1. Vrai ou faux

1. $(\mathbb{N},+)$ est un groupe abélien.
2. $(\mathbb{R},\times)$ est un groupe abélien.
3. Si H sous-groupe de G, alors l'élément neutre de G est aussi celui de H.
4. La réunion d'une famille de sous-groupes de G est un sous-groupe de G.
5. Si $(G,\star)$ groupe, $a,b,c\in G$, $a\star b=a\star c \Longleftrightarrow b=c$.
6. Si $(A,+,\times)$ est un anneau, $(A,+)$ et $(A,\times)$ sont des groupes.
7. Si $(\mathbb{K},+,\times)$ est un corps, $(\mathbb{K},+)$ et $(\mathbb{K},\times)$ sont des groupes.
8. $\{\pm 1\}$ est un sous groupe de $(\mathbb{R}^*,\times)$.
9. 1 est le seul élément inversible de $(\mathbb{Z},+,\times)$.
10. Tout anneau intègre est un corps.
11. $\mathbb{Z}^2$ est intègre.
12. Dans un anneau, si a différent de zéro, alors a est un diviseur de zéro.
13. Dans un anneau, $a^2-b^2=(a-b)\times(a+b)$.
14. Dans un anneau, $a^2=b^2 \Longleftrightarrow a=\pm b$.
15. $\mathbb{R}$ est une sous-algèbre de la $\mathbb{C}$-algèbre $\mathbb{C}$.

2. Exercices traités en cours

1 Soient E et F deux ensembles et $f\in F^E=\mathscr{F}(E,F)$. Montrer que

1. f est injective si et seulement s'il existe $g\in E^F$ telle que $g\circ f=\mathrm{id}_E$.
2. f est surjective si et seulement s'il existe $h\in E^F$ telle que $f\circ h=\mathrm{id}_F$.

2 Soit $(G,\star)$ un groupe, H,K sont des sous groupes de $(G,\star)$. Montrer que

$$H\cup K \text{ sous-groupe de } G \Longleftrightarrow H\subset K \text{ ou } K\subset H.$$

Solution de 2 :

- $\Longleftarrow$: ok
- $\Longrightarrow$: Si $H\cup K$ sous- groupe de G et $H\not\subset K$, on va montrer que $K\subset H$.
  On a $h\in H\setminus K$.
  Soit $k\in K$. Alors $k\star h\in H\cup K$ par stabilité de $\star$ sur $H\cup G$.
  Si $k\star h\in K$, alors $h=k^{-1}\star(k\star h)\in K$, ce qui n'est pas possible.
  C'est donc que $k\star h\in H$ et donc $k=(k\star h)\star h^{-1}\in H$.
  Finalement, on a bien $K\subset H$.

3 **1.** Montrer que $f:\left|\begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{C}^* \\ x & \longmapsto & \mathrm{e}^{\mathrm{i}x}\end{array}\right.$ est un morphisme de groupes.
Déterminer son image et son noyau.

2. Montrer que $f : \left|\begin{array}{ccc} \mathbb{R}^* & \longrightarrow & \mathbb{R}^* \\ x & \longmapsto & \frac{x}{|x|} \end{array}\right.$ est un morphisme de groupes.
   Déterminer son image et son noyau.
3. Même question pour $g : \left|\begin{array}{ccc} \mathbb{C}^* & \longrightarrow & \mathbb{C}^* \\ z & \longmapsto & \frac{z}{|z|} \end{array}\right.$.

4 Montrer que si $f : (A,+,\times) \to (A',\oplus,\otimes)$ est un morphisme d'anneaux :

- L'image réciproque d'un sous-anneau de A' est un sous-anneau de A.
- L'image directe d'un sous-anneau de A est un sous-anneau de A'.
- L'image réciproque d'un idéal de A' par f est un idéal de A.
- L'image directe d'un idéal de A par f est un idéal de $f(A)$.

3. Structure de groupe

5 Soit E un ensemble muni d'une loi interne $*$ associative. Montrer que l'ensemble des éléments réguliers à gauche (c'est-à-dire $x \in E$ tels que $\forall\, a, b \in E, \quad x * a = x * b \Rightarrow a = b$) (respectivement réguliers à droite) est stable pour $*$.

6 Soit $G =]-1,1[$ et pour $(x,y) \in G^2$, $x \star y = \dfrac{x+y}{1+xy}$.

Montrer que $(G,\star)$ est un groupe. Est-il commutatif ?

7 Soit G un groupe tel que pour tout $x \in G$, $x^2 = e$.

1. Montrer que G est abélien.
2. Soient H un sous-groupe strict de G, $a \in G \setminus H$. Montrer que $H \cup aH$ est un sous-groupe de G.
3. Si G est fini, en créant par récurrence un suite de sous-groupe de G de cardinal une puissance de 2, montrer que le cardinal de G est une puissance de 2.

8 **Transport de structure**

Soient G un ensemble muni d'une loi de composition interne $\star$, $(H,\times)$ un groupe et f une application surjective de H vers G telle que

$$\forall\, x, y \in H, \quad f(x \times y) = f(x) \star f(y).$$

Montrer que $(G,\star)$ est un groupe, et que si f est bijective, $(G,\star)$ isomorphe à $(H,\times)$.

Applications :

- Montrer que $(\mathbb{R},\star)$ est un groupe isomorphe à $(\mathbb{R},+)$, avec $a \star b = \sqrt[2021]{a^{2021} + b^{2021}}$
- Montrer que $(]-1,1[,\vartriangle)$ est un groupe isomorphe à $(\mathbb{R},+)$ avec $a \vartriangle b = \dfrac{a+b}{1+ab}$ (Utiliser th).

9 **Centre d'un groupe**

Soit G un groupe. On appelle *centre* de G, noté $Z(G)$, l'ensemble des éléments de G qui commutent avec tous les autres. Montrer qu'il s'agit d'un sous-groupe commutatif de G.

10 Soit $(G,\star)$ un groupe commutatif de neutre e. On pose $T(G) = \{x \in G \mid \exists\, n \in \mathbb{N}^*, \quad x^n = e\}$.

Montrer que $T(G)$ est un sous-groupe de $(G,\star)$.

11 Théorème de Lagrange

Soit $(G,*)$ un groupe d'**ordre** (c'est-à-dire de cardinal) fini, H un sous-groupe de G.

1. Montrer que la relation définie par $x\mathscr{R}y \iff x^{-1}*y\in H$ est une relation d'équivalence sur G.
2. Vérifier que les classes d'équivalence ont toutes le même cardinal.
3. Démontrer le théorème de Lagrange : $|H|$ divise $|G|$.

12

Pour tout $x\in\mathbb{R}$, on pose $M(x)=\begin{pmatrix}1 & 0 & x\\ -x & 1 & -\frac{x^2}{2}\\ 0 & 0 & 1\end{pmatrix}$.

Soit $G=\{M(x), x\in\mathbb{R}\}$. Montrer que $(G,\times)$ est un groupe. Est-il abélien ?

13

Soit G un ensemble et $\star$ une loi de composition interne associative sur G telle qu'il existe $e\in G$ tel que

- $\forall x\in G,\quad x\star e=x$
- $\forall x\in G,\ \exists x'\in G,\quad x\star x'=e$

Montrer que $(G,\star)$ est un groupe.

14

Soit $(G,\times)$ un groupe, $a\in G$ et H un sous-groupe de $(G,\times)$. On note $aHa^{-1}=\left\{aha^{-1}, h\in H\right\}$. Montrer que aHa^{-1} est un sous-groupe de $(G,\times)$.

15 Automorphismes intérieurs

Soit $(G,*)$ un groupe. Pour tout $a\in G$, on note $\varphi_a:\left|\begin{array}{ccc} G & \longrightarrow & G\\ x & \longmapsto & a*x*a^{-1}\end{array}\right.$

1. Soit $a\in G$. Montrer que φ_a est un automorphisme du groupe $(G,*)$.
2. On note $\mathrm{Int}(G)=\{\varphi_a, a\in G\}$. Montrer que $(\mathrm{Int}(G),\circ)$ est un groupe.

16 Sous-groupes distingués

Soit $(G,\times)$ un groupe. On dit qu'un sous-groupe H de $(G,\times)$ est distingué si

$$\forall (a,h)\in G\times H,\quad a\times h\times a^{-1}\in H.$$

1. Soit f un morphisme du groupe $(G,\times)$ vers un groupe $(G',*)$. Montrer que $\mathrm{Ker}\,f$ est un sous-groupe distingué de $(G,\times)$.
2. Soit H un sous-groupe distingué de $(G,\times)$ et K un sous-groupe de $(G,\times)$.
   On note $HK=\{x\times y, x\in H, y\in K\}$.
   Montrer que HK est un sous-groupe de $(G,\times)$.

4. Anneaux et idéaux, corps

17 Idéal annulateur

Soit A un anneau commutatif et M une partie de A. On appelle **annulateur** de M l'ensemble des éléments $a\in A$ tels que $am=0_A$ pour tout $m\in M$. Montrer qu'il s'agit d'un idéal de A.

18 Idéaux premiers

Soit A un anneau commutatif et I un idéal de A. On dit que l'idéal I est **premier** si pour tout $a,b\in A$, $ab\in I\Longrightarrow a\in I \text{ ou } b\in I$.

1. Quels sont les idéaux premiers de $\mathbb{Z}$?

2. Montrer que si f est un morphisme d'anneaux de A dans A', l'image réciproque d'un idéal premier de A' est un idéal premier de A.

19 **Idéaux d'un corps** Quels sont les idéaux d'un corps ?

Montrer que si un anneau commutatif ne possède que $\{0_A\}$ et A comme idéaux, c'est un corps.

20 **Idéaux de $\mathscr{M}_n(\mathbb{K})$** Pour $1 \leqslant i, j \leqslant n$, on note $E_{i,j}$ la matrice élémentaire ayant tous ses cœfficients nuls, sauf le cœfficient de la i^e ligne et de la j^e colonne qui vaut 1.

1. Rappeler la formule donnant $E_{i,j} \times E_{k,\ell}$.
2. Soit $M \in \mathscr{M}_n(\mathbb{K})$. Que valent $E_{i,j}M$ et $ME_{k,\ell}$?
3. On appelle idéal de $\mathscr{M}_n(\mathbb{K})$ tout sous-groupe I de $(\mathscr{M}_n(\mathbb{K}),+)$ tel que pour tout $A \in I$ et $M \in \mathscr{M}_n(\mathbb{K})$, $AM \in I$ et $MA \in I$.
   Démontrer que les seuls idéaux de $\mathscr{M}_n(\mathbb{K})$ sont $\{0\}$ et $\mathscr{M}_n(\mathbb{K})$.

21 **Nilpotents d'un anneau**

On dit qu'un élément a d'un anneau A est *nilpotent* lorsqu'il existe $n \in \mathbb{N}$ tel que $a^n = 0_A$. Le plus petit $n \in \mathbb{N}$ vérifiant cette propriété est alors appelé **indice de nilpotence** de a.

1. Quels sont les éléments nilpotents d'un anneau intègre ?

2. Montrer que si $a, b \in A$ nilpotents qui commutent, $a+b$ et ab le sont. Que peut-on dire de leurs indices de nilpotence ?

3. Montrer que si A est commutatif, l'ensemble des éléments nilpotents est un idéal de A.

4. Montrer que si ab est nilpotent, ba l'est aussi. Comparer leurs indices de nilpotence.

5. Soit a nilpotent. Montrer que $1_A - a$ est inversible dans A et préciser son inverse.

6. Démontrer que l'ensemble des éléments nilpotentes d'un anneau commutatif, appelé **nilradical de l'anneau** est un idéal de A.

22

Montrer que tout anneau fini intègre est un corps.

On pourra vérifier qu'une translation $x \mapsto ax$ est bijective.

23

Montrer que $\mathbb{Q}$ ne possède qu'un sous-corps.

24

Déterminer les endomorphismes de l'anneau $\mathbb{Z}$, puis de l'anneau $\mathbb{Q}$ et enfin de l'anneau $\mathbb{R}$.

Indication : pour le passage de $\mathbb{Q}$ à $\mathbb{R}$, on pourra vérifier que l'image d'un nombre positif l'est encore et en déduire qu'un endomorphisme est croissant puis utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$

25

Déterminer les endomorphismes de l'anneau $\mathbb{C}$ laissant $\mathbb{R}$ globalement invariant.

26

Soit A un anneau.

1. Justifier que les endomorphismes du groupe $(A,+)$ forment un anneau pour les lois $+$ et $\circ$, noté $\mathrm{Endo}(A)$.

2. Pour $a \in A$, on note $f_a : \left| \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array} \right.$. Montrer que l'application $\phi : \left| \begin{array}{ccc} A & \longrightarrow & \mathrm{Endo}(A) \\ a & \longmapsto & \phi(a) = f_a \end{array} \right.$ est bien définie et est un morphisme d'anneau.

27 Entiers de Gauss

On définit l'ensemble des entiers de Gauss comme étant l'ensemble des nombres complexes à coordonnées entières $\mathbb{Z}[\mathrm{i}] = \mathbb{Z} + \mathrm{i}\mathbb{Z} = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$.

1. Montrer qu'il s'agit d'un anneau intègre.
2. On définit, pour $z \in \mathbb{C}$, $N(z) = |z|^2$. Déterminer le groupe des inversibles de $\mathbb{Z}[\mathrm{i}]$ en utilisant N.
3. Un élément a de $\mathbb{Z}[\mathrm{i}]$ est dit irréductible dans $\mathbb{Z}[\mathrm{i}]$ lorsque

$$(\exists\, u, v \in \mathbb{Z}[\mathrm{i}],\quad a = uv) \Rightarrow u \text{ est inversible ou } v \text{ est inversible.}$$

Montrer que 2 n'est pas irréductible dans $\mathbb{Z}[\mathrm{i}]$.

4. Soit $\varphi : \mathbb{Z}[\mathrm{i}] \to \mathbb{Z}[\mathrm{i}]$ un endomorphisme d'anneaux.
   4.a) Calculer les deux valeurs possibles pour $\varphi(\mathrm{i})$.
   4.b) Quels sont les endomorphismes d'anneaux de $\mathbb{Z}[\mathrm{i}]$?
5. **Division euclidienne ★**
   5.a) Soit $z \in \mathbb{C}$. Démontrer qu'il existe $\omega \in \mathbb{Z}[\mathrm{i}]$ tel que $|z - \omega| < 1$.
   Indication : s'appuyer sur un dessin.
   5.b) Soient $u, v \in \mathbb{Z}[\mathrm{i}]$ avec $v \neq 0$. Démontrer qu'il existe $q, r \in \mathbb{Z}[i]$ avec $u = qv + r$ et $|r| < |v|$. A-t-on unicité ?
   5.c) Démontrer que $\mathbb{Z}[\mathrm{i}]$ est principal.

On définit l'ensemble des rationnels de Gauss comme étant l'ensemble des nombres complexes à coordonnées rationnelles $\mathbb{Q}[\mathrm{i}] = \mathbb{Q} + \mathrm{i}\mathbb{Q} = \{a + \mathrm{i}b \mid a, b \in \mathbb{Q}\}$.

6. Montrer qu'il s'agit d'un corps.
7. Quels sont les endomorphismes de corps de $\mathbb{Q}[\mathrm{i}]$?

28 Anneau de Boole

On considère $(A, +, \times)$ un anneau de Boole c'est-à-dire un anneau non nul tel que tout élément est idempotent pour la 2e loi ce qui signifie $\forall\, x \in A,\quad x^2 = x$.

1. Montrer que $\forall\, (x, y) \in A^2,\quad xy + yx = 0_A$ et en déduire que $\forall\, x \in A,\quad x + x = 0_A$.
   En déduire que l'anneau A est commutatif.
2. Montrer que la relation binaire définie sur A par $x \preccurlyeq y \iff yx = x$ est une relation d'ordre.
3. Montrer que $\forall\, (x, y) \in A^2,\quad xy(x + y) = 0_A$.
   En déduire qu'un anneau de Boole intègre ne peut avoir que deux éléments.

29 Soit E un ensemble. On note $\mathscr{P}(E)$ l'ensemble des parties de E.

Soit A et B deux parties de E. On appelle différence symétrique de A et B l'ensemble

$$A\Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

1. Montrer que Δ est une loi associative à l'aide d'une table de vérité dont les entêtes sont $x \in A$, $x \in B$, $x \in C$, $x \in A\Delta B$, $x \in (A\Delta B)\Delta C$, $x \in B\Delta C$ et $x \in A\Delta(B\Delta C)$
2. Montrer que $(\mathscr{P}(E), \Delta)$ est un groupe abélien.
3. Montrer que $\cap$ est distributive sur Δ
4. Montrer que $(\mathscr{P}(E), \Delta, \cap)$ est un anneau commutatif.
5. Montrer que $(\mathscr{P}(E), \Delta, \cap)$ est un anneau de Boole (voir exercice précédent).
6. Soit $E' \subset E$. Démontrer que $I = \mathscr{P}(E')$ est un idéal de $\mathscr{P}(E)$.
7. Réciproquement, soit I un idéal de $\mathscr{P}(E)$, montrer que

$$\forall X \in I, \ \ \forall Y \subset X, \ \ Y \in I$$

et

$$\forall X \in I, \ \ \forall Y \subset I, \ \ X \cup Y \in I$$

8. En déduire qu'il existe $E' \subset E$ tel que $I = \mathscr{P}(E')$.
9. Si E est infini, démontrer que l'ensemble des parties finies de E forme un idéal de $\mathscr{P}(E)$ qui n'est pas de la forme $\mathscr{P}(E)$.

30 **Radical d'un idéal** Soit A un anneau commutatif. Si I est un idéal de A, on appelle **radical de** I l'ensemble

$$\sqrt{I} = \left\{x \in A, \ \exists\, n \geqslant 1, \ \ x^n \in I\right\}.$$

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Soient I, J deux idéaux de A et $p \geqslant 1$. Montrer que

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}\ ;$$

$$\sqrt{\sqrt{I}} = \sqrt{I}\ ;$$

$$\sqrt{I^p} = \sqrt{I}.$$

3. Si $A = \mathbb{Z}$ et $I = k\mathbb{Z}$ avec $k \geqslant 1$, déterminer le radical de I.

31 Soient $\alpha \in \mathbb{Q}_*^+$ tel que $\sqrt{\alpha} \notin \mathbb{Q}$ et $\mathbb{Q}(\sqrt{\alpha}) = \mathbb{Q} + \sqrt{\alpha}\mathbb{Q} = \{r + r'\sqrt{\alpha}\ ;\ r, r' \in \mathbb{Q}\}$.

1. Montrer que $(\mathbb{Q}(\sqrt{\alpha}), +, \times)$ est un corps.
2. Montrer que les anneaux $\mathbb{Q}(\sqrt{\alpha})$ et $\mathbb{Q}^2$ ne sont pas isomorphes[1].
3. Montrer que les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ ne sont pas isomorphes[2].

---

1. *Si c'était le cas, calculer $f(r)$ pour $r \in \mathbb{Q}$ puis $f(\sqrt{\alpha})$...*

2. *Si c'était le cas, considérer le carré de l'image de $\sqrt{2}$, puis l'image elle-même... On pourra utiliser que $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{R} \setminus \mathbb{Q}$.*

5. Arithmétique entière

32 CCINP 86 - Petit théorème de Fermat

1. Soit $(a,b,p)\in\mathbb{Z}^3$. Prouver que : si $p\wedge a=1$ et $p\wedge b=1$, alors $p\wedge(ab)=1$.
2. Soit p un nombre premier.
   (a) Prouver que $\forall k\in[\![1,p-1]\!]$, p divise $\binom{p}{k}k!$ puis en déduire que p divise $\binom{p}{k}$.
   (b) Prouver que : $\forall n\in\mathbb{N},\ n^p\equiv n\ [p]$.
   Indication : procéder par récurrence.
   (c) En déduire, pour tout entier naturel n, que : p ne divise pas $n\Longrightarrow n^{p-1}\equiv 1\ [p]$.

Solution de 32 : CCINP 86 - Petit théorème de Fermat

1. On suppose $p\wedge a=1$ et $p\wedge b=1$.
   D'après le théorème de Bézout,
   $\exists(u_1,v_1)\in\mathbb{Z}^2$ tel que $u_1p+v_1a=1$. (1)
   $\exists(u_2,v_2)\in\mathbb{Z}^2$ tel que $u_2p+v_2b=1$. (2)
   En multipliant les équations (1) et (2), on obtient :

   $$\underbrace{(u_1u_2p+u_1v_2b+u_2v_1a)}_{\in\mathbb{Z}}p+\underbrace{(v_1v_2)}_{\in\mathbb{Z}}(ab)=1.$$

   Donc, d'après le théorème de Bézout, $p\wedge(ab)=1$.
2. Soit p un nombre premier.
   (a) Soit $k\in[\![1,p-1]\!]$. $\binom{p}{k}=\dfrac{p!}{k!(p-k)!}=\dfrac{p(p-1)...(p-k+1)}{k!}$.
   Donc $\binom{p}{k}k!=p(p-1)...(p-k+1)$.
   donc $p\mid\binom{p}{k}k!$. (3)
   Or, $p\wedge k=1$ (car p est premier) donc, d'après 1., $p\wedge k!=1$.
   Donc, d'après le lemme de Gauss, (3) $\Longrightarrow p\mid\binom{p}{k}$.
   (b) Procédons par récurrence sur n.
   Pour $n=0$ et pour $n=1$, la propriété est vérifiée.
   Soit $n\in\mathbb{N}$.
   Supposons que la propriété (P_n) : $n^p\equiv n\ [p]$ soit vérifiée.
   Alors, d'après la formule du binôme de Newton, $(n+1)^p=n^p+\sum\limits_{k=1}^{p-1}\binom{p}{k}n^k+1$. (4)
   Or $\forall k\in[\![1,p-1]\!]$, $p\mid\binom{p}{k}$ donc $p\mid\sum\limits_{k=1}^{p-1}\binom{p}{k}n^k$.
   Donc d'après (4) et (P_n), $(n+1)^p\equiv n+1\ [p]$ et (P_{n+1}) est vraie.
   (c) Soit $n\in\mathbb{N}$ tel que p ne divise pas n.
   Comme p est premier, alors $p\wedge n=1$.
   La question précédente donne p divise $n^p-n=n(n^{p-1}-1)$.
   Or comme p est premier avec n, on en déduit, d'après le lemme de Gauss, que p divise $n^{p-1}-1$.
   Ce qui signifie que $n^{p-1}\equiv 1\ [p]$. (petit théorème de Fermat).

33 À savoir faire absolument

Résoudre, dans $\mathbb{Z}$, $3x+11y=2$ puis $14x+35y=5$ et $14x+35y=7$.

34 1. Pour quelles valeurs de n a-t-on $(n^3+n)\wedge(2n+1)=1$?
2. Pour quelles valeurs de $n\in\mathbb{Z}$ a-t-on $(n+2)|(2n^2+9n+13)$?
3. Montrer que pour tout $n\in\mathbb{Z}$, $(21n+4)\wedge(14n+3)=1$.

Solution de 34 :

1. $(n^3+n)\wedge(2n+1)=1$ si et seulement si
$$n(n^2+1)\wedge(2n+1)=1$$
si et seulement si
$$\begin{cases} n\wedge(2n+1)=1 \\ (n^2+1)\wedge(2n+1)=1 \end{cases}$$
Il s'agit de la propriété $ab\wedge c=1 \Longleftrightarrow a\wedge c=1$ et $b\wedge c=1$: le sens direct s'obtient avec le théorème de Bézout ou en s'intéressant au diviseurs communs possibles de a et c d'une part et de b et c d'autre part, le sens réciproque s'obtient en multipliant des relations de Bézout : $1=(au+cv)(bu'+cv')=abU+cV\ldots$
Or, en se souvenant de la propriété d'Euclide $a\wedge b=(a-bq)\wedge b$ (pas nécessairement une division euclidienne), on obtient $n\wedge(2n+1)=n\wedge 1=1$ toujours vrai.
Puis, toujours avec cette propriété $(n^2+1)\wedge(2n+1)=(n^2-2n)\wedge(2n+1)=n(n-2)\wedge(2n+1)$.
Donc
$$(n^3+n)\wedge(2n+1)=1 \Longleftrightarrow \begin{cases} n\wedge(2n+1)=1 \\ (n-2)\wedge(2n+1)=1 \end{cases} \Longleftrightarrow (n-2)\wedge(2n+1)=1 \Longleftrightarrow (n-2)\wedge\big(2n+1-2(n-2)\big)=(n-2)\wedge 5=1$$
Comme 5 est premier, on en déduit que les solutions sont les entiers n tels que $5\nmid(n-2)$ c'est-à-dire tels que $\boxed{n\not\equiv 2\ [5].}$
2. On écrit $2n^2+9n+13=2(n+2)^2+n+5=2(n+2)^2+(n+2)+3$.
Donc $(n+2)|(2n^2+9n+13)$ si et seulement si $n+2|3$ si et seulement si $n+2\in\{-1,1,-3,3\}$. Les solutions sont $\boxed{-3,-1,-5,1}$ (ce que l'on peut effectivement vérifier).
3. Avec la propriété d'Euclide, si $n\in\mathbb{Z}$,
$$(21n+4)\wedge(14n+3)=\big(21n+4-(14n+3)\big)\wedge(14n+3)=(7n+1)\wedge\big(14n+3-2(7n+1)\big)=(7n+1)\wedge 1=1$$
Autre méthode, avec une relation de Bézout :
$$-2(21n+4)+3(14n+3)=1.$$

35 Nombres de Mersenne [3] - Très classique - Oral Centrale

Montrer que si $a \in \mathbb{N}, n \in \mathbb{N} \setminus \{0,1\}$ tel que $a^n - 1$ est premier, alors $a = 2$ et n est premier.

Solution de 35 : Nombres de Mersenne [4] - Très classique - Oral Centrale

La factorisation

$$a^n - 1 = (a-1)(a^{n-1} + \cdots + 1)$$

donne la première réponse, puis

$$2^{n_1 n_2} - 1 = (2^{n_1})^{n_2} - 1 = (2^{n_1} - 1)(\ldots)$$

donne la deuxième.

36 Nombres de Fermat [5] - Très classique - Oral Mines

1. Soient $a, n \in \mathbb{N}^*$, $a \geqslant 2$. Montrer que si $a^n + 1$ est premier, a est pair et n est une puissance de 2. On appelle nombres de Fermat les nombres $F_n = 2^{2^n} + 1$. Ils sont premiers pour n de 2 à 4, mais ne le sont pas pour n de 5 à 32 (contrairement à ce que conjectura Fermat).
2. Démonstration de 1734 d'Euler du fait que F_5 n'est pas premier.
   (a) Comparer $5^4 + 2^4$ et $1 + 5 \times 2^7$ (sans calculatrice !).
   (b) En déduire que $5^4 \times 2^{28} \equiv 1 \ [641]$.
   (c) Conclure que 641 divise F_5.
3. Montrer que pour tout $n \in \mathbb{N}$, $F_{n+1} = (F_n - 1)^2 + 1$ et en déduire que F_n et F_{n+1} sont premiers entre eux.
4. Pour $n \in \mathbb{N}$, établir que $F_{n+1} = \prod_{k=0}^{n} F_k + 2$. En déduire que les F_n sont premiers entre eux deux à deux. Retrouver le fait que le nombre de nombres premiers est infini.

Solution de 36 : Nombres de Fermat [6] - Très classique - Oral Mines

Si n a un facteur premier impair p, on écrit

$$2^n + 1 = 2^{mp} + 1 = (2^m)^p + 1$$

Or on connaît très bien

$$a^n - b^n = (a-b)(\ldots)$$

Mais, si n est impair, remplaçant b par $-b$, on en déduit

$$a^n + b^n = (a+b)(a^{n-1} - b a^{n-2} + \cdots + b^{n-1})$$

Appliqué à notre situation, on trouve

$$2^n + 1 = (2^m + 1)(2^{m(p-1)} - 2^{m(p-2)} \cdots + 1)$$

On prend bien soin de justifier que c'est une vraie factorisation ($1 < 2^m + 1 < 2^n + 1$). Et on a résolu la première question. Comme souvent, c'est l'exercice classique sur les nombres de Mersenne (si $a^n - 1$ est premier, $a = 2$ et n est premier) qui peut donner l'idée

37

En s'inspirant de la démonstration sur l'infinité des nombres premiers, montrer qu'il existe une infinité de nombres premiers de la forme $4k - 1$ [7].

3. Un tel nombre est alors appelé nombre de Mersenne (mathématicien français 1588-1648). La réciproque est fausse ($2^{11} - 1 = 23 \times 89$). Les plus grands nombres premiers connus actuellement sont des nombres de Mersenne : $2^{77\,232\,917} - 1$ a été découvert le 26 décembre 2017 (23 249 425 chiffres en base décimale).
5. Ils interviennent dans la constructibilité à la règle et au compas des polygones réguliers.
7. Le théorème de Dirichlet (difficile) affirme qu'il existe une infinité de nombres premiers congrus à a modulo b si a et b sont premiers entre eux.

Solution de 37 :

S'intéresser aux diviseurs premiers de $N=4p_1\cdots p_n-1$ si les nombres premiers de la forme $4k-1$ sont exactement $p_1,\dots,p_n$.

38 Justifier l'existence de 1000 entiers consécutifs sans nombre premier.

Solution de 38 :

Il suffit de considérer les entiers de $1001!+2$ à $1001!+1001$.

39 Formule de Legendre - Très classique - Oraux divers

Combien y a-t-il de zéros à la fin de $100!$? De $1000!$? De $2021!$?

Montrer que $v_p(n!)=\displaystyle\sum_{k=1}^{+\infty}\left\lfloor\frac{n}{p^k}\right\rfloor$ pour p premier et $n\in\mathbb{N}^*$.

Solution de 39 : Formule de Legendre - Très classique - Oraux divers

Les multiples de q s'écrivent $k=q\ell$ avec $\ell\in\mathbb{Z}$ uniquement déterminé par k et q, et alors $1\leqslant k=q\ell\leqslant n$ si et seulement si $\frac{1}{q}\leqslant\ell\leqslant\frac{n}{q}$ si et seulement si $1\leqslant\ell\leqslant\left\lfloor\frac{n}{q}\right\rfloor$ avec $\ell\in\mathbb{Z}$.

Le nombre de multiples de q entre 1 et n est donc $\left\lfloor\frac{n}{q}\right\rfloor$.

Ainsi, la valuation p-adique de $n!$ avec p premier s'obtient en ajoutant les valuations p-adiques des entiers entre 1 et m, d'après la question précédente :

- les $\left\lfloor\frac{n}{p}\right\rfloor$ multiples de p fournissent chacun (au moins) un facteur p,
- les $\left\lfloor\frac{n}{p^2}\right\rfloor$ multiples de p^2 fournissent chacun (au moins) un facteur p supplémentaire,
- les $\left\lfloor\frac{n}{p^3}\right\rfloor$ multiples de p^3 fournissent chacun (au moins) un facteur p supplémentaire,
- et ainsi de suite.

Le décompte s'arrête car la suite entière $\left(\left\lfloor\frac{n}{p^i}\right\rfloor\right)_{i\in\mathbb{N}^*}$ finit par s'annuler et on obtient la formule de Legendre (avec un nombre fini de termes non nuls) :

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

Autre rédaction possible : on peut dénombrer les entiers entre 1 et n ayant une valuation q-adique exactement égale à $i\in\mathbb{N}$: il s'agit des multiples de q^i qui ne sont pas multiples de q^{i+1} et qui sont au nombre de $\left\lfloor\frac{n}{q^i}\right\rfloor-\left\lfloor\frac{n}{q^{i+1}}\right\rfloor$, d'où la formule (les sommes étant toujours faussement infinies)

$$v_p(n!)=\sum_{i=0}^{+\infty}i\cdot\left(\left\lfloor\frac{n}{p^i}\right\rfloor-\left\lfloor\frac{n}{p^{i+1}}\right\rfloor\right)=\sum_{i=1}^{+\infty}i\cdot\left\lfloor\frac{n}{p^i}\right\rfloor-\sum_{i=1}^{+\infty}(i-1)\cdot\left\lfloor\frac{n}{p^i}\right\rfloor=\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor.$$

40 On note p_n le n^{e} nombre premier et $\pi(x)$ le nombre de nombres premiers $\leqslant x$.

1. Montrer que pour tout $n\geqslant1$, $p_{n+1}\leqslant p_1\cdots p_n+1$.
2. Montrer que pour tout $n\geqslant1$, $2n-1\leqslant p_n\leqslant 2^{2^{n-1}}$.
3. Justifier[8] que $\forall x>0,\ \ln(\ln x)<\pi(x)<x$.

41 En utilisant l'algorithme d'Euclide, montrer que pour tout $n,m\in\mathbb{N}$, $(2^n-1)\wedge(2^m-1)=2^{n\wedge m}-1$.

8. Le (difficile) théorème de Hadamard et De la Vallée-Poussin dit « Théorème des Nombres Premiers » affirme que $\pi(x)\sim\dfrac{x}{\ln x}$, ou, de manière équivalente, $p_n\sim n\ln n$.

42 Oral Centrale

Déterminer le chiffre des unité de 1587^{413}.

Solution de 42 : Oral Centrale

7

43

Soit $n=4444^{4444}$. Calculer la somme des chiffres de la somme des chiffres de la somme des chiffres de n.

Solution de 43 :

$f\,:\,k\mapsto$(somme des chiffres de k). Calculer $f\circ f\circ f(n)$.

$f(n)\equiv n\ [9]$. Or $4444=9\times 493+7$, donc $4444\equiv 7\ [9]$ et $4444^{4444}\equiv 7^{4444}\ [9]$.

Mais $7^2\equiv 4\ [9]$, $7^3\equiv -2\ [9]$ et $7^3\equiv 1\ [9]$. D'où $7^{4444}=7^{3k+1}\equiv 7\ [9]$ donc $f(n)\equiv 7\ [9]$. Puis $f(f(f(n)))\equiv 7\ [9]$.

De plus, $n\leqslant 10000^{5000}=10^{20000}$. Donc n possède au plus $20\ 000$ chiffres et $f(n)\leqslant 9\times 20000=180000$.

Puis $f(f(n))\leqslant 1+8+4\times 9=45$ et $f(f(n))\equiv f(n)\equiv 7\ [9]$.

Donc $f(f(f(n)))<4+9=13$ et $f(f(f(n)))\equiv 7\ [9]$. Donc $f(f(f(n)))=7$.

44 Oral Mines

Soit $p\geqslant 5$ un nombre premier. Montrer que 24 divise p^2-1.

Solution de 44 : Oral Mines

p est congru à 1 ou à -1 modulo 3 (car $p>3$), donc $p+1$ ou $p-1$ est divisible par 3. Donc p^2-1, leur produit, l'est. De plus, p, premier et impair car >2, est congru à 1, 3, 5 ou 7 modulo 8. Donc son carré est congru à 1, 1, 1 ou 1 modulo 8. Donc p^2-1 est divisible par 3 et par 8, qui sont premiers entre eux, il est donc divisible par 24.

Autre méthode : remarquer que parmi $p-1$, p et $p+1$, l'un est divisible par 3 et parmi $p-1$, p, $p+1$, $p+2$, l'un est divisible par 4.

45

Montrer que pour tout $n\in\mathbb{N}$

1. $6\,|\,5n^3+n$
2. $7\,|\,3^{2n+1}+2^{n+2}$
3. $5\,|\,2^{2n+1}+3^{2n+1}$
4. $11\,|\,3^{8n}5^4+5^{6n}7^3$
5. $9\,|\,4^n-1-3n$
6. $15^2\,|\,16^n-1-15n$.

46 Cryptographie à clé publique RSA [9]

La cryptographie à clé publique est une méthode pour crypter un message à destination d'une personne (Alice), par une méthode que tout le monde connaît, mais de façon à ce que seul le destinataire puisse décoder le message. Les messages considérés ici seront des nombres (par exemple fabriqués en remplaçant chacune des lettres du message à envoyer par son code ASCII, après découpage en morceaux pour obtenir des nombres pas trop grands).

La destinataire Alice choisit deux « grands » nombres premiers p et q, et calcule le produit $N=pq$. Elle rend N public et surtout garde pour elle les valeurs de p et q. Elle choisit ensuite un entier e premier avec $(p-1)(q-1)$ et le donne à tout le monde : (N,e) sera la clé publique. Elle choisit en général e ayant peu de termes dans sa décomposition en binaire, pour que le cryptage ne demande pas trop longtemps.

Comme Alice est la seule à connaître p et q, elle est également la seule à pouvoir calculer $(p-1)(q-1)$, et donc à déterminer un entier de Bézout d tel que de $de\equiv 1\ \left[(p-1)(q-1)\right]$. d sera la clé de décodage, que l'on conserve bien sûr très secrète.

Le principe de la méthode est alors le suivant. Bob, qui veut envoyer un message M à Alice calcule $M'\equiv M^e\ [N]$ et envoie M' à Alice. Celle-ci calcule ensuite $M''\equiv M'^d\ [N]$.

Montrer que M et M'' sont égaux modulo N, et donc que Alice peut décoder le message de Bob pourvu que M soit inférieur à N.

9. Rivest, Shamir et Adleman, 1979

47 **Triplets pythagoriciens** On résout dans $\mathbb{Z}^3$ l'équation $x^2+y^2=z^2$.

1. Montrer que l'on peut se ramener au cas où $x \wedge y \wedge z = 1$. Montrer qu'alors x, y, z sont deux à deux premiers entre eux.
2. On suppose que c'est le cas. Montrer que deux des trois nombres x, y, z sont impairs et que le est pair puis montrer que z est impair.
   On suppose dorénavant que x,z sont impairs et y pair.
   On pose $y=2y'$, $X=\dfrac{z+x}{2}$ et $Z=\dfrac{z-x}{2}$.
3. Montrer que $X \wedge Z = 1$ et que X et Z sont des carrés parfaits.
4. En déduire que l'ensemble des triplets pythagoriciens est l'ensemble des triplets de la forme

$$\left(d\left(u^2-v^2\right), 2duv, d\left(u^2+v^2\right)\right)$$

où $d \in \mathbb{N}$, $(u,v) \in \mathbb{Z}^2$, à une permutation près des deux premières composantes.