ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°87

Exercice 1 (**)

Soit n entier avec $n \geqslant 2$. Montrer que n ne divise pas $2^n - 1$.

Corrigé : Supposons $n | 2^n - 1$. Soit p le plus petit facteur premier de n. On a clairement p impair puisque $2^n - 1$ est impair. Puis, on trouve $2^n \equiv 1$ $[p]$. Ainsi, dans $\mathrm{U}(\mathbb{Z}/p\mathbb{Z})$, on a $o(\bar{2}) | n$ et comme $\varphi(p) = p - 1$, on a aussi $o(\bar{2}) | p - 1$. Or, l'entier p est le plus petit facteur premier de n d'où $o(\bar{2}) = 1$ ce qui signifie $2 \equiv 1$ $[p]$ et qui est absurde. Ainsi

$$\boxed{\text{Pour } n \geqslant 2, \text{ l'entier } n \text{ ne divise pas } 2^n - 1.}$$

Exercice 2 (**)

Soit p un nombre premier impair et $x \in \mathbb{Z}$. Montrer

$$\bar{x} \in \mathbb{F}_p \text{ est un carré} \iff x^{\frac{p+1}{2}} \equiv x \; [p]$$

On admettra le résultat suivant : pour $\mathrm{P} \in \mathbb{F}_p[\mathrm{X}]$, le polynôme P admet au plus $\deg \mathrm{P}$ racines distinctes.

Corrigé : On peut réduire le problème à l'équivalence

$$\bar{x} \in \mathbb{F}_p \text{ est un carré non nul} \iff x^{\frac{p-1}{2}} \equiv 1 \; [p]$$

Si $\bar{x} = \bar{a}^2$, alors on a $\bar{x}^{\frac{p-1}{2}} = \bar{a}^{p-1} = \bar{1}$ d'après le petit théorème de Fermat. Réciproquement, considérons

$$\psi : \begin{cases} \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^* \\ x \longmapsto x^2 \end{cases}$$

C'est un morphisme de groupes multiplicatifs et chaque carré admet deux antécédents puisque

$$\psi(\bar{x}) = \psi(\bar{a}) \iff \bar{x}\bar{a}^{-1} \in \mathrm{Ker}\ \psi \quad \text{avec} \quad \mathrm{Ker}\ \psi = \{\pm \bar{1}\}$$

le noyau s'obtenant par intégrité en résolvant $(\bar{x} - \bar{1})(\bar{x} + \bar{1}) = \bar{0}$. On en déduit, comme dans l'exercice 0 feuille 0

$$\mathrm{Card}\ \mathrm{Im}\ \psi = \frac{\mathrm{Card}\ \mathbb{F}_p^*}{\mathrm{Card}\ \mathrm{Ker}\ \psi} = \frac{p-1}{2}$$

et par conséquent $\qquad \forall \bar{x} \in \mathrm{Im}\ \psi \qquad \bar{x}^{\frac{p-1}{2}} = \bar{1}$

Or, le polynôme $\mathrm{X}^{\frac{p-1}{2}} - 1$ admet au plus $\dfrac{p-1}{2}$ solutions donc les racines sont exactement les élément de $\mathrm{Im}\ \psi$ d'où la réciproque. On conclut

$$\boxed{\bar{x} \in \mathbb{F}_p \text{ est un carré} \iff x^{\frac{p+1}{2}} \equiv x \; [p]}$$

Variante : Chaque carré admet deux antécédents car par intégrité

$$\bar{x}^2 - \bar{a}^2 = (\bar{x} - \bar{a})(\bar{x} + \bar{a}) = \bar{0} \iff \bar{x} \in \{\bar{a}, -\bar{a}\}$$

On retrouve Card Im $\psi = \dfrac{p-1}{2}$.

Application : On a en particulier

$$-\bar{1} \text{ carré } \iff -1^{\frac{p-1}{2}} \equiv 1\ [p]$$

et
$$\frac{p-1}{2} \text{ pair } \iff p \equiv 1\ [4]$$

d'où
$$-\bar{1} \text{ carré } \iff p \equiv 1\ [4]$$

Exercice 3 (**)

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
$$y^2 = 1 \iff y \in \{\bar{1}, \bar{5}, -\bar{5}, -\bar{1}\}$$

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

Exercice 4 (***)

Déterminer tous les entiers $n \in \mathbb{N}^*$ tels que 7 divise $n^n - 3$.

Corrigé : Notons r le reste de la division euclidienne de n par 7 et s le reste de la division euclidienne de n par 6. D'après le petit théorème de Fermat, comme 7 est premier, on a

$$n^n \equiv n^{6\times q+s} \equiv (n^6)^q \times n^s \equiv n^s \equiv r^s\ [7]$$

Les cas $s = 0$, $r = 1$ et $r = 6 \equiv -1\ [7]$ sont clairement exclus. Pour $(r, s) \in [\![2\,;\,5]\!] \times [\![1\,;\,5]\!]$, on calcule $r^s\ [7]$ et on trouve $(r, s) = (3, 1)$ et $(r, s) = (5, 5)$. Ainsi, les solutions vérifient nécessairement

$$\begin{cases} n \equiv 3\ [7] \\ n \equiv 1\ [6] \end{cases} \quad \text{ou} \quad \begin{cases} n \equiv 5\ [7] \\ n \equiv 5\ [6] \end{cases}$$

On a $$7\times 1+6\times(-1)=1$$

Pour le premier système, une solution particulière est donnée par $n_0=7\times 1+3\times 6\times(-1)=-11$. La plus petite solution positive est donnée par $-11+6\times 7=31$. Pour le deuxième système, une solution particulière évidente est $n_1=5$. On conclut

$$\boxed{\text{Les ensembles solutions sont } \{31+42k, k\in\mathbb{N}\} \text{ et } \{5+42k, k\in\mathbb{N}\}.}$$

Exercice 5 (***)

Déterminer les entiers $n\geqslant 2$ tel que $\varphi(n)$ divise n.

Corrigé : Notons $n=\prod\limits_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i nombres premiers strictement ordonnés et les α_i entiers non nuls. On a $\varphi(n)=\prod\limits_{i=1}^{r}\left[p_i^{\alpha_i-1}(p_i-1)\right]$ d'où

$$\varphi(n)|n \iff \prod_{i=1}^{r}(p_i-1)|\prod_{i=1}^{r}p_i$$

Or, excepté le cas où $p_i=2$, on a p_i impair donc p_i-1 pair. Si $p_1>2$, on a $2^r|\prod\limits_{i=1}^{r}(p_i-1)$ d'où $2^r|\prod\limits_{i=1}^{r}p_i$. Or, le nombre $\prod\limits_{i=1}^{r}p_i$ est impair d'où l'absurdité. On a donc $p_1=2$. Si $r=1$, alors $\varphi(2^\alpha)=2^{\alpha-1}$ divise 2. Si $r>1$, on a

$$2^{r-1}|\prod_{i=1}^{r}(p_i-1) \implies 2^{r-2}|\prod_{i=2}^{r}p_i$$

Or, le nombre $\prod\limits_{i=2}^{r}p_i$ est impair d'où $r=2$. Ainsi, l'entier n s'écrit $n=2^\alpha p^\beta$ avec α,β entiers non nuls et p un nombre premier impair. On a

$$\varphi(n)|n \iff 2^{\alpha-1}p^{\beta-1}(p-1)|2^\alpha p^\beta \iff \frac{p-1}{2}|p$$

Comme p est premier, ses seuls diviseurs sont 1 et lui même et comme on a $\dfrac{p-1}{2}<p$, il s'ensuit nécessairement

$$\frac{p-1}{2}=1 \iff p=3$$

On conclut $$\boxed{\forall n\geqslant 2 \qquad \varphi(n)|n \iff n\in\left\{2^\alpha 3^\beta, (\alpha,\beta)\in\mathbb{N}^*\times\mathbb{N}\right\}}$$

Exercice 6 (***)

Soient p,q deux nombres premiers distincts. Montrer

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

Corrigé : On note

$$\Delta_0=[\![1\,;\,q-1]\!]\times[\![1\,;\,p-1]\!] \qquad \Delta_3=\{(k,\ell)\in\Delta_0 \mid pk=q\ell\}$$

$$\Delta_1=\{(k,\ell)\in\Delta_0 \mid pk<q\ell\} \qquad \Delta_2=\{(k,\ell)\in\Delta_0 \mid pk>q\ell\}$$

et on pose $$\varphi\colon \left\{\begin{array}{rcl} \Delta_0 & \longrightarrow & \Delta_0 \\ (k,\ell) & \longmapsto & (q-k,p-\ell) \end{array}\right.$$

La famille $(\Delta_i)_{i\in[\![\,1\,;\,3\,]\!]}$ est une partition de Δ_0. Pour $(k,\ell)\in\Delta_3$, comme $p\wedge q=1$ et $\ell<p$, $k<q$, il s'ensuit que $\Delta_3=\varnothing$. Soit $(k,\ell)\in\Delta_1$. On a

$$pk<q\ell \iff qp-pk>qp-q\ell \iff p(q-k)>q(p-\ell)$$

Comme $\varphi^2=\mathrm{id}$, on en déduit que φ réalise une bijection de Δ_1 sur Δ_2. Par suite

$$\mathrm{Card}\ \Delta_0=\mathrm{Card}\ \Delta_1+\mathrm{Card}\ \Delta_2=2\,\mathrm{Card}\ \Delta_2=(p-1)(q-1)$$

et $$\mathrm{Card}\ \Delta_2=\sum_{k=1}^{q-1}\left(\sum_{1\leqslant\ell\leqslant p-1,\ q\ell<pk}1\right)=\sum_{k=1}^{q-1}\left(\sum_{1\leqslant\ell<pk/q}1\right)$$

D'où $$\boxed{\sum_{k=1}^{q-1}\left\lfloor\frac{kp}{q}\right\rfloor=\frac{(p-1)(q-1)}{2}}$$

Variante : Notons r l'application qui à $k\in[\![\,1\,;\,q-1\,]\!]$ associe le reste de la division euclidienne de kp par q. Cette application est bien définie par unicité du reste et on a

$$\forall k\in[\![\,1\,;\,q-1\,]\!]\qquad kp=\left\lfloor\frac{kp}{q}\right\rfloor q+r(k)$$

L'application r est à valeurs *a priori* dans $[\![\,0\,;\,q-1\,]\!]$. Soit $k\in[\![\,1\,;\,q-1\,]\!]$. On a $k\wedge q=1$ puis avec le théorème de Gauss

$$r(k)=0\iff kp=\left\lfloor\frac{kp}{q}\right\rfloor q\quad\Longrightarrow\quad q|p$$

ce qui est absurde. On en déduit que r est à valeurs dans $[\![\,1\,;\,q-1\,]\!]$. Soit $(k,\ell)\in[\![\,1\,;\,q-1\,]\!]$ avec $k\neq\ell$, par exemple $k<\ell$. On a $\ell-k\in[\![\,1\,;\,q-2\,]\!]$ d'où $(\ell-k)\wedge q=1$ puis, avec le théorème de Gauss

$$r(k)=r(\ell)\iff p(\ell-k)=q\left(\left\lfloor\frac{\ell p}{q}\right\rfloor-\left\lfloor\frac{kp}{q}\right\rfloor\right)\quad\Longrightarrow\quad q|p$$

ce qui est absurde et prouve donc l'injectivité de r. Ainsi, l'application r est injective de $[\![\,1\,;\,q-1\,]\!]$ dans $[\![\,1\,;\,q-1\,]\!]$ ce qui prouve que c'est une permutation de $[\![\,1\,;\,q-1\,]\!]$. Puis, on a

$$\sum_{k=1}^{q-1}\left\lfloor\frac{kp}{q}\right\rfloor=\sum_{k=1}^{q-1}\frac{kp-r(k)}{q}=\frac{p}{q}\frac{q(q-1)}{2}+\frac{1}{q}\sum_{k=1}^{q-1}r(k)\quad\text{et}\quad\sum_{k=1}^{q-1}r(k)=\sum_{k=1}^{q-1}k=\frac{q(q-1)}{2}$$

On conclut $$\boxed{\sum_{k=1}^{q-1}\left\lfloor\frac{kp}{q}\right\rfloor=\frac{(p-1)(q-1)}{2}}$$

Exercice 7 (***)

Soit $n\geqslant 3$ entier impair.

1. Soit p nombre premier impair et α entier non nul. Montrer
$$x^2\equiv 1\ [p^\alpha]\iff x\equiv\pm 1\ [p^\alpha]$$
2. Combien y-a-t-il d'éléments x de $[\![\,1\,;\,n-1\,]\!]$ vérifiant $x^2\equiv 1\ [n]$?
3. Déterminer le nombre de carrés de $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$?

Corrigé : 1. On procède par récurrence sur α. Si $\alpha = 1$, le résultat est vrai par intégrité dans $\mathbb{F}_p$:

$$x^2 \equiv 1 \ [p] \iff (x-1)(x+1) \equiv 0 \ [p] \iff x \equiv \pm 1 \ [p]$$

Supposons le résultat vrai au rang α entier non nul. Soit x entier tel que $x^2 \equiv 1 \ [p^{\alpha+1}]$. Alors, on a $x^2 \equiv 1 \ [p^\alpha]$ d'où $x = \varepsilon + kp^\alpha$ avec $\varepsilon \in \{-1, 1\}$ et $k \in \mathbb{Z}$. Puis

$$x^2 \equiv 1 \ [p^{\alpha+1}] \iff (\varepsilon + kp^\alpha)^2 \equiv 1 \ [p^{\alpha+1}] \iff \varepsilon^2 + 2k\varepsilon p^\alpha + k^2 p^{2\alpha} \equiv 1 \ [p^{\alpha+1}]$$

Comme $p^{2\alpha} \equiv 0 \ [p^{\alpha+1}]$, on trouve $2k\varepsilon p^\alpha \equiv 0 \ [p^{\alpha+1}]$ autrement dit $2k\varepsilon \equiv 0 \ [p]$. On a $2\varepsilon \in \mathrm{U}(\mathbb{F}_p)$ d'où $k \equiv 0 \ [p]$, autrement dit $k = p\ell$ avec $\ell \in \mathbb{Z}$. Ainsi, on a

$$x = \varepsilon + \ell p^{\alpha+1} \equiv \pm 1 \ [p^{\alpha+1}]$$

ce qui clôt la récurrence. On conclut

$$\boxed{x^2 \equiv 1 \ [p^\alpha] \iff x \equiv \pm 1 \ [p^\alpha]}$$

2. On décompose $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers et les α_i entiers non nuls. D'après le théorème d'isomorphisme des restes chinois, on a

$$x^2 \equiv 1 \ [n] \iff \forall i \in [\![1\,;\, r]\!] \qquad x^2 \equiv 1 \ [p_i^{\alpha_i}]$$

Avec le résultat de la question précédente, on a donc

$$x^2 \equiv 1 \ [n] \iff \forall i \in [\![1\,;\, r]\!] \qquad x \equiv \pm 1 \ [p_i^{\alpha_i}]$$

On conclut $$\boxed{\mathrm{Card}\ \{x \in [\![1\,;\, n-1]\!] \mid x^2 \equiv 1 \ [n]\} = 2^r}$$

3. On pose $$\psi \colon \begin{cases} \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \\ \qquad x \qquad \longmapsto x^2 \end{cases}$$

Il s'agit d'un morphisme de groupes multiplicatifs. Le nombre de carrés de $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$ est précisément $\mathrm{Card\ Im}\ \psi$ et on a établi précédemment $\mathrm{Card\ Ker}\ \psi = 2^r$. Pour $(x, y) \in \mathrm{U}(\mathbb{Z}/n\mathbb{Z})^2$, on a

$$\psi(x) = \psi(y) \iff xy^{-1} \in \mathrm{Ker}\ \psi$$

Ainsi, on a $x = \alpha y$ avec $\alpha \in \mathrm{Ker}\ \psi$. Pour un carré de $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$, il y a donc 2^r racines. On conclut

$$\boxed{\text{Il y a } \mathrm{Card\ Im}\ \psi = \frac{\mathrm{Card\ U}(\mathbb{Z}/n\mathbb{Z})}{\mathrm{Card\ Ker}\ \psi} = \frac{\varphi(n)}{2^r} \text{ carrés dans } \mathrm{U}(\mathbb{Z}/n\mathbb{Z}).}$$

Remarque : Il s'agit d'un cas particulier d'utilisation du résultat de l'exercice 8 feuille 80.