DM 08
à rendre le lundi 16 décembre

Exercice 1. *Étude d'une suite récurrente*. Étudier la suite définie par $u_0 \in]0,1[$ et $u_{n+1} = \dfrac{2}{1+u_n}$: on souhaite un dessin, puis l'étude des variations des suites des termes pairs et impairs, et enfin la convergence éventuelle de $(u_n)_{n\in\mathbb{N}}$.

Correction 1. La fonction $f : x \mapsto \dfrac{2}{1+x}$ est strictement décroissante sur $\mathbb{R}_+$ (qui est clairement un intervalle stable) : Ainsi, $[0,2]$ est même stable par f ! Et 1 est le point fixe de f dans $\mathbb{R}_+$ (en effet, si $x \in \mathbb{R}$, $f(x) = x \Leftrightarrow x = 1$ ou $x = -2$).
De plus, pour tout x, $f(x) - x = \dfrac{2}{1+x} - \dfrac{x+x^2}{1+x} = \dfrac{2-x-x^2}{1+x} = \dfrac{-(x-1)(x+2)}{1+x}$, strictement positif sur $]0,1[$, strictement négatif sur $]1,+\infty[$.
Ainsi, $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ sont strictement monotones, de monotonies contraires.
On sait que, $u_{2(n+1)} = f \circ f(u_n)$ et $u_{2(n+1)+1} = f \circ f(u_{2n+1})$.
De plus, par le tableau de variations de f, on remarque que $[0,1]$ est stable par $f \circ f$, et $[1,2]$ aussi. Ainsi, pour tout n, $u_{2n} \in [0,1]$ et $u_{2n+1} \in [1,2]$.

Étudions plus précisément $f \circ f$:

$$f \circ f : x \mapsto \frac{2}{1+\frac{2}{1+x}} = \frac{2(1+x)}{1+x+2} = \frac{2+2x}{3+x},$$

et

$$f \circ f - \mathrm{Id} : x \mapsto \frac{2+2x}{3+x} - x = \frac{2+2x-x(3+x)}{3+x} = \frac{-x^2-x+2}{3+x} = \frac{-(x-1)(x+2)}{3+x}.$$

Donc, comme $u_0 \in]0,1[$, $u_2 = f \circ f(u_0) > u_0$, donc $(u_{2n})_{n\in\mathbb{N}}$ est croissante, majorée par 1, donc converge vers 1, seul point fixe strictement positif de $f \circ f$. De même pour $(u_{2n+1})_{n\in\mathbb{N}}$, décroissante minorée, qui converge donc vers 1.
Ainsi, $u_n \underset{n\to+\infty}{\longrightarrow} 1$.

Exercice 2. *Deux questions d'arithmétique*.

1. Démontrer que pour tout n dans $\mathbb{N}$, 6 divise $5n^3 + n$.

   Correction 2. On propose 3 preuves : **Preuve 1 : par récurrence.** On montre, pour tout n, $\mathcal{P}_n : 6|5n^3+n$.
   Initialisation : $5 \times 0^3 + 0 = 0$, divisible par 6.
   Hérédité : on suppose que 6 divise $5n^3 + n$. Alors

   $$\begin{aligned} 5(n+1)^3 + n + 1 &= 5(n^3+3n^2+3n+1) + n + 1 \\ &= 5n^3 + 15n^2 + 15n + 5 + n + 1 \\ &= (5n^3+n) + 15n(n+1) + 6. \end{aligned}$$

   Or, 6 divise $5n^3+n$ par HR, 6 divise 6 et, parmi n et $n+1$, l'un des deux entiers est pair, donc 2 divise $n(n+1)$ et 3 divise 15 donc 6 divise $15n(n+1)$. Donc 6 divise $5(n+1)^3 + n + 1$, d'où $\mathcal{P}_{n+1}$, d'où l'hérédité et le résultat.
   Preuve 2 : par disjonction. Soit n dans $\mathbb{N}$. Alors

- si n est pair, n^3 est pair, donc $5n^3+n \equiv 0[2]$.
- si n est impair, $n \equiv 1[2]$ donc $n^3 \equiv 1[2]$ donc $5n^3+n \equiv 0[2]$

De plus,

- si $n \equiv 0[3]$, alors n^3 aussi donc $5n^3+n \equiv 0[3]$.
- si $n \equiv 1[3]$, alors n^3 aussi donc $5n^3+n \equiv 5+1 \equiv 0[3]$.
- si $n \equiv 2[3]$, alors $n^3 \equiv 8 \equiv 2[3]$ donc $5n^3+n \equiv 12 \equiv 0[3]$.

Donc, quel que soit le cas considéré, 2 et 3 divisent $5n^3+n$ donc 6 divise $5n^3+n$.
Preuve 3 : par calcul malin et disjonction directe. Écrivons

$$5n^3+n = 6n^3+n-n^3 = 6n^3-(n^3-n) = 6n^3-n(n^2-1) = 6n^3-n(n-1)(n+1).$$

Or, 6 divise $6n^3$. De plus parmi n, $n-1$ et $n+1$, l'un des trois est pair et l'un des trois est multiple de 3. Donc 6 divise $n(n-1)(n+1)$. Donc 6 divise $5n^3+n$.

2. Démontrer que $\sqrt[3]{5}$ est irrationnel.

Correction 3. Supposons que $\sqrt[3]{5}$ soit rationnel. Alors on dispose de $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $\sqrt[3]{5} = \dfrac{p}{q}$. Comme $\sqrt[3]{5} > 0$, on a de plus $p > 0$. Donc $5 = \dfrac{p^3}{q^3}$ i.e. $5p^3 = q^3$. Alors

$$v_5(5p^3) = v_5(q^3),$$

i.e.

$$1 + 3v_5(p) = 3v_5(q),$$

ce qui est absurde car l'entier de droite est divisible par 3 et pas celui de gauche !
Donc $\sqrt[3]{5}$ est irrationnel !

Exercice 3. *Une autre preuve du petit théorème de Fermat*. Soit p un nombre premier, soit a un entier premier avec p.

1. Montrer que pour tous entiers m et n,

$$(ma \equiv na[p]) \Leftrightarrow (m \equiv n[p]).$$

Correction 4. Soient m et n deux entiers naturels.

$\boxed{\Leftarrow}$ Si $m \equiv n[p]$, alors par les règles usuelles sur les congruences, $am \equiv an[p]$.
$\boxed{\Rightarrow}$ Si $am \equiv an[p]$, alors p divise $am - an = a(m-n)$. Mais $a \wedge p = 1$, donc, d'après le théorème de Gauss, $m \equiv n[p]$.

2. Démontrer que l'application $\psi : \{a, 2a, \dots, (p-1)a\} \to \{1, 2, \dots, p-1\}$, qui à x associe son reste dans la division euclidienne par p, est une bijection.

Correction 5. Nommons $E_a = \{a, 2a, \dots, (p-1)a\}$. On a alors $E_1 = \{1, 2, \dots, p-1\}$. Comme E_a et E_1 sont deux ensembles finis de même cardinal, il suffit de montrer que ψ est injective. Soient x et x' dans E_a tels que $\psi(x) = \psi(x')$. Alors on dispose de k et k' dans E_1 tels que $x = ka$ et $x' = k'a$. Comme $\psi(x) = \psi(x')$, alors $ka \equiv k'a[p]$. Ainsi, par la question précédente, $k \equiv k'[p]$, donc p divise $k - k'$. Mais $|k - k'| < p$, donc, nécessairement, $k = k'$. Donc $x = x'$, d'où l'injectivité.
Ainsi, ψ est injective, donc elle est surjective.

3. En déduire que $a \times (2a) \times \cdots \times ((p-1)a) \equiv (p-1)![p]$.

Correction 6. On sait, par la question précédente, que

$$\prod_{k=1}^{p-1} \psi(ka) \equiv \prod_{k=1}^{n} (ka)[p].$$

Notons alors $\varphi(k) = \psi(ka)$. On sait que

$$\prod_{k=1}^{p-1} \psi(ka) = \prod_{k=1}^{p-1} \varphi(k) = \prod_{k=1}^{p-1} k,$$

car φ est une bijection de E_1 dans E_1. Ainsi,

$$(p-1)! \equiv a \times (2a) \times \cdots \times ((p-1)a)[p]$$

4. Montrer qu'on a alors $(p-1)!(a^{p-1}-1) \equiv 0[p]$. En déduire que $a^{p-1} \equiv 1[p]$.

Correction 7. Or, $a \times (2a) \times \cdots \times ((p-1)a) = a^{p-1}(p-1)!$, donc $a^{p-1}(p-1)! \equiv (p-1)![p]$. Donc $(a^{p-1}-1)(p-1)! \equiv 0[p]$. Or,

- p est premier et il ne divise aucun des entiers entre 1 et $p-1$, donc p ne divise pas $(p-1)!$ donc $p \wedge (p-1)! = 1$,
- p divise $(a^{p-1}-1)(p-1)!$,

donc, d'après le théorème de Gauss, p divise $a^{p-1}-1$, donc $a^{p-1}-1 \equiv 0[p]$, i.e. $a^{p-1} \equiv 1[p]$.

5. Montrer qu'alors pour tout entier a, $a^p \equiv a[p]$.

Correction 8. Si p ne divise pas a, on a $a^{p-1} \equiv 1[p]$, donc $a^p \equiv a[p]$.
Si p divise a, $a \equiv 0[p]$, donc $a^p \equiv 0[p]$, et donc $a^p \equiv a[p]$.

Exercice 4. *Théorème de Wilson*. Soit p un nombre premier différent de 2.

1. Montrer que $(p-1)^2 \equiv 1[p]$.

Correction 9. $(p-1)^2 = p^2 - 2p + 1$. Or, $p^2 \equiv 0[p]$ et $-2p \equiv 0[p]$, donc $(p-1)^2 \equiv 1[p]$.

2. Montrer que $x^2 \equiv 1[p]$ si, et seulement si $x \equiv 1[p]$ ou $x \equiv -1[p]$.

Correction 10. $\boxed{\Leftarrow}$ Déjà si $x \equiv 1[p]$ ou $x \equiv -1[p]$, $x^2 \equiv 1[p]$ par les règles de calcul sur les congruences.
$\boxed{\Rightarrow}$ Ensuite, si $x^2 \equiv 1[p]$, alors p divise $x^2 - 1 = (x-1)(x+1)$, donc, comme p est premier, p divise $x-1$ ou p divise $x+1$, donc $x \equiv 1[p]$ ou $x \equiv -1[p]$.

3. Soit n dans $\{1, 2, \ldots, p-1\}$ Montrer qu'il existe un unique entier m dans $\{1, 2, \ldots, p-1\}$ tel que $mn \equiv 1[p]$. Quand a-t-on $m = n$?

Correction 11. On sait que n est premier avec p donc par le théorème de Bézout, on dispose de u et v tels que $un+vp=1$. Effectuons la division euclidienne de u par p : $u=pq+r$, avec $1\leqslant r<p$. Donc $un+vp=(pq+r)n+vp=rn+(qn+v)p$. Donc $rn-1$ est divisible par p, i.e. $rn\equiv 1[p]$. D'où l'existence de cet entier.
Pour l'unicité, si $rn\equiv 1[p]$ et $mn\equiv 1[p]$, alors $rn\equiv nm[p]$, donc, comme n est premier avec p, $r=m$. D'où l'unicité.
Pour avoir $m=n$, il faut avoir $m^2\equiv 1[p]$, i.e. $m\equiv 1[p]$ ou $m\equiv -1[p]$, i.e., comme $m\in\{1,\dots p-1\}$, $m=1$ ou $m=p-1$. Réciproquement, si $m=1$ ou $m=p-1$, $m^2\equiv 1[p]$.

4. Démontrer que $(p-1)!\equiv p-1[p]$.

Correction 12. Écrivons $(p-1)!=(p-1)\times(2\times\cdots\times(p-2))$. On sait que pour tout élément m de $\{2,\dots,p-2\}$ il existe un unique m *différent de* m tel que $mn\equiv 1[p]$. En regroupant par paires ces éléments, on en déduit que $2\times\cdots\times(p-2)\equiv 1[p]$, et donc $(p-1)!\equiv p-1[p]$.

5. Déduire de ce qui précède une preuve du théorème de Wilson : pour tout entier naturel q, q est premier si, et seulement si $(q-1)!\equiv q-1[q]$.

Correction 13. On vient de montrer que si q est premier alors $(q-1)!\equiv q-1[q]$.
Réciproquement, si q vérifie $(q-1)!\equiv q-1[q]$, alors q divise $(q-1)!-(q-1)=(q-1)((q-2)!-1)$, donc, come $q\wedge(q-1)=1$, q divise $(q-2)!-1$. Donc on dispose de k dans $\mathbb{Z}$ tel que

$$(q-2)!-kq=1,$$

donc tous les entiers de 1 à $q-2$ satisfont une relation de Bézout avec q. Donc q est premier avec touts les entiers de 2 à $q-2$, donc, en particulier, n'est divisible par aucun de ces entiers. Il n'est pas non plus divisible par $q-1$, donc q n'est divisible par aucun des entiers entre 2 et $q-1$, donc q est premier.

Exercice 5. On note, pour tout entier naturel n, $\mathcal{P}(n)=\{k\in[\![0,n-1]\!],\ k\wedge n=1\}$ l'ensemble des entiers strictement inférieurs à n et premiers avec n. On note $\varphi(n)$ le nombre d'éléments de $\mathcal{P}(n)$.

1. Si p est premier et α est dans $\mathbb{N}$, montrer que $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

Correction 14. Si p est premier, les nombres non-premiers avec p^α sont ceux qui ont au moins un facteur commun avec lui : il s'agit donc exactement des nombres divisibles par p. Entre 0 et $p^\alpha-1$, il y en a exactement $\dfrac{\text{Card}([\![0,p^\alpha-1]\!])}{p}=\dfrac{p^\alpha}{p}=p^{\alpha-1}$. D'où au total $p^\alpha-p^{\alpha-1}$ nombres premiers avec p dans $[\![0,p^\alpha-1]\!]$, d'où $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

2. Soient m et n deux entiers premiers entre eux. Soit θ l'application qui à $k\in\mathcal{P}(mn)$ associe le couple (r,s) où r est le reste de la division euclidienne de k par m et s est le reste de la division euclidienne de k par n.

(a) Montrer que θ est à valeurs dans $\mathcal{P}(m)\times\mathcal{P}(n)$.

Correction 15. Si $k\in\mathcal{P}(mn)$, alors on écrit $\theta(k)=(r,s)$. On sait que $k=am+r$ et $\ell=bn+s$.
Or, par l'algorithme d'Euclide, on sait que $k\wedge m=m\wedge r$. Comme k est premier avec mn, il ne possède pas de diviseur premier commun avec mn, donc il n'a aucun facteur premier en commun avec m, donc $k\wedge m=1$. Donc $m\wedge r=1$. Donc $r\in\mathcal{P}(m)$. De même, $s\in\mathcal{P}(n)$.

(b) Soient (r,s) dans $\mathcal{P}(m)\times\mathcal{P}(n)$. Montrer que le système de congruences

$$\begin{cases} k\equiv r[m] \\ k\equiv s[n] \end{cases}$$

d'inconnue $k\in[\![1,mn]\!]$, admet une unique solution, et que cette solution est dans $\mathcal{P}(mn)$.

Correction 16. **Existence.** On sait que m et n sont premiers entre eux donc on dispose de u et v entiers tels que $mu+nv=1$. En particulier $mu\equiv 1[n]$ et $nv\equiv 1[m]$. Posons $k_0=mus+nvr$. Alors $k_0\equiv mus\equiv s[n]$ et $k\equiv nvr\equiv r[m]$. Donc k_0 est solution du système de congruences. Posons alors k le reste de la division euclidienne de k_0 par mn. Alors $k\equiv k_0[m]$ et $k\equiv k_0[n]$, et $k\in[\![0,mn-1]\!]$.
Unicité Soit ℓ une autre solution au problème. Alors $\ell\equiv k[m]$ et $\ell\equiv k[n]$, donc m divise $\ell-k$ et n divise $\ell-k$, donc, comme m et n sont premiers entre eux, mn diviser $\ell-k$. Mais $0\leqslant\ell\leqslant mn-1$ et $1-mn\leqslant -k\leqslant 0$ donc $|\ell-k|<mn$, donc, comme mn divise $\ell-k$, $\ell-k=0$, d'où l'unicité !
Appartenance à $\mathcal{P}(mn)$. On montre que la solution trouvée est première avec mn. On sait que $k\equiv r[m]$ donc $k\wedge m=r\wedge m$ (par la propriété de récurrence de l'algorithme d'Euclide). Comme $r\in\mathcal{P}(m)$, $k\wedge m=1$. De même $k\wedge n=1$. Donc k n'a pas de facteur premier commun avec m ni avec n. Comme m et n sont premiers entre eux, ils n'ont pas non plus de facteur premier commun, donc k n'a pas de facteur premier commun avec mn donc k est premier avec mn. Enfin, k est bien dans $[\![0,n-1]\!]$, donc $k\in\mathcal{P}(mn)$.

(c) Conclure que si n et m sont premiers entre eux, $\varphi(mn)=\varphi(m)\varphi(n)$.

Correction 17. On conclut que θ est bijective (on a trouvé sa bijection réciproque). Donc les deux ensembles $\mathcal{P}(mn)$ et $\mathcal{P}(m)\times\mathcal{P}(n)$ sont en bijection, donc $\text{Card}(\mathcal{P}(mn))=\text{Card}(\mathcal{P}(m)\times\mathcal{P}(n))$, donc $\varphi(mn)=\varphi(m)\times\varphi(n)$.

3. Si n est un entier naturel et $\prod_{i=1}^{r}p_i^{\alpha_i}$ sa décomposition en facteurs premiers, que vaut $\varphi(n)$?

Correction 18. Si n est dans $\mathbb{N}$ et $\prod_{i=1}^{r}p_i^{\alpha_i}$ sa décomposition en facteurs premiers, alors, comme $p_i^{\alpha_i}$ et $p_j^{\alpha_j}$ sont premiers entre eux si $i\neq j$,

$$\begin{aligned}\varphi(n)&=\varphi\left(\prod_{i=1}^{r}p_i^{\alpha_i}\right)\\ &=\prod_{i=1}^{r}\varphi(p_i^{\alpha_i}) \text{ par la question 10.(iv) et récurrence immédiate}\\ &=\prod_{i=1}^{r}\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right) \text{ par la question 9}\\ &=\prod_{i=1}^{r}p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)=n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\end{aligned}$$

(c'est la dernière formulation qui intéresse le plus les arithméticiens, parce qu'elle est reliée, d'une manière que je ne vais pas détailler ici, aux séries $\sum\frac{1}{k^s}$ (fonction ζ de Riemann))