# Corrigé partiel du T. D. B4
# Arithmétique

**1** Décomposer en produit de facteurs premiers :

$a = 10!$ $b = 20!$ $c = \binom{20}{7}$ $d = \binom{50}{12}$

$a = 2^8 \times 3^4 \times 5^2 \times 7$
$b = 2^{18} \times 3^8 \times 5^4 \times 7^2 \times 11 \times 13 \times 17 \times 19$
$c = 2^4 \times 3 \times 5 \times 17 \times 19$
$d = 2^2 \times 5^2 \times 7^2 \times 13 \times 23 \times 41 \times 43 \times 47$

**2** Décomposer en produit de facteurs premiers les entiers $a = 2\,613\,600$ et $b = 4\,306\,500$. Calculer ensuite leur PGCD, et la décomposition en facteurs premier de leur PPCM.

$2\,613\,600 = 2^5 \times 3^3 \times 5^2 \times 11^2$
$4\,306\,500 = 2^2 \times 3^3 \times 5^3 \times 11 \times 29$
Leur PGCD est $2^2 \times 3^3 \times 5^2 \times 11 = 29\,700$
Leur PPCM est $2^5 \times 3^3 \times 5^3 \times 11^2 \times 29$

**3** Donner des coefficients de Bézout pour les $n$-uplets :

a. $(24, 35)$ b. $(55, 143)$ c. $(101, 120)$
d. $(6, 10, 15)$ e. $(60, 70, 105)$ f. $(10n + 3, 7n + 2)$

Par exemple :

a. $11 \times 35 - 16 \times 24 = 1$
b. $2 \times 143 - 5 \times 55 = 11$
c. $16 \times 120 - 19 \times 101 = 1$
d. $1 \times 6 - 2 \times 10 + 1 \times 15 = 1$
e. $3 \times 60 - 10 \times 70 + 5 \times 105 = 5$
f. $7(10n + 3) - 10(7n + 2) = 1$ grâce à l'algorithme d'Euclide.

**4** Démontrer que si $p$ est un nombre premier strictement supérieur à 3 alors $p^2 - 1$ est multiple de 24.

Comme $p$ est un nombre premier strictement supérieur à 3 alors il n'est pas congru à 0 modulo 2 ni modulo 3.
Ainsi $p \equiv \pm 1$ ou $\pm 3$ [8] donc $p^2 \equiv 1$ [8].
De plus $p \equiv \pm 1$ [3] donc $p^2 \equiv 1$ [3].
Ceci montre que $3 \mid p^2 - 1$ et $8 \mid p^2 - 1$, donc $3 \vee 8 \mid p^2 - 1$, soit $24 \mid p^2 - 1$.
En conclusion : $p^2 \equiv 1$ [24].

**5** Démontrer que pour tout $n \in \mathbb{N}$ :

a. $n^3 - n$ est multiple de 6.
b. $n^3 + (n+1)^3 + (n+2)^3$ est un multiple de 9.

a. On peut remarquer que $n^3 - n = (n-1)n(n+1)$.
L'un des facteurs $(n-1)$, $n$, $(n+1)$ est multiple de 3, et au moins un est pair. Donc le produit est multiple de 6.
On peut aussi utiliser le petit théorème de Fermat : comme 2 et 3 sont premiers alors $n^2 \equiv n$ [2] et $n^3 \equiv n$ [3]. Ceci montre que 2 divise $n^2 - n$, et 3 divise $n^3 - n$. Comme $n^3 - n = (n+1)(n^2 - n)$ alors 2 divise $n^3 - n$.
Finalement 2 et 3 divisent $n^3 - n$, donc 6 divise $n^3 - n$.
Enfin, on peut aussi écrire toutes les possibilités pour $n$ modulo 6.
b. On calcule $3n^3 + 9n^2 + 15n + 9 = 3n(n^2+5) + 9(n^2+1)$.
D'après le a. : $n(n^2+5) \equiv n(n^2-1) \equiv 0$ [3].
Ceci donne le résultat.
On peut aussi raisonner par récurrence.

**8** Résoudre les équations suivantes, où les inconnues sont des entiers relatifs.

| | | |
|---|---|---|
| a. $3m + 7n = 0$ | b. $3m + 7n = 32$ | c. $15m + 11n = 3$ |
| d. $6m + 15n = 40$ | e. $6m + 15n = 39$ | f. $28m + 66n = 40$ |
| g. $2m + 3n + 5p = 0$ | h. $2m + 3n + 5p = 1$ | |

$\mathcal{S}_a = \{(7k, -3k) \mid k \in \mathbb{Z}\}$
$\mathcal{S}_b = \{(7k-1, 5-3k) \mid k \in \mathbb{Z}\}$
$\mathcal{S}_c = \{(11k-2, 3-15k) \mid k \in \mathbb{Z}\}$
$\mathcal{S}_d = \varnothing$
$\mathcal{S}_e = \{(5k-1, 3-2k) \mid k \in \mathbb{Z}\}$
$\mathcal{S}_f = \{(33k-8, 4-14k) \mid k \in \mathbb{Z}\}$
$\mathcal{S}_g = \{(-p-3k, 2k-p, p) \mid (k,p) \in \mathbb{Z}^2\}$
$\mathcal{S}_h = \{(-p-3k-1, 2k-p+1, p) \mid (k,p) \in \mathbb{Z}^2\}$

**9** Résoudre les équations et systèmes d'équations suivants, d'inconnues entières.

a. $7n \equiv 16\,[18]$ b. $11n \equiv 7\,[27]$ c. $\begin{cases} n \equiv 2\,[5] \\ n \equiv 3\,[8] \end{cases}$

d. $\begin{cases} 3n \equiv 7\,[10] \\ 5n \equiv 1\,[9] \end{cases}$ e. $\begin{cases} n \equiv 1\,[3] \\ n \equiv 2\,[7] \\ n \equiv 3\,[8] \end{cases}$ f. $\begin{cases} 2m + 3n \equiv 1\,[17] \\ 11m + 13n \equiv 5\,[17] \end{cases}$

$\mathscr{S}_a = \{10 + 18k \mid k \in \mathbb{Z}\}$ $\mathscr{S}_b = \{8 + 27k \mid k \in \mathbb{Z}\}$ $\mathscr{S}_c = \{27 + 40k \mid k \in \mathbb{Z}\}$

$\mathscr{S}_d = \{29 + 90k \mid k \in \mathbb{Z}\}$ $\mathscr{S}_e = \{168k - 5 \mid k \in \mathbb{Z}\}$

$\mathscr{S}_f = \{(10 + 17k, 5 + 17\ell) \mid (k, \ell) \in \mathbb{Z}^2\}$

**10** Résoudre les équations suivantes, où l'inconnue est un entier relatif.

a. $n^2 + 4n + 6 \equiv 0\ [11]$ b. $n^2 - n + 3 \equiv 0\ [11]$ c. $3n^2 + 5n + 6 \equiv 0\,[13]$

d. $3n^2 + 5n + 10 \equiv 0\,[13]$ e. $n^2 + 3n - 1 \equiv 0\ [15]$ f. $n^2 - n - 12 \equiv 0\ [15]$

$\mathscr{S}_a = \{1, 6\}$ $\mathscr{S}_b = \{6\}$ $\mathscr{S}_c = \varnothing$

$\mathscr{S}_d = \{3, 4\}$ $\mathscr{S}_e = \varnothing$ $\mathscr{S}_f = \{4, 7, 9, 12\}$

**11** Déterminer tous les couples d'entiers naturels $(m, n)$ tels que :

a. $m \wedge n = 5$ et $m \vee n = 60$ b. $m \wedge n = 6$ et $m + n = 72$

c. $m \vee n = 2100$ et $m + n = 159$ d. $m \vee n = (m \wedge n)^2$ et $m + n = 70$

Soit $d = m \wedge n$, et $a = \frac{m}{d}$, $b = \frac{n}{d}$. Alors $a$ et $b$ sont entiers et d'après le lemme de réduction des rationnels $a$ et $b$ sont premiers entre eux.

a. On otient $ab = 12$ avec $a \wedge b = 1$, soit $\{a, b\} = \{1, 12\}$ ou $\{a, b\} = \{3, 4\}$.
Finalement : $\mathscr{S}_a = \{\{5, 60\}, \{15, 20\}\}$.

b. On obtient $a + b = 12$ avec $a \wedge b = 1$, soit $\{a, b\} = \{1, 11\}$ ou $\{a, b\} = \{5, 7\}$.
Finalement : $\mathscr{S}_b = \{\{6, 66\}, \{30, 42\}\}$.

c. On démontre que $m \wedge n = 3$, puis on obtient $ab = 700$ avec $a + b = 53$ et $a \wedge b = 1$.
Finalement : $\mathscr{S}_c = \{\{75, 84\}\}$.

d. On aboutit à $ab(a + b) = 70 = 2 \times 5 \times 7$ avec $a \wedge b = 1$.
Finalement : $\mathscr{S}_d = \{\{20, 50\}\}$.

**12** Soit $a$ et $b$ deux entiers tels que $0 < b < a$.

a. Démontrer que pour tout $n \in \mathbb{N}$ : $a - b$ divise $a^n - b^n$.

b. Démontrer que pour tout $(m, n) \in \mathbb{N}^2$ : si $m$ divise $n$ alors $a^m - b^m$ divise $a^n - b^n$.

c. Soit $a$ et $n$ deux entiers tels que $a \geqslant 2$ et $n \geqslant 2$. Démontrer que si $a^n - 1$ est premier, alors $a = 2$ et $n$ est premier.

d. Pour tout $p$ premier on note $M_p = 2^p - 1$.

Donner quatre nombres $M_p$ premiers.

Ces nombres sont appelés *nombres premiers de Mersenne*.

a. Comme $a \equiv b \ [a-b]$ alors $a^n \equiv b^n \ [a-b]$, donc $a - b$ divise $a^n - b^n$.

On peut aussi écrire $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$.

d. Si $p = 2$, $p = 3$, $p = 5$, $p = 7$ alors $M_p$ est premier.

Pour $p = 11$ on obtient $M_p = 2\,047 = 23 \times 89$, $M_p$ n'est pas premier.

Pour $p = 13$ on obtient $M_p = 8\,191$ qui est premier.

On connaît actuellement 48 nombres de Mersenne premiers, dont le plus grand nombre premier connu : $2^{136\,279\,841} - 1$ (12 octobre 2024), il comporte 41 024 320 chiffres.

**13** Pour tout entier $p$ premier on note $M_p = 2^p - 1$. Un entier $m$ est dit *parfait* si la somme de ses diviseurs autres que lui-même est égale à $m$.

a. Démontrer que si $M_p$ est premier, alors $2^{p-1}M_p$ est parfait.

On démontre dans la suite une réciproque, due à Euler : tout nombre parfait pair est de la forme $2^{p-1}M_p$ où $p$ et $M_p$ sont premiers.

Soit $m$ un nombre parfait pair.

b. Justifier qu'il existe $k \in \mathbb{N}^*$ et $u \in \mathbb{N}$ impair tels que $m = 2^k u$.

c. Soit $d_1, \ldots, d_r$ les diviseurs de $u$ et $\sigma$ leur somme. Démontrer que $2m = \left(2^{k+1} - 1\right)\sigma$.

d. Démontrer qu'il existe un entier $v$ tel que $u = (2^{k+1} - 1)v$.

e. Justifier que si $v > 1$ alors $\sigma \geqslant 1 + v + u$.

En déduire une contradiction.

f. Conclure.

On ne connaît aucun nombre parfait impair.

a. On obtient 6, 28, 496 et 8128. le suivant est 33 550 336.

d. Lemme de Gauss : $(2^{k+1} - 1)$ divise $u$.

e. Si $v > 1$ alors 1, $v$ et $u$ sont trois diviseurs distincts de $u$. On ne peut avoir $v = u$ car $k > 0$.

Comme $2m = 2^{k+1}u$ et $u + v = 2^{k+1}v$ on en déduit la contradiction $2^{k+1}v \geqslant 1 + 2^{k+1}v$.

f. Ainsi $v = 1$ puis $m = 2^k(2^{k+1} - 1)$ donc $m = 2^k M_{k+1}$ et $u = M_{k+1}$. Enfin $2m = (2^{k+1} - 1)\sigma$ montre que $\sigma = 2^{k+1}$, or $\sigma$ est la somme des diviseurs de $u = 2^{k+1} - 1$, ce qui montre que $u$ est premier. Donc $k + 1$ est premier. On pose $p = k + 1$, ainsi $m = 2^{p-1}M_p$ avec $M_p$ (donc $p$) premier.

**14** Soit $a$, $b$, $n$ trois entiers avec $n$ non-nul.

Démontrer que si $a \equiv b\,[n]$ alors $a^n \equiv b^n\,[n^2]$.

On part de $a = b + kn$ avec $k \in \mathbb{Z}$. On développe $a^n$ grâce à la formule du binôme.
Autre méthode : on utilise

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

Comme $a \equiv b\ [n]$ alors $n$ divise $a - b$. De plus :

$$\sum_{k=0}^{n-1} a^k b^{n-1-k} \equiv \sum_{k=0}^{n-1} b^{n-1} \equiv nb^{n-1} \equiv 0\ [n]$$

Ainsi $n$ divise $(a-b)$ et $\displaystyle\sum_{k=0}^{n-1} a^k b^{n-1-k}$ donc $n^2$ divise $a^n - b^n$.

**15** Pour tout $n \in \mathbb{N}$ on note $u_n = 2^n - 1$.

a. Soit $(m, n) \in \mathbb{N}^*$. Démontrer que si $m$ divise $n$ alors $u_m$ divise $u_n$.

b. Soit $a$ et $b$ deux entiers avec $a > b > 0$, et soit $r$ le reste de la division euclidienne de $a$ par $b$.

Démontrer que $u_r$ est le reste de la division euclidienne de $u_a$ par $u_b$.

En déduire que $u_a \wedge u_b = u_b \wedge u_r$.

c. Déterminer $u_a \wedge u_b$.

a. Soit $k$ est l'entier tel que $n = km$.
Alors $2^m \equiv 1\ [2^m - 1]$ donc $2^{km} \equiv 1^k = 1\ [2^m - 1]$ et $2^m - 1$ divise $2^n - 1$.

b. On écrit $u_a = (2^{bq} - 1)2^r + 2^r - 1 = u_{bq}2^r + u_r$ avec $0 \leqslant u_r < u_b$.
Comme $u_{bq}$ divise $u_b$ alors il existe un entier $q'$ tel que :

$$u_a = q' u_b + u_r \qquad \text{avec} \qquad 0 \leqslant u_r < u_b.$$

Il s'agit de la division euclidienne de $u_a$ par $u_b$.
Le PGCD de $u_a$ et $u_b$ divise donc $u_r$. Or il divise $u_b$, donc il divise $u_b \wedge u_r$.
Le PGCD de $u_b$ et $u_r$ divise $u_a$. Or il divise $u_b$, donc il divise $u_a \wedge u_b$.
Par antisymétrie : $u_a \wedge u_b = u_b \wedge u_r$.

c. En utilisant l'algortihme d'Euclide : $u_a \wedge u_b = u_{a \wedge b}$

**16** Soit $a$ et $b$ deux entiers naturels non-nuls, $q$ et $r$ le quotient et le reste de la division euclidienne de $a-1$ par $b$.

Déterminer, pour tout $n \in \mathbb{N}^*$, le quotient et le reste de la division euclidienne de $ab^n - 1$ par $b^{n+1}$.

Par définition de la division euclidienne :

$$a - 1 = qb + r \qquad \text{avec} \qquad 0 \leqslant r \leqslant b - 1.$$

On en déduit :

$$ab^n - 1 = qb^{n+1} + (r+1)b^n - 1 \qquad \text{avec} \qquad 0 \leqslant (r+1)b^n - 1 \leqslant b^{n+1} - 1 < b^{n+1}$$

Par unicité de la division euclidienne, le reste et le quotient de la division euclidienne de $ab^n$ par $b^{n+1}$ sont respectivement $q$ et $(r+1)b^n - 1$.

**17** Soit $a$, $b$, $k$ trois entiers non-nuls.

Démontrer que :

$$ka \wedge kb = k(a \wedge b) \qquad \text{et} \qquad ka \vee kb = k(a \vee b)$$

Soit $d = a \wedge b$. Alors $kd$ divise $ka$ et $kb$, donc $kd$ divise $ka \wedge kb$.

Réciproquement, $ka \wedge kb$ divise $ka$ et $kb$ donc divise $auk + bvk$ pour tous entiers $u$ et $v$, donc $ka \wedge kb$ divise $dk = k(a \wedge b)$.

Pour le PPCM on peut utiliser $ab = (a \vee b)(a \wedge b)$, ou alors $a \vee b = \text{Min}\,(a\mathbb{N}^* \cap b\mathbb{N}^*)$.

Méthode directe : $ka \mid ka \vee kb$ donc $k \mid ka \vee kb$ et $ka \vee kb = kc$ pour un $c \in \mathbb{Z}$.

Alors $ka \mid kc$ donc $a \mid c$, de même $b \mid c$, donc $a \vee b \mid c$, puis $k(a \vee b) \mid kc = ka \vee kb$.

Réciproquement : $a \mid a \vee b$ donc $ka \mid k(a \vee b)$ et de même $kb \mid k(a \vee b)$, donc $ka \vee kb \mid k(a \vee b)$.

**18** Soit $a$, $b$, $n$ entiers naturels, avec $n > 0$.

a. Démontrer que si $a^n$ divise $b^n$ alors $a$ divise $b$.

b. Démontrer que pour tout $n \in \mathbb{N}$ :

$$(a \wedge b)^n = a^n \wedge b^n \quad \text{et} \quad (a \vee b)^n = a^n \vee b^n$$

a. Si $a^n \mid b^n$ alors pour tout $p$ premier $v_p(a^n) \leqslant v_p(b^n)$.

Ainsi $v_p(a) \leqslant v_p(b)$, ceci pour tout nombre premier $p$, donc $a$ divise $b$.

b. Pour tout $p$ premier :

$$v_p((a \wedge b)^n) = n\,\text{Min}\,(v_p(a), v_p(b)) = \text{Min}\,(v_p(a^n), v_p(b^n)) = v_p(a^n \wedge b^n)$$

Ceci montre que $(a \wedge b)^n = a^n \wedge b^n$.

On démontre de même la formule pour le PPCM, avec les maximums au lieu de minimums.

**19** a. Par combien de zéros se termine 1000! ?

b. Soit $n$ un entier naturel et $p$ un nombre premier. Démontrer que :

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

a. 1000! se termine par 249 zéros.

Pour ceci on calcule $v_5(1000!) = 249$ et $v_2(1000!) = 994$.

b. On commence par démontrer :

$$\forall n \in \mathbb{N} \qquad v_p(n!) = \left\lfloor \tfrac{n}{p} \right\rfloor + v_p\Big(\left\lfloor \tfrac{n}{p} \right\rfloor !\Big) \tag{1}$$

En effet $v_p(n!) = \sum_{k=1}^{n} v_p(k)$, mais si $k$ n'est pas multiple de $p$ alors $v_p(k) = 0$, donc :

$$v_p(n!) = \sum_{\substack{k=1 \\ p|k}}^{n} v_p(k)$$

Les multiples de $p$ inférieurs ou égaux à $n$ sont les $pj$ pour $j$ entier tel que $1 \leqslant j \leqslant \frac{n}{p}$, ce qui donne $j = 1, \dots, \left\lfloor \frac{n}{p} \right\rfloor$, donc :

$$v_p(n!) = \sum_{j=1}^{\lfloor \frac{n}{p} \rfloor} v_p(pj) = \sum_{j=1}^{\lfloor \frac{n}{p} \rfloor} (1 + v_p(j)) = \left\lfloor \tfrac{n}{p} \right\rfloor + \sum_{j=1}^{\lfloor \frac{n}{p} \rfloor} v_p(j) = \left\lfloor \tfrac{n}{p} \right\rfloor + v_p\Big(\left\lfloor \tfrac{n}{p} \right\rfloor !\Big)$$

La formule (1) est démontrée.

Soit maintenant $n \in \mathbb{N}$ fixé. On démontre par récurrence sur $r$ la propriété :

$$\forall r \in \mathbb{N} \qquad v_p(n!) = \sum_{k=1}^{r} \left\lfloor \tfrac{n}{p^k} \right\rfloor + v_p\Big(\left\lfloor \tfrac{n}{p^r} \right\rfloor !\Big) \tag{2}$$

L'initialisation est immédiate.

Pour l'hérédité il faut démontrer :

$$\forall (a,b) \in (\mathbb{N}^*)^2 \qquad \left\lfloor \frac{\lfloor \frac{n}{a} \rfloor}{b} \right\rfloor = \left\lfloor \tfrac{n}{ab} \right\rfloor$$

Pour ceci on considère les divisions euclidiennes :

$$n = aq + r \quad \text{avec} \quad 0 \leqslant r \leqslant a-1 \qquad q = bq' + r' \quad \text{avec} \quad 0 \leqslant r' \leqslant b-1$$

Alors $\quad n = abq' + br + r' \quad$ avec $\quad 0 \leqslant br + r' \leqslant ab - 1, \quad$ on en déduit :

$$\left\lfloor \tfrac{n}{ab} \right\rfloor = q' \qquad \text{et} \qquad \left\lfloor \frac{\lfloor \frac{n}{a} \rfloor}{b} \right\rfloor = \left\lfloor \tfrac{q}{b} \right\rfloor = q'$$

Ceci permet de conclure le raisonnement par récurrence, et donc la propriété (2) est démontrée.

Posons alors $m = \left\lfloor \log_p(n) \right\rfloor$, ce qui donne $p^m \leqslant n < p^{m+1}$, puis $1 \leqslant \frac{n}{p^m} < p$, donc $\left\lfloor \frac{n}{p^m} \right\rfloor < p$, et $v_p\Big(\left\lfloor \frac{n}{p^m} \right\rfloor !\Big) = 0$.

La propriété (2) pour $r = m$ donne alors le résultat.

**20** Résoudre les équations suivantes, d'inconnues $(m,n) \in \mathbb{N}^2$.

a. $m^2 = n^2 + 1$ b. $m^2 = n^2 + 6$ c. $m^2 = n^2 + 7$ d. $m^2 = n^2 + 40$

e. $3^m + 1 = n^2$ f. $3^m - 1 = n^2$ g. $m^3 + m = n^2$ h. $m^3 - m = n^2$

i. $m^3 = n^3 + 218$ j. $m^3 = n^3 + 999$

$\mathscr{S}_a = \{(1,0)\}$ $\mathscr{S}_b = \varnothing$ $\mathscr{S}_c = \{(4,3)\}$ $\mathscr{S}_d = \{(11,9),(7,3)\}$

$\mathscr{S}_e = \{(1,2)\}$ $\mathscr{S}_f = \{(0,0)\}$ $\mathscr{S}_g = \{(0,0)\}$ $\mathscr{S}_h = \{(0,0),(1,0)\}$

$\mathscr{S}_i = \{(7,5)\}$ $\mathscr{S}_j = \{(12,9),(10,1)\}$

a. L'équation équivaut à $(m-n)(m+n) = 1$ avec $m$ et $n$ entiers naturels.
Donc $m+n = m-n = 1$, ce qui donne $m = 1$ et $n = 0$.

b. L'équation équivaut à $(m-n)(m+n) = 6$ avec $m$ et $n$ entiers naturels.
On remarque que $m+n$ et $m-n$ ont même parité, car $m - n \equiv m + n \ [2]$.
Ainsi $(m-n)(m+n)$ est impair ou multiple de 4, donc ne peut valoir 6.

c. On obtient $m+n = 7$ et $m-n = 1$, donc $m = 4$ et $n = 3$.

d. On obtient $(m-n)(m+n) = 40$, sachant que $m$ et $n$ ont même parité, et $m-n \leqslant m+n$.
Donc $m-n$ et $m+n$ sont multiples de 2.
Le couple $(m-n, m+n)$ peut prendre les valeurs $(2,20)$ et $(4,10)$, donc $(m,n) = (11,9)$ ou $(m,n) = (7,5)$.

e. L'équation donne $3^m = (n-1)(n+1)$, donc $n-1$ et $n-1$ sont des puissances de 3.
De plus $n - 1 \geqslant 1$ donc $n + 1 \geqslant 3$. On en déduit $n + 1 \equiv 0 \ [3]$, puis $n - 1 \equiv 1 \ [3]$.
En conséquence $n - 1 = 1$ puisque $n - 1$ est une puissance de 3, donc $n = 2$, puis $m = 1$.

f. Les valeurs de $n^2$ modulo 3 sont 0 et 1, donc celles de $n^2 + 1$ sont 1 et 2.
Or $3^m = n^2 + 1$, donc $3^m = 1$, puis $m = 0$ et $n = 0$.

g. Si $m = 0$ ou $n = 0$ alors $m = n = 0$.
Sinon : soit $d = m \wedge n$, puis $a = \frac{m}{d}$ et $b = \frac{n}{d}$. Alors $a$ et $b$ sont des entiers premiers entre eux.
L'équation donne $d^2a^3 + a = db^2$.
Ceci montre que $d$ divise $a$ et $a$ divise $d$ (d'après le lemme d'Euclide, car $a$ divise $db^2$ et $a$ est premier avec $b$).
Donc $a = d$, puis $m = d^2$ et $d^4 + 1 = b^2$. D'après la question a ceci donne $a = 0$ et $b = 1$, alors que $m$ est supposé non-nul.
Donc $(0,0)$ est la seule solution.

h. Le couple $(0,0)$ est solution. Si $(m,n) \neq (0,0)$ on procède comme ci-dessus, on obtient $d^4 - 1 = b^2$, donc $d = 1$ et $b = 0$, ce qui ajoute la solution $(1,0)$.

i. L'équation donne $(m-n)(m^2+mn+n^2) = 218 = 2 \times 109$ avec 109 premier.
Comme $m^3 = n^2 + 218$ alors $m > 216 = 6^3$, et $m^2 + mn + n^2 > 36$, donc $m - n$ peut prendre les valeurs 1 ou 2.

Si $m-n=1$ alors $m^2+mn+n^2=218$ et $m^2+mn+n^2=3n^2+3n+1$ ce qui est impossible car 217 n'est pas multiple de 3.

Si $m-n=2$ alors $m^2+mn+n^2=109$ et $m^2+mn+n^2=3n^2+6n+4$ ce qui donne $n^2+2n-35=0$, soit $n=5$ ou $n=-7$, donc $n=5$ car $n$ est positif, puis $m=7$.

j. De la même façon on obtient l'équation $(m-n)(m^2+mn+n^2)=999=3^3\times 37$, avec $m^2+mn+n^2\geqslant 100$, donc $m-n$ peut prendre les valeurs 1, 3, 9 ou 27.

Si $m-n=a$ alors $3an^2+3a^2n+a^3=999$, ce qui montre que $a$ est multiple de 3.

On pose $a=3b$ et on obtient $bn^2+3b^2n+3b^3=111$.

En testant $b=1$, $b=3$ et $b=9$ on obtient les deux solutions $(m,n)=(12,9)$ et $(m,n)=(10,1)$.

**21** Soit $a$ et $b$ deux entiers naturels strictement supérieurs à 1.

Démontrer que si $a$ et $b$ sont premiers entre eux alors $\frac{\ln a}{\ln b}$ est irrationnel.

On raisonne par l'absurde.

Comme $a$ et $b$ sont strictement supérieurs à 1 alors $\frac{\ln a}{\ln b}$ est strictement positif.

S'il est rationnel alors il existe deux entiers $m$ et $n$ strictement positifs tels que $\frac{\ln a}{\ln b}=\frac{m}{n}$.

Ceci donne $n\ln a=m\ln b$ donc $a^n=b^m$.

Comme $a$ et $b$ sont premiers entre eux alors aucun nombre premier ne peut diviser à la fois $a^n$ et $b^m$, donc $a^n=b^m=1$, puis $a=b=1$.

Cette contradiction montre que $\frac{\ln a}{\ln b}$ est irrationnel.

**22** Démontrer que l'équation $x^3+x=1$ admet une et une seule solution dans $\mathbb{R}$, puis que cette solution est irrationnelle.

La fonction $f:x\mapsto x^3+x$ est strictement croissante sur $\mathbb{R}$ et continue, donc elle réalise une bijection de $\mathbb{R}$ dans $\mathbb{R}$.

Ainsi l'équation $f(x)=1$ admet une et une seule solution réelle $\alpha$.

Si $\alpha=\frac{a}{b}$ est racine avec $a$ et $b$ entiers premiers entre eux, alors $a^3+ab^2=b^3$.

D'après le lemme d'Euclide tout nombre premier divisant $a$ divise $b$ et réciproquement. Donc $a=b=1$. Or 1 n'est pas solution, donc cette contradiction montre que $\alpha$ est irrationnel.

**23**

a. Soit $x$ un réel et $r$ un rationnel. Démontrer que si $x+r$ et irrationnel alors $x$ est irrationnel, et si $rx$ est irrationnel alors $x$ est irrationnel.
b. Soit $x$ un réel. Démontrer que s'il existe $n \in \mathbb{N}^*$ tel que $x^n$ est irrationnel alors $x$ est irrationnel.
c. Soit $p$ un nombre premier. Démontrer que $\sqrt{p}$ est irrationnel.
d. Soit $n$ un entier naturel. Démontrer que $\sqrt{n}$ est entier ou irrationnel.
e. Démontrer que $\sqrt{2}+\sqrt{3}$ et $\sqrt[3]{2}+\sqrt[3]{3}$ sont irrationnels.
f. Démontrer que $\sqrt{2}+\sqrt{3}+\sqrt{5}$ est irrationnel.
g. Démontrer que $\sqrt{2}+\sqrt[3]{2}$ est irrationnel.

a. On raisonne par contraposée, sachant que la somme et le produit de deux rationnels sont rationnels.
b. De même, si $x$ est rationnel alors pour tout $n \in \mathbb{N}^*$ $x^n$ est rationnel.

   Par contraposé, si il existe $n \in \mathbb{N}^*$ tel que $x^n$ est irrationnel alors $x$ est irrationnel.
c. S'il existe $(a,b) \in (\mathbb{N}^*)^2$ tel que $\sqrt{p} = \frac{a}{b}$ alors $2v_p(a) = 2v_p(b)+1$, ce qui donne la contradiction $0 \equiv 1$ [2].
d. S'il existe $(a,b) \in (\mathbb{N}^*)^2$ tel que $\sqrt{n} = \frac{a}{b}$ alors pour tout $p$ premier : $2v_p(a) = 2v_p(b) + v_p(n)$.

   Donc $v_p(n)$ est pair pour tout $p$ premier, ce qui montre que $n$ est un carré et donc $\sqrt{n}$ est entier.

   Ainsi $\sqrt{n}$ est entier ou irrationnel.
e. Soit $x = \sqrt{2}+\sqrt{3}$. Alors $x^2 = 5+2\sqrt{6}$. Si $x$ est rationnel alors $\sqrt{6}$ est rationnel, ce qui est faux d'après la question précédente.

   Soit $y = \sqrt[3]{2}+\sqrt[3]{3}$. Alors $y^3 = 5+3\sqrt[3]{6}y$. Si $y$ est rationnel alors $\sqrt[3]{6}$ est rationnel.

   On en déduit une contradiction grâce à la valuation 2-adique.
f. Posons $x = \sqrt{2}+\sqrt{3}+\sqrt{5}$. Alors $x$ est non-nul.

   De plus $\sqrt{2}+\sqrt{3} = x-\sqrt{5}$, ce qui donne en élevant au carré $2\sqrt{6} = x^2 - 2x\sqrt{5}$, puis en élevant encore au carré $24 = x^4 + 20x^2 - 4x^3\sqrt{5}$.

   Si $x$ est rationnel, comme $x$ est non-nul alors par somme et quotient $\sqrt{5}$ est rationnel, ce qui est faux. Donc $x$ est irrationnel.
g. Soit $x = \sqrt{2}+\sqrt[3]{2}$. Alors $\sqrt[3]{2} = x-\sqrt{2}$, ce qui donne en élevant au cube :

$$2 = x^3 - 3\sqrt{2}x^2 + 6x - 2\sqrt{2} = x^3 + 6x - (3x^2+2)\sqrt{2}.$$

   Comme $3x^2+2$ est non-nul alors :

$$\sqrt{2} = \frac{x^3+6x-2}{3x^2+2}$$

   Si $x$ est rationnel alors par produit, somme et quotient $\sqrt{2}$ est rationnel, ce qui est faux. Donc $x$ est irrationnel.