comme dans $\mathbb{R}$ avec la factorisation canonique suivante : pour $(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{F}_{13}^3$ et $\bar{a} \neq \bar{0}$

$$\bar{a}x^2 + \bar{b}x + \bar{c} = \bar{0} \iff \bar{a}(x + \bar{2}^{-1}\bar{a}^{-1}\bar{b})^2 = \bar{2}^{-2}\bar{a}^{-2}(\bar{b}^2 - \bar{4}\bar{a}\bar{c})$$

On retrouve donc les formules habituelles avec le discriminant dont il faudra chercher une racine.

2. Dans $\mathbb{Z}/12\mathbb{Z}$, on opte pour une approche différente puisque l'anneau n'est pas intègre. On a

$$x^2 - \bar{4}x + \bar{3} = \bar{0} \iff (x-\bar{2})^2 = \bar{1}$$

Or, on trouve $\qquad y^2 = 1 \iff y \in \{\bar{1}, \bar{5}, -\bar{5}, -\bar{1}\}$

Ainsi $\qquad \boxed{\text{Dans } \mathbb{Z}/12\mathbb{Z}, \text{ on a } x^2 - \bar{4}x + \bar{3} = \bar{0} \iff x \in \{-\bar{3}, \bar{1}, \bar{3}, \bar{7}\}.}$

Exercice 14 (**)

Soit n un entier impair non multiple de 5. Montrer qu'il existe un multiple positif de n dont l'écriture décimale est constituée de 1.

Corrigé : Supposons le problème résolu. Cela signifie qu'il existe k et N entiers non nuls tels que

$$kn = \sum_{i=0}^{\mathrm{N}-1} 10^i = \frac{10^{\mathrm{N}} - 1}{10 - 1} \iff 9kn + 1 = 10^{\mathrm{N}}$$

Comme n est impair et non multiple de 5, on a $10 \wedge n = 1$ et aussi $10 \wedge 9 = 1$ d'où $\overline{10} \in \mathrm{U}(\mathbb{Z}/9n\mathbb{Z})$. Ainsi, prenant $\mathrm{N} = o(\overline{10})$ l'ordre de $\overline{10}$ dans $\mathrm{U}(\mathbb{Z}/9n\mathbb{Z})$, on a bien $10^{\mathrm{N}} \equiv 1\ [9n]$, autrement dit on dispose de $k \in \mathbb{Z}$ tel que

$$10^{\mathrm{N}} = 1 + 9kn$$

Il est clair que k est strictement positif et on conclut

$$\boxed{\exists k \in \mathbb{N}^* \quad | \quad kn = \sum_{i=1}^{\mathrm{N}-1} 10^i}$$