ISM MP, Mathématiques
Année 2025/2026

Feuille d'exercices n°87

Exercice 1 (**)

Montrer qu'il existe une infinité de nombres premiers de la forme $p = 4n + 3$ avec n entier non nul.

Corrigé : Il en existe, 7 par exemple. Supposons qu'ils soient en nombre fini $p_1, \dots, p_n$ et posons $\mathrm{A} = 4\prod_{k=1}^{n} p_k - 1$. Ainsi, on a $\mathrm{A} \equiv 3\ [4]$ et $\mathrm{A} > p_n$ d'où A non premier. On a $\mathrm{A} \equiv -1\ [p_k]$ pour tout $k \in [\![1\,;\, n]\!]$ donc A premier avec tous les p_k. Par conséquent, les diviseurs de A sont nécessairement de la forme $4m+1$ avec m entier ce qui implique $\mathrm{A} \equiv 1\ [4]$ en contradiction avec précédemment. On conclut

Il existe une infinité de nombres premiers de la forme $4n + 3$ avec n entier non nul.

Exercice 2 (**)

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

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

Exercice 3 (**)

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

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

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

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

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

Or, le polynôme $X^{\frac{p-1}{2}} - 1$ admet au plus $\dfrac{p-1}{2}$ solutions donc les racines sont exactement les élément de Im ψ 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 $\qquad \dfrac{p-1}{2} \text{ pair } \iff p \equiv 1 \ [4]$

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

Exercice 4 (***)

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 5 (***)

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 $\bar{a} \in \text{U}(\mathbb{Z}/p\mathbb{Z})$ 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

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

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

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

Exercice 6 (***)

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

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

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 7 (***)

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 $$\varphi : \begin{cases} \Delta_0 & \longrightarrow \Delta_0 \\ (k, \ell) & \longmapsto (q-k, p-\ell) \end{cases}$$

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 8 (****)

Pour n entier non nul, on note $\mathcal{P}(n)$ l'ensemble des nombres premiers inférieurs ou égaux à n puis on pose

$$\mathrm{P}_n = \prod_{p \in \mathcal{P}(n)} p \quad \text{et} \quad \pi(n) = \mathrm{Card}\ \mathcal{P}(n)$$

et $$\forall x > 0 \qquad \varphi(x) = x\,(\ln(x) - 1)$$

1. Montrer $$\forall n \in \mathbb{N} \qquad \binom{2n+1}{n} \leqslant 4^n$$
2. Établir $$\forall n \in \mathbb{N}^* \qquad \mathrm{P}_{2n+1} \leqslant 4^n \mathrm{P}_{n+1}$$
3. Montrer $$\forall n \in \mathbb{N}^* \qquad \mathrm{P}_n \leqslant 4^n$$
4. Établir $$\forall n \in \mathbb{N}^* \qquad \varphi(n) \leqslant \ln(n!)$$
5. Montrer $$\forall n \geqslant 2 \qquad 2n\ln(2) \leqslant \varphi\left(\mathrm{e}\,\frac{n}{\ln(n)}\right)$$
6. En déduire $$\forall n \geqslant 2 \qquad \pi(n) \leqslant \mathrm{e}\,\frac{n}{\ln(n)}$$

Corrigé : 1. Soit n entier. On a

$$(1+1)^{2n+1} = \sum_{k=0}^{2n+1} \binom{2n+1}{k} \geqslant \binom{2n+1}{n} + \binom{2n+1}{n+1} = 2\binom{2n+1}{n}$$

D'où $$\boxed{\forall n \in \mathbb{N}^* \qquad \binom{2n+1}{n} \leqslant 4^n}$$

Variante : On a $\displaystyle\binom{2n+1}{n} = \frac{\prod_{k=1}^{n}(2k)\prod_{k=1}^{n}(2k+1)}{\prod_{k=1}^{n}k\prod_{k=1}^{n}(k+1)} = 2^n\prod_{k=1}^{n}\underbrace{\left(\frac{2k+1}{k+1}\right)}_{\leqslant 2} \leqslant 4^n$

2. Soit n entier. On a $\displaystyle \mathrm{P}_{2n+1} = \mathrm{P}_{n+1}\prod_{p\in\mathcal{P}\cap[\![\, n+2\,;\,2n+1\,]\!]} p$

et $\displaystyle n!\binom{2n+1}{n} = \frac{(2n+1)!}{(n+1)!} = \prod_{k=n+2}^{2n+1} k$

d'où $\displaystyle \prod_{p\in\mathcal{P}\cap[\![\, n+2\,;\,2n+1\,]\!]} p \quad \text{divise} \quad n!\binom{2n+1}{n}$

Or, pour p premier dans $[\![\, n+2\,;\,2n+1\,]\!]$, on a $p\wedge n! = 1$ d'où $\displaystyle\left(\prod_{n+1<p\leqslant 2n+1} p\right)\wedge n! = 1$. D'après le lemme de Gauss, il s'ensuit que $\displaystyle\prod_{p\in\mathcal{P}\cap[\![\, n+2\,;\,2n+1\,]\!]} p$ divise $\binom{2n+1}{n}$ et d'après le résultat de la question précédente, on conclut

$$\boxed{\forall n\in\mathbb{N}^* \qquad \mathrm{P}_{2n+1}\leqslant 4^n\mathrm{P}_{n+1}}$$

3. On procède par récurrence. Pour n entier non nul, on pose

$$\mathscr{P}(n) : \quad \forall k\in[\![\, 1\,;\,2n\,]\!] \qquad \mathrm{P}_k\leqslant 4^k$$

La propriété $\mathscr{P}(1)$ est vraie. On suppose $\mathscr{P}(n)$ vraie pour n entier non nul fixé. D'après le résultat de la question 2.(b) et l'hypothèse de récurrence, il vient

$$\mathrm{P}_{2n+1}\leqslant 4^n\mathrm{P}_{n+1}\leqslant 4^{2n+1}$$

Enfin, on observe que $\mathrm{P}_{2n+2} = \mathrm{P}_{2n+1}$ puisque l'entier $2n+2$ est pair et n'est donc pas premier.

Par conséquent, on a $\mathrm{P}_{2n+2} = \mathrm{P}_{2n+1}\leqslant 4^{2n+1}\leqslant 4^{2n+2}$

ce qui prouve l'hérédité et clôt la récurrence. On conclut

$$\boxed{\forall n\in\mathbb{N}^* \qquad \mathrm{P}_n\leqslant 4^n}$$

4. Soit n entier non nul. Si $n=1$, l'inégalité est triviale. On suppose $n\geqslant 2$. Par une technique de comparaison série/intégrale, on obtient

$$\sum_{k=2}^{n}\int_{k-1}^{k}\ln(t)\,\mathrm{d}t\leqslant\sum_{k=2}^{n}\ln(k)$$

c'est-à-dire $\displaystyle\int_1^n\ln(t)\,\mathrm{d}t = \varphi(n)+1\leqslant\ln(n!)$

Ainsi $\boxed{\forall n\in\mathbb{N}^* \qquad \varphi(n)\leqslant\ln(n!)}$

5. Soit $n\geqslant 2$. On a les équivalences

$$\begin{aligned}2n\ln(2)\leqslant\varphi\left(\mathrm{e}\,\frac{n}{\ln(n)}\right) &\iff 2n\ln(2)\leqslant\mathrm{e}\,\frac{n}{\ln(n)}\left(\ln(n)+1-\ln(\ln(n))-1\right)\\ &\iff 2\ln(2)\leqslant\mathrm{e}\left(1-\frac{\ln(\ln(n))}{\ln(n)}\right)\end{aligned}$$

On pose $\displaystyle\forall x>0 \qquad \psi(x) = \frac{\ln(x)}{x}$

La fonction ψ est dérivable sur $]\,0\,;+\infty\,[$ et on trouve

$$\forall x > 0 \qquad \psi'(x) = \frac{1 - \ln(x)}{x^2}$$

d'où $$\forall x > 0 \qquad \psi(x) \leqslant \psi(\mathrm{e}\,) = \mathrm{e}^{-1}$$

On en déduit

$$\forall n \geqslant 2 \qquad \mathrm{e}\,-1 = \mathrm{e}\,(1-\psi(\mathrm{e}\,)) \leqslant \mathrm{e}\,(1-\psi(n)) = \mathrm{e}\,\left(1 - \frac{\ln(\ln(n))}{\ln(n)}\right)$$

Enfin, par concavité de $t \mapsto \ln(1+t)$ et convexité de $t \mapsto \mathrm{e}^t$, il vient

$$\forall t \in [\,0\,;1\,] \qquad 1 + \ln(1+t) \leqslant 1 + t \leqslant \mathrm{e}^t$$

d'où $$2\ln(2) = \int_0^1 [1 + \ln(1+t)]\ \mathrm{d}t \leqslant \int_0^1 \mathrm{e}^t\,\mathrm{d}t = \mathrm{e}\,-1$$

On conclut $$\boxed{\forall n \geqslant 2 \qquad 2n\ln(2) \leqslant \varphi\left(\mathrm{e}\,\frac{n}{\ln(n)}\right)}$$

6. On note $(p_k)_{k\geqslant 1}$ la suite strictement ordonnée des nombres premiers. Soit $n \geqslant 2$. On a

$$\pi(n)! = \prod_{k=1}^{\pi(n)} k \leqslant \prod_{k=1}^{\pi(n)} p_k = \mathrm{P}_n$$

D'après le résultat de la troisième question, il vient

$$\ln(\pi(n)!) \leqslant \ln(\mathrm{P}_n) \leqslant \ln(4^n) = 2n\ln(2)$$

et d'après le résultat des deux questions précédentes, on obtient

$$\varphi(\pi(n)) \leqslant \ln(\pi(n)!) \leqslant 2n\ln(2) \leqslant \varphi\left(\mathrm{e}\,\frac{n}{\ln(n)}\right)$$

La fonction φ est dérivable sur $[\,1\,;+\infty\,[$ avec $\varphi'(x) = \ln(x) > 0$ pour $x > 1$. Ainsi, la fonction φ croît strictement sur $[\,1\,;+\infty\,[$ et on conclut

$$\boxed{\forall n \geqslant 2 \qquad \pi(n) \leqslant \mathrm{e}\,\frac{n}{\ln(n)}}$$