Structures algébriques

- Il faut connaître la définition d'un groupe, d'un anneau, d'un corps, mais on ne s'en sert directement que rarement.
- La plupart du temps, pour montrer qu'on a un groupe, on montre plutôt que c'est un sous-groupe d'un groupe connu, en reconnaissant une partie d'un groupe connu et
  - ⋆ en utilisant la caractérisation d'un sous-groupe, c'est ce qui sert le plus dans la pratique,
  - ⋆ en faisant apparaître l'ensemble comme image directe ou réciproque d'un sous-groupe par un morphisme de groupe,
  - ⋆ en voyant l'ensemble comme image d'un groupe par une bijection vérifiant la propriété des morphismes de groupes.
- Attention à l'erreur très classique consistant à appliquer la formule du binôme dans un anneau sans vérifier que les deux éléments commutent.
- Attention aussi à bien penser à vérifier, pour un sous-anneau la présence de 1_A et pour un morphisme d'anneaux l'image de 1_A.

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, $a,b,c\in G$, $a\star b=a\star c\iff b=c$.
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, $a^2=b^2\iff a=\pm b$.
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

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

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 $\forall a,b\in E,\ x*a=x*b\Rightarrow a=b$) (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 $]-1,1[,\triangle)$ est un groupe isomorphe à $(\mathbb{R},+)$ avec $a\triangle b=\dfrac{a+b}{1+ab}$ (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 $T(G)=\{x\in G\mid \exists n\in\mathbb{N}^*,\ x^n=e\}$.

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

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

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 $a,b\in A$, $ab\in I\Longrightarrow a\in I$ 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 coefficients nuls, sauf le coefficient 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 $\mathcal{M}_n(\mathbb{K})$ tout sous-groupe I de $(\mathcal{M}_n(\mathbb{K}),+)$ tel que pour tout $A\in I$ et $M\in\mathcal{M}_n(\mathbb{K})$, $AM\in I$ et $MA\in I$.
Démontrer que les seuls idéaux de $\mathcal{M}_n(\mathbb{K})$ sont $\{0\}$ et $\mathcal{M}_n(\mathbb{K})$.

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 $v\neq0$. 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 $\forall\, x\in A,\ \ x^2=x$.

1. Montrer que $\forall\,(x,y)\in A^2,\ \ xy+yx=0_A$ et en déduire que $\forall\, x\in A,\ \ x+x=0_A$.
   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 $\forall\,(x,y)\in A^2,\ \ xy(x+y)=0_A$.
   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

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

et

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

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

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

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

- le fait que $a \wedge b = (a - bq) \wedge b$ pour tout $q \in \mathbb{Z}$ permet parfois des simplifications intéressantes.
- Lorsque l'on manipule des équations avec pgcd et/ou ppcm, il est souvent intéressant de se ramener à des nombres premiers entre eux en posant $x = dx'$ et $y = dy'$ où $d = x \wedge y$.
- Pour savoir si des nombres sont premiers entre eux, on peut penser au théorème de Bézout ou revenir à la définition (les diviseurs communs sont triviaux). Penser aussi aux nombres premiers :pas de diviseur premier en commun.
- Pour des problèmes de divisibilité, penser à travailler avec des congruences.
- Tous les nombres premiers sont impairs... sauf 2, le seul pair. Penser à ce cas particulier. Et 1 n'est pas premier.
- En algèbre modulaire, on ne manipule jamais de grande valeur : penser à réduire systématiquement pour se ramener dans $[\![0, n-1]\!]$ (voire $\left[\!\left[\frac{-n}{2}, \frac{n}{2}\right]\!\right]$...)

32 **CCINP 86 - 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 $n \in \mathbb{Z}$, $(21n + 4) \wedge (14n + 3) = 1$.

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.

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 $5^4 \times 2^{28} \equiv 1 \ [641]$.

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 : $2^{136\,279\,841} - 1$ a été découvert le 21 octobre 2024 (41 024 320 chiffres en base décimale).

5. Ils interviennent dans la constructibilité à la règle et au compas des polygones réguliers.

(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.

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].

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

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

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

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

42 **Oral Centrale** Déterminer le chiffre des unité de 1587^{413}.

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

44 **Oral Mines**

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

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

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

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

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 $de \equiv 1\ [(p-1)(q-1)]$. 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.

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 $y = 2y'$, $X = \frac{z+x}{2}$ et $Z = \frac{z-x}{2}$.
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

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

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

9. Rivest, Shamir et Adleman, 1979