ISM MP, Mathématiques
Année 2024/2025

# Feuille d'exercices n°86

## Exercice 1 (**)

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 2 (**)

Déterminer les entiers relatifs $n$ tels que $n^{13}\equiv n\ [42]$.

**Corrigé :** Soit $n$ entier. On a les factorisations

$$\begin{aligned}n^{13}-n=n(n^{12}-1)&=n(n^6-1)(n^6+1)=(n^7-n)(n^6+1)\\&=n(n^2-1)(n^4+n^2+1)(n^6+1)=(n^3-n)(n^4+n^2+1)(n^6+1)\end{aligned}$$

D'après le petit théorème de Fermat, on a $7|n^7-n$ puis $3|(n^3-n)$ d'où $3|(n^3-n)(n^4+n^2+1)=(n^7-n)$ et $2|n(n-1)$ d'où d'où $2|n(n^6-1)$. Les entiers 2, 3 et 7 sont premiers entre eux donc

$$2\times 3\times 7=42|(n^7-n)(n^6+1)=n^{13}-n$$

Ainsi $\boxed{\text{Tous les entiers relatifs } n \text{ vérifient } n^{13}\equiv n\ [42].}$

**Remarque :** On a établi un résultat un peu plus précis que celui attendu, à savoir $42|n^7-n$.

## Exercice 3 (***)

Soit $p$ premier et $k$ entier. Montrer que

$$\sum_{\bar{x}\in\mathbb{F}_p}\bar{x}^k=\bar{0}\quad\text{ou}-\bar{1}$$

**Corrigé :** Soit $\bar{a}\in\mathbb{F}_p^*$. L'application $\bar{x}\mapsto\bar{a}\bar{x}$ est une permutation de $\mathbb{F}_p$. On a

$$\sum_{\bar{x}\in\mathbb{F}_p}\bar{x}^k=\sum_{\bar{x}\in\mathbb{F}_p}(\bar{a}\bar{x})^k=\bar{a}^k\sum_{\bar{x}\in\mathbb{F}_p}\bar{x}^k\quad\Longrightarrow\quad(\bar{1}-\bar{a}^k)\sum_{\bar{x}\in\mathbb{F}_p}\bar{x}^k=0$$

Si $\bar{a}^k=1$ pour tout $\bar{a}\in\mathbb{F}_p^*$ (possible avec $k=p-1$ par exemple), alors

$$\sum_{\bar{x}\in\mathbb{F}_p} \bar{x}^k = \bar{0} + \sum_{\bar{x}\in\mathbb{F}_p^*} \bar{x}^k = \overline{p-1} = -\bar{1}$$

D'où $$\boxed{\sum_{\bar{x}\in\mathbb{F}_p} \bar{x}^k = \bar{0} \quad \text{ou} \quad = -\bar{1}}$$

## Exercice 4 (***)

Soit $a$ entier non nul et $p$ entier avec $p \geqslant 2$ tels que $a^{p-1} \equiv 1\ [p]$. On suppose que pour tout diviseur strict $d$ de $p-1$, l'entier $a^d - 1$ est premier avec $p$. Montrer que $p$ est premier.

**Corrigé :** On a $a^{p-1} \equiv 1\ [p]$ d'où $\bar{a} \in \mathrm{U}(\mathbb{Z}/p\mathbb{Z})$ et $o(\bar{a})|p-1$. Soit $d$ diviseur strict de $p-1$. Si $\bar{a}^d \equiv 1\ [p]$, alors $p|a^d - 1$ ce qui contredit $a^d - 1$ premier avec $p$. Par conséquent, on a $\bar{a}^d \not\equiv 1\ [p]$ et il en résulte que $o(\bar{a}) = p-1$. Ainsi, on obtient

$$\varphi(p) = \mathrm{Card}\ \mathrm{U}(\mathbb{Z}/p\mathbb{Z}) \geqslant \mathrm{Card}\ \langle a\rangle = p-1$$

et comme $\varphi(p) < p$, on en déduit $\varphi(p) = p-1$ ce qui prouve l'égalité $\mathrm{U}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$ puisque $\mathrm{U}(\mathbb{Z}/p\mathbb{Z}) \subset (\mathbb{Z}/p\mathbb{Z})^*$ et par conséquent

$$\boxed{\text{L'entier } p \text{ est premier.}}$$

## Exercice 5 (***)

Soit $p$ un nombre premier tel que $p^2+2$ est aussi premier. Montrer que $p^3+2$ l'est aussi.

**Corrigé :** Si $p = 2$, on a $p^2+2 \notin \mathcal{P}$. Si $p = 3$, on a $p^2+2 = 11 \in \mathcal{P}$ et $p^3+2 = 29 \in \mathcal{P}$. Si $p \geqslant 5$, on $p \equiv \pm 1\ [3]$ d'où $p^2 \equiv 1\ [3]$ et par suite $p^2+2 \equiv 0\ [3]$ ce qui prouve que $p^2+2$ n'est pas premier pour $p$ premier $\geqslant 5$. On conclut

$$\boxed{\text{Soit } p \in \mathcal{P} \text{ tel que } p^2+2 \in \mathcal{P}. \text{ Alors, on a } p^3+2 \in \mathcal{P}.}$$

## Exercice 6 (**)

Existe-il $n$ entier non nul tel que l'écriture en base 10 de $n^{2025}$ commence (au sens des puissances de 10 croissantes) par 2025 ?

**Corrigé :** Soit $n$ entier non nul tel que $n^{2025} \equiv 2025\ [10000]$. On dispose de $k \in \mathbb{Z}$ tel que

$$n^{2025} = 3^4 \times 5^2 + 2^4 \times 5^4 \times k = 5\,(3^4 \times 5 + 2^4 \times 5^3 \times k)$$

On en déduit $5|n^{2025}$ d'où $5|n$. Ainsi, il existe $m$ entier non nul tel que $n = 5m$. Par suite, on a

$$5\,(5^{2022}m^{2025} - 2^4 \times 5k) = 3^4$$

ce qui est absurde. On conclut

$$\boxed{\text{Il n'existe pas d'entier } n \text{ non nul tel que } n^{2025} \equiv 2025\ [10000].}$$

## Exercice 7 (***)

Quel est le chiffre des unités de $2024^{2024^{2024}}$ ?

**Corrigé :** On a $\quad 4^1 \equiv 4\ [10], \quad 4^2 \equiv 6\ [10], \quad 4^3 \equiv 4\ [10] \ldots$

Par récurrence, on montre pour tout $k$ entier

$$4^{2k} \equiv 6\ [10]$$

Comme l'exposant $2024^{2024}$ est pair on conclut

$$\boxed{2024^{2024^{2024}} \equiv 6\ [10]}$$

## Exercice 8 (***)

Soient $m, n$ des entiers non nuls. Établir

$$(3^n - 1) \wedge (3^m - 1) = 3^{n \wedge m} - 1$$

**Corrigé :** Notons $c = (3^n - 1) \wedge (3^m - 1)$ et $d = n \wedge m$. On a $d|n$ d'où $n = dk$ avec $k \in \mathbb{N}$ puis, avec l'identité de Bernoulli

$$3^n - 1 = (3^d)^k - 1 = (3^d - 1)\sum_{j=0}^{k-1} 3^{jk} \quad \Longrightarrow \quad 3^d - 1 | 3^n - 1$$

et de même pour $3^m - 1$ donc $3^d - 1|c$. D'après la propriété de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $d = um + vn$. Les entiers relatifs $u$ et $v$ ne sont pas tous deux strictement positifs sinon $d$ serait strictement supérieur à $n$ et $m$ alors qu'il en est un diviseur et comme $d$ est positif, les entiers $u$ et $v$ ne sont pas tous deux strictement négatifs. Sans perte de généralité, on peut supposer $u \leqslant 0$ et $v \geqslant 0$. Puis, on trouve

$$3^d - 1 = 3^{um+vn} - 1 = 3^{um+vn} - 3^{vn} + 3^{vn} - 1 = -3^{um+vn}(3^{-um} - 1) + 3^{vn} - 1$$

et à nouveau par des factorisations avec l'identité de Bernoulli, on obtient

$$3^d - 1 = (3^m - 1)(-3^d)3^v n \sum_{j=0}^{-u-1} 3^{mj} + (3^n - 1)\sum_{j=0}^{v-1} 3^{nj} \in (3^m - 1)\mathbb{Z} + (3^n - 1)\mathbb{Z} = c\mathbb{Z}$$

ce qui prouve $c|3^d - 1$. Les entiers $c$ et $3^d - 1$ sont donc associés et on conclut

$$\boxed{(3^n - 1) \wedge (3^m - 1) = 3^{n \wedge m} - 1}$$

**Variante :** On conserve les notations précédentes. On effectue la division euclidienne $n = mq + r$ avec $r \in [\![ 0\,;\, m - 1 ]\!]$. On a

$$3^n - 1 = 3^{mq+r} - 1 = 3^{mq+r} - 3^r + 3^r - 1 = 3^r(3^{mq} - 1) + 3^r - 1$$

$$= 3^r(3^m - 1)(1 + 3^m + \ldots + 3^{m(q-1)}) + 3^r - 1 = (3^m - 1)\mathrm{Q} + 3^r - 1$$

avec $\mathrm{Q} = 3^r(1 + 3^m + \ldots + 3^{m(q-1)})$. D'après le théorème d'Euclide, on a

$$(3^n - 1) \wedge (3^m - 1) = (3^m - 1) \wedge (3^r - 1)$$

Il suffit ensuite d'utiliser l'algorithme d'Euclide. On définit la suite $(u_k)_k$ par $u_0 = n$, $u_1 = m$ et $u_{k+2}$ le reste de la division euclidienne de $u_k$ par $u_{k+1}$. Il existe un seuil $p$ entier tel que $u_{p+1} = 0$. D'après la propriété établie, la suite $\left((3^{u_k} - 1) \wedge (3^{u_{k+1}} - 1)\right)_k$ est constante. Ainsi

$$(3^n - 1) \wedge (3^m - 1) = (3^{u_p} - 1) \wedge (3^{u_{p+1}} - 1) = 3^{u_p} - 1$$

et l'algorithme d'Euclide se termine avec $u_p = n \wedge m$ ce qui prouve le résultat souhaité.

## Exercice 9 (***)

Soit $p$ nombre premier impair. Déterminer le nombre de carrés dans $\mathbb{F}_p$.

**Corrigé :** 1. Notons $\Psi : \mathbb{F}_p \to \mathbb{F}_p, \bar{x} \mapsto \bar{x}^2$. Pour $x \in \mathbb{F}_p$, on a

$$\Psi(\bar{x}) = \bar{0} \iff \bar{x}^2 = \bar{0} \iff \bar{x} = \bar{0}$$

par intégrité du corps $\mathbb{F}_p$. Ceci prouve que $\bar{0}$ est un carré avec $\bar{0}$ pour unique antécédent. Soit $\bar{y} \in \text{Im } \Psi \setminus \{\bar{0}\}$. On dispose de $\bar{a} \in \mathbb{F}_p^*$ tel que $\psi(\bar{a}) = \bar{y}$ puis, pour $\bar{x} \in \mathbb{F}_p$

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

par intégrité du corps $\mathbb{F}_p$. Par ailleurs, on a

$$\bar{a} = -\bar{a} \iff \bar{2}\bar{a} = \bar{0} \underbrace{\iff}_{\bar{2} \in \mathrm{U}(\mathbb{F}_p)} \bar{a} = \bar{0}$$

d'où $\bar{a} \neq -\bar{a}$. Ainsi, tout élément de $\text{Im } \Psi \setminus \{\bar{0}\}$ admet exactement 2 antécédents dans $\mathbb{F}_p^*$ d'où

$$\text{Card } \mathbb{F}_p^* = p - 1 = 2 \,\text{Card } (\text{Im } \Psi \setminus \{\bar{0}\})$$

On conclut

$$\boxed{\text{Le nombre de carrés de } \mathbb{F}_p \text{ est } \frac{p+1}{2}.}$$

## Exercice 10 (***)

Soit $p$ entier avec $p \geqslant 2$. Montrer le théorème de *Wilson* :

$$(p-1)! \equiv -1 \ [p] \iff p \text{ premier}$$

**Corrigé :** Supposons $p$ premier $\geqslant 3$. Les éléments de $\mathbb{F}_p$ qui sont leur propre inverse vérifient

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

par intégrité du corps $\mathbb{F}_p$. On a $\bar{1} \neq -\bar{1}$ puisque $p > 2$. Par conséquent, dans le produit $\prod_{k=1}^{p-1} \bar{k}$, exceptés $\bar{1}$ et $\overline{p-1}$ qui sont leur propre inverse, tous les autres termes admettent leur inverse dans la liste $\left\{\bar{2}, \ldots, \overline{p-2}\right\}$. En les associant par paire, il vient

$$\prod_{k=1}^{p-1} \bar{k} = \bar{1} \times \overline{p-1} = -\bar{1}$$

Si $p = 2$, le résultat est toujours vrai. Supposons $(p-1)! \equiv -1 \ [p]$. Par suite, toutes les classes $\bar{1}, \ldots, \overline{p-1}$ sont inversibles puisque

$$\forall k \in [\![\, 1 \,;\, p-1 \,]\!] \qquad \bar{k} \times \left( - \prod_{i \in [\![\, 1 \,;\, p-1 \,]\!] \setminus \{k\}} \bar{i} \right) = \bar{1}$$

d'où $\mathbb{Z}/p\mathbb{Z}$ est un corps ce qui implique $p$ premier. Ainsi

$$\boxed{(p-1)! \equiv -1 \ [p] \iff p \text{ premier}}$$

## Exercice 11 (***)

1. Soit $p > 2$ un nombre premier. Montrer :

$$-\bar{1} \text{ carré dans } \mathbb{F}_p \iff p \equiv 1 \ [4]$$

2. En déduire qu'il existe une infinité de nombres premiers de la forme $1 + 4n$ avec $n$ entier.

**Corrigé :** 1. Supposons que $-\bar{1}$ soit un carré dans $\mathbb{F}_p$ et soit $\bar{x} \in \mathbb{F}_p$ tel que $\bar{x}^2 = -\bar{1}$. On a nécessairement $\bar{x} \in \mathbb{F}_p^*$. Comme $\bar{x}^4 = \bar{1}$, son ordre dans $\mathbb{F}_p^* = \mathrm{U}(\mathbb{F}_p)$ vérifie $o(\bar{x})|4$ et n'est ni 1 ni 2 d'où $o(\bar{x}) = 4$. Ainsi, on a 4 divise $p - 1$ d'où $p \equiv 1 \ [4]$. Réciproquement, si $p \equiv 1 \ [4]$, on note $p = 1 + 4n$ avec $n$ entier non nul. D'après le théorème de Wilson, on a $(p-1)! \equiv -1 \ [p]$ d'où

$$\prod_{k=1}^{4n} k \equiv -1\ [p] \iff \prod_{k=1}^{2n} k \times \prod_{k=1}^{2n}(-k) \equiv (-1)^{2n}(2n)!^2 \equiv (2n)!^2 \equiv -1\ [p]$$

On conclut $\boxed{-1 \text{ carré dans } \mathbb{F}_p \iff p \equiv 1\ [4]}$

2. Supposons que les nombres premiers de la forme $1+4n$ avec $n$ entier soient en nombre fini et notons $p$ le plus grand d'entre eux. On pose $\mathrm{N} = 1 + (p!)^2$ et soit $q$ facteur premier de N. On a $(p!)^2 \equiv -1\ [q]$ d'où $q$ de la forme $1+4n$ avec $n$ entier, d'après le résultat de la première question. Par hypothèse sur $p$, on a $q \leqslant p$ d'où $q$ divise $p!$ et comme $q$ divise N alors $q$ divise $\mathrm{N} - (p!)^2 = 1$ ce qui est absurde. On conclut

$\boxed{\text{Il existe une infinité de nombres premiers de la forme } 1+4n \text{ avec } n \text{ entier.}}$

**Remarque :** Il s'agit d'un cas particulier du *théorème de Dirichlet* encore appelé *théorème de la progression arithmétique* : soient $a$ et $b$ des entiers premiers entre eux, il existe une infinité de nombres premiers de la forme $an+b$ avec $n$ entier.

## Exercice 12 (***)

Soit $n$ un entier avec $n \geqslant 2$ et $p$ un nombre premier. Montrer

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

**Corrigé :** Soit $n \geqslant 2$. On a

$$v_p(n!) = v_p\left(\prod_{k=1}^{n} k\right) = \sum_{k=1}^{n} v_p(k) = \sum_{k=1}^{n}\left(\sum_{i\in\mathbb{N}^*,\ p^i|k} 1\right)$$

La somme en $i$ est finie puisque $p^i$ divise $k$ impose $p^i \leqslant k$ soit $i \leqslant \ln k / \ln p$. Comme les sommes sont finies, en changeant l'ordre de sommation, on obtient

$$v_p(n!) = \sum_{(k,i)\in[\![1\,;n]\!]\times\mathbb{N}^*,\ p^i|k} 1 = \sum_{i=1}^{+\infty}\left(\sum_{k\in[\![1\,;n]\!],\ p^i|k} 1\right) = \sum_{i=1}^{+\infty}\left(\sum_{k\in\{p^i,2p^i,\dots\lfloor n/p^i\rfloor p^i\}} 1\right)$$

On conclut $\boxed{\forall n \geqslant 2 \qquad \forall p \in \mathcal{P} \qquad v_p(n!) = \sum_{k=1}^{+\infty}\left\lfloor \frac{n}{p^k}\right\rfloor}$

**Remarque :** Ce résultat s'intitule *théorème de Legendre.*

## Exercice 13 (***)

Soit $n$ entier impair, $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$ et $\mathrm{Z} = \sum_{k=0}^{n-1}\omega^{k^2}$. Calculer $|\mathrm{Z}|^2$.

**Corrigé :** Soit $k \in [\![0\,;n-1]\!]$. On observe $\omega^k = \omega^\ell$ pour $(k,\ell) \in \bar{k}^2$. Ainsi, la valeur de $\omega^\ell$ est indépendante du choix de $\ell \in \bar{k}$. On définit

$$\forall k \in [\![0\,;n-1]\!] \qquad \omega^{\bar{k}} = \omega^k$$

En remarquant l'égalité $\bar{\omega} = \omega^{-1}$, il vient

$$|\mathrm{Z}|^2 = \left(\sum_{k=0}^{n-1}\omega^{k^2}\right)\left(\overline{\sum_{\ell=0}^{n-1}\omega^{\ell^2}}\right) = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{k^2}\bar{\omega}^{\ell^2} = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{k^2-\ell^2} = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{(k+\ell)(k-\ell)}$$

Ainsi $$|\mathrm{Z}|^2 = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{\overline{(k+\ell)(k-\ell)}} = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{(\overline{k+\ell})(\overline{k-\ell})}$$

L'application $(\bar{k},\bar{\ell}) \to (\overline{k+\ell},\overline{k-\ell})$ réalise une permutation de $(\mathbb{Z}/n\mathbb{Z})^2$. En effet, pour $(k,\ell)$ et $(p,q)$ dans $[\![\,0\,;\,n-1\,]\!]^2$, on a

$$\begin{cases}\overline{k+\ell}=\bar{p}\\ \overline{k-\ell}=\bar{q}\end{cases} \iff \begin{cases}\bar{2}\bar{k}=\bar{p}+\bar{q}\\ 2\ell=\bar{p}-\bar{q}\end{cases} \iff \begin{cases}\bar{k}=\bar{2}^{-1}(\bar{p}+\bar{q})\\ \bar{\ell}=\bar{2}^{-1}(\bar{p}-\bar{q})\end{cases}$$

les équivalences ayant lieu car $\bar{2}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ puisque $2\wedge n=1$. Ainsi, on a

$$|\mathrm{Z}|^2=\sum_{0\leqslant p,q\leqslant n-1}\omega^{\bar{p}\bar{q}}=\sum_{0\leqslant p,q\leqslant n-1}\omega^{\overline{pq}}=\sum_{0\leqslant p,q\leqslant n-1}\omega^{pq}=n+\sum_{p=1}^{n-1}\underbrace{\sum_{q=0}^{n-1}(\omega^p)^q}_{=0}$$

On conclut $\boxed{|\mathrm{Z}|^2=n}$

**Remarque :** Les sommes $\sum_{k=0}^{n-1}\omega^{k^2}$ avec $\omega=\mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$ et $n$ entier non nul sont les célèbres *sommes de Gauss* dont la détermination du signe devant les expressions algébriques résista à Gauss durant plusieurs années.