Diviseurs

Exercice 1. Nombre de diviseurs. *Soit a un entier naturel qui s'écrit $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, où $p_1, \dots, p_r$ sont des entiers premiers distincts et $\alpha_1, \dots, \alpha_r$ des entiers naturels. Combien a possède t-il de diviseurs positifs ?*

Correction. *Les diviseurs de a sont de la forme $p_1^{\beta_1} \dots p_r^{\beta_r}$ avec $0 \leq b_i \leq \alpha_i$ donc pour tout $i \in [\![1, r]\!]$, on a $\alpha_i + 1$ choix pour b_i.*

Conclusion : $\boxed{a \text{ possède } \prod_{i=1}^{r}(1+\alpha_i) \text{ diviseurs positifs}}$.

Exercice 2. Carré parfait. *Soit n un entier naturel qui s'écrit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, où $p_1, \dots, p_r$ sont des entiers premiers distincts et $\alpha_1, \dots, \alpha_r$ des entiers naturels.*
À quelle condition nécessaire et suffisante n est-il un carré parfait, c'est-à-dire s'écrit-il m^2, avec $m \in \mathbb{N}$?

Correction.

- *Supposons qu'il existe $m \in \mathbb{N}^2$ tel que $n = m^2$. Alors $m|n$ donc les diviseurs premiers de m divisent n, donc sont inclus dans $\{p_1, \dots, p_r\}$, et il existe des entiers naturels $\beta_i \leq \alpha_i$ tels que $m = p_1^{\beta_1} \dots p_r^{\beta_r}$. On a alors :*
$$n = m^2 = p_1^{2\beta_1} \dots p_r^{2\beta_r}.$$
Par unicité de la décomposition en produit de nombres premiers de n, on a pour tout $i \in [\![1, r]\!]$, $\alpha_i = 2\beta_i$, donc α_i est pair.
- *Réciproquement, si pour tout i, α_i est pair, on pose $m = \prod_{i=1}^{r} p_i^{\alpha_i/2}$, de sorte que $n = m^2$ avec $m \in \mathbb{N}$ donc n est un carré parfait.*
- *Conclusion :* $\boxed{n \text{ est un carré parfait ssi pour tout } i \in [\![1, r]\!], \alpha_i \text{ est pair}}$.

Exercice 3. *Trouver tous les entiers $n > 0$ tels que $n^2 + 1$ est divisible par $n + 1$.*

Correction. *Soit $n \in \mathbb{N}^*$. On écrit*
$$n^2 + 1 = (n+1)(n-1) + 2,$$
donc $n + 1$ divise $n^2 + 1$ si et seulement si $n + 1$ divise 2.
Comme $2 \neq 0$, on sait que les diviseurs de 2 sont en valeur absolue ≤ 2.
Ici, $n + 1 \geq 2$, donc $n + 1$ divise 2 si et seulement si $n + 1 = 2$, i.e. si $\boxed{n = 1}$.
On a donc l'équivalence : $\boxed{n + 1 \text{ divise } n^2 + 1 \text{ si et seulement si } n = 1.}$

Exercice 4. *Déterminer les entiers $n \in \mathbb{N}$ tels que $n-3$ divise n^3-3.*

Correction. *On écrit*

$$\forall n \in \mathbb{N},\ n^3-3 = (n-3)(n^2+3n+9)+24,$$

donc $n-3$ divise n^3-3 si et seulement si $n-3$ divise 24.
Connaissant les diviseurs positifs de 24, on a $n-3 \in \{1,2,3,4,6,8,12,24\}$ puis $\boxed{n \in \{4,5,6,7,9,11,15,27\}}$.

Exercice 5. *Soit $(a,b) \in \mathbb{Z}^2$ tel que 7 divise a^2+b^2. Montrer que 7 divise a et b.*

On pourra utiliser un tableau de congruences.

Correction.

- *Les D.E. de a et b par 7 (qui est non nul) assurent que a et b sont congrus à un entier dans $[\![0,6]\!]$ modulo 7, donc à $0, \pm 1, \pm 2$ ou ± 3 $(\mathrm{mod}\ 7)$.*
- *Par propriétés des congruences, a^2 et b^2 sont congrus à 0^2, 1^2, 2^2 ou 3^2 $(\mathrm{mod}\ 7)$, c'est-à-dire à 0, 1, 4, 2 $(\mathrm{mod}\ 7)$.*
- *On a plus précisément :*

a	0	1	2	3	-3	-2	-1
a^2	0	1	4	2	2	4	1

. De même pour b.

- *En faisant un tableau à double entrée, on se rend compte que*

$$a^2+b^2 \equiv 0 \pmod 7 \iff (a^2 \equiv 0 \text{ et } b^2 \equiv 0 \pmod 7).$$

D'après le tableau précédent, $a^2 \equiv 0 \pmod 7 \iff a \equiv 0 \pmod 7$ donc

$$a^2+b^2 \equiv 0 \pmod 7 \iff (a \equiv 0 \text{ et } b \equiv 0 \pmod 7).$$

En particulier, l'implication directe répond à la question posée.

Exercice 6. *Les questions suivantes sont indépendantes. A l'aide de la formule du binôme, montrer que :*

1. *pour tout $n \in \mathbb{N}^*$, n^2 divise $(n+1)^n-1$.*

   Correction. *Soit $n \in \mathbb{N}^*$. On écrit :*

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

   Or, pour tout $k \in [\![2,n]\!]$, n^2 divise n^k donc n^2 divise $\displaystyle\sum_{k=2}^{n} \binom{n}{k} n^k$, donc $\boxed{n^2 \text{ divise } (n+1)^n-1}$.

2. *pour tout $n \in \mathbb{N}^*$, 2^n+1 est divisible par 3 si, et seulement si, n est impair.*

Correction. *Soit $n \in \mathbb{N}^*$. Une astuce consiste à écrire $2 = 3 - 1$. Ainsi,*

$$2^n = (3-1)^n = \sum_{k=0}^{n} \binom{n}{k} 3^k (-1)^{n-k} = (-1)^n + 3p, \text{ avec } p = \sum_{k=1}^{n} \binom{n}{k} 3^{k-1}(-1)^{n-k} \in \mathbb{Z}.$$

Faisons une disjonction de cas selon la parité de n.

- *Si n est impair, alors l'égalité précédente s'écrit $2^n + 1 = 3p$ donc $2^n + 1$ est divisible par 3.*
- *Si n est pair, alors $2^n - 1 = 3p$ donc $2^n + 1 = 3p + 2$ (il s'agit de la division euclidienne de $2^n + 1$ par 3, et son reste est non nul), donc $2^n + 1$ n'est pas divisible par 3.*

Ainsi, $\boxed{2^n + 1 \text{ est divisible par 3 si, et seulement si, } n \text{ est impair}}$.

3. *pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{4n+2}$ est divisible par 7.*

Correction. *Soit $n \in \mathbb{N}$. Remarquons que $2^{4n+2} = 4^{2n+1}$ et écrivons $3 = 7 - 4$. Alors*

$$3^{2n+1} = (7-4)^{2n+1} = \sum_{k=0}^{2n+1} \binom{2n+1}{k} 7^k (-4)^{2n+1-k} = (-4)^{2n+1} + 7p,$$

avec $p = \sum_{k=1}^{2n+1} \binom{2n+1}{k} 7^{k-1}(-4)^{2n+1-k} \in \mathbb{Z}$.
Ainsi, $3^{2n+1} + 2^{4n+2} \in 7\mathbb{Z}$ donc $\boxed{3^{2n+1} + 2^{4n+2} \text{ est divisible par } 7}$.

Exercice 7. *Soit p un nombre premier supérieur ou égal à 5. Montrer que 24 divise $p^2 - 1$.*

Correction.

- *Écrivons : $24 = 3 \times 8$ et $p^2 - 1 = (p-1)(p+1)$.*
- *$p \geq 5$ et p est premier donc p est impair puis $p-1$ et $p+1$ sont pairs. Ainsi, $4|(p^2-1)$.*
  Mieux : quand on a deux nombres pairs consécutifs, l'un des deux (exactement) est divisible par 4. Donc
  $$(4|(p-1) \text{ et } 2|(p+1)) \text{ ou } (4|(p+1) \text{ et } 2|(p-1)).$$
  Dans tous les cas, $\underline{8|(p^2-1)}$.

  > *En effet, on peut trouver $a \in \mathbb{N}^*$ tel que $p - 1 = 2a$, donc $p + 1 = 2a + 2 = 2(a+1)$ donc $(p-1)(p+1) = 4a(a+1)$, où a et $a+1$ sont deux entiers consécutifs, donc l'un (exactement) des deux est pair, donc $2|a(a+1)$ d'où $8|4a(a+1)$.*

- *$p-1, p, p+1$ sont consécutifs donc l'un des trois est multiple de 3. Or, p est premier et $p > 3$ donc 3 ne divise pas p. Ainsi, 3 divise $p-1$ ou $p+1$. Dans tous les cas, $\underline{3|(p^2-1)}$.*
- *En conclusion, $3|(p^2-1)$, $8|(p^2-1)$ et $3 \wedge 8 = 1$ donc $\boxed{24|(p^2-1)}$ (on utilise ici la propriété n°5 de l'exercice 9).*
  Alternative. *On a $3|(p^2-1)$, $2^3|(p^2-1)$ et 2 et 3 sont des nombres premiers distincts, donc leur*

produit divise (p^2-1) (on utilise ici le corollaire du théorème fondamental de l'arithmétique).

Exercice 8. *Montrer que pour $n \in \mathbb{N}^*$, on a $169 | 3^{3n+3} - 26n - 27$.*

Correction. *Remarquons que $169 = 13^2$ et $3^{3n+3} = 27^{n+1}$.*
Première preuve (par récurrence). *Pour tout $n \in \mathbb{N}^*$, on note $\mathscr{P}(n)$: « $169 | 27^{n+1} - 26n - 27$ ».*

- $27^2 - 26 - 27 = 27 \times 26 - 26 = 26 \times 26 = 13^2 \times 4 = 169 \times 4$ *donc* $\mathscr{P}(1)$.
- *Soit $n \in \mathbb{N}^*$ tel que $\mathscr{P}(n)$.*
  Alors il existe $k \in \mathbb{N}$ tel que $27^{n+1} - 26n - 27 = 169k$.

$$\begin{aligned} 27^{n+2} - 26(n+1) - 27 &= 27(169k + 26n + 27) - 26(n+1) - 27 \\ &= 169 \times 27k + 26n(27-1) + 27(27-1) - 26 \\ &= 169 \times 27k + 26^2 n + 27 \times 26 - 26 \\ &= 169 \times 27k + 26^2 n + 26^2 \\ &= 169 \times 27k + 169 \times 4n + 169 \times 4 \\ &= 169(\underbrace{27k + 4n + 4}_{\in \mathbb{N}}). \end{aligned}$$

On a $\mathscr{P}(n+1)$, ce qui montre l'hérédité et conclut la récurrence.

Deuxième preuve (directe). *On écrit, pour tout $n \in \mathbb{N}^*$,*

$$\begin{aligned} 3^{3n+3} - 26n - 27 &= 27^{n+1} - 27 - 26n \\ &= 27 \times (27^n - 1) - 26n \\ &= 27 \times 26 \times (1 + 27 + 27^2 + \cdots + 27^{n-1}) - 26n \\ &= 26 \times \left[27 \times (1 + 27 + 27^2 + \cdots + 27^{n-1}) - n \right]. \end{aligned}$$

Or, la parenthèse est congrue à n modulo 26^*, donc le crochet est un multiple de 26 (et donc de 13), et le nombre recherché est un multiple de $13^2 = 169$.

> *En effet, $a \equiv b\ [n]$ et $c \equiv d\ [n]) \Longrightarrow ac \equiv bd\ [n]$, donc $\forall k \in \mathbb{N},\ a \equiv b\ [n] \Longrightarrow a^k \equiv b^k\ [n]$, et on peut aussi sommer dans des congruences.*

PGCD, PPCM

Exercice 9. Compléments de cours. *Soit $(a,b,c) \in (\mathbb{Z}^*)^3$. Démontrer les propriétés suivantes :*

1. **Homogénéité du PGCD** *:* $(ac) \wedge (bc) = |c|(a \wedge b)$.

Correction.
Méthode 1 (décomposition en facteurs premiers).

- *Si $(a,b,c) \in (\mathbb{N}^*)^3$, alors il existe $r \in \mathbb{N}$ et des nombres premiers $p_1 < \cdots < p_r$ tels que :*

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}, \ b = \prod_{i=1}^{r} p_i^{\beta_i} \quad et \quad c = \prod_{i=1}^{r} p_i^{\gamma_i},$$

avec pour tout $i \in [\![1,r]\!]$, $\alpha_i, \beta_i, \gamma_i \in \mathbb{N}$. Alors :

$$(ac) \wedge (bc) = \prod_{i=1}^{r} p_i^{\min(\alpha_i+\gamma_i, \beta_i+\gamma_i)} = \prod_{i=1}^{r} p_i^{\gamma_i + \min(\alpha_i,\beta_i)} = \prod_{i=1}^{r} p_i^{\gamma_i} \times \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)} = c(a \wedge b).$$

- *Dans le cas général,*

$$(ac) \wedge (bc) = |ac| \wedge |bc| = |a||c| \wedge |b||c| \underset{*}{=} |c|(|a| \wedge |b|) = |c|(a \wedge b),$$

*où * découle du premier cas.*

- **Alternative de rédaction.** *Comme $(a,b,c) \in (\mathbb{Z}^*)^3$, on peut les écrire*

$$a = \pm \prod_{i=1}^{r} p_i^{\alpha_i}, \ b = \pm \prod_{i=1}^{r} p_i^{\beta_i} \quad et \quad c = \pm \prod_{i=1}^{r} p_i^{\gamma_i}.$$

On sait que $(ac) \wedge (bc) = |ac| \wedge |bc|$, avec $|ac| = \prod_{i=1}^{r} p_i^{\alpha_i+\gamma_i}$ et $|bc| = \prod_{i=1}^{r} p_i^{\beta_i+\gamma_i}$,
donc, d'après la caractérisation du PGCD pour les entiers naturels écrits comme produits de nombres premiers, on a :

$$|ac| \wedge |bc| = \prod_{i=1}^{r} p_i^{\min(\alpha_i+\gamma_i, \beta_i+\gamma_i)} = \prod_{i=1}^{r} p_i^{\gamma_i + \min(\alpha_i,\beta_i)} = \prod_{i=1}^{r} p_i^{\gamma_i} \times \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)} = |c|(|a| \wedge |b|),$$

c'est-à-dire

$$\boxed{(ac) \wedge (bc) = |c|(a \wedge b)}.$$

Méthode 2 (avec l'algo d'Euclide).

Premier cas. *Si $(b,c) \in (\mathbb{N}^*)^2$, alors $bc \in \mathbb{N}^*$ et on peut faire la D.E. d'un entier par b et par bc. Si $a = bq + r_0$ avec $0 \leq r_0 < b$, alors $ca = cbq + cr_0$ avec $0 \leq cr_0 < cb$ (car $c > 0$) donc cr_0 est le reste de la division de ca par cb par unicité de l'écriture.*
En utilisant les notations de l'algorithme d'Euclide et en multipliant chaque membres des égalités par c, on obtient : $\text{pgcd}(ca, cb) = \text{pgcd}(cb, cr_0) = \cdots = cr_{m-1} = c\text{pgcd}(a,b)$.

Cas général. *Le même que précédemment.*

2. *Si $d = a \wedge b$, alors il existe $(a',b') \in (\mathbb{Z}^*)^2$ tel que $a' \wedge b' = 1$, $a = da'$ et $b = db'$.*

En déduire que tout nombre rationnel s'écrit sous **forme irréductible**.

Correction.

- *Posons $d = a \wedge b$. Par définition du PGCD, $d|a$ et $d|b$ donc l'existence de a' et b' est assurée. Par homogénéité du PGCD et puisque $a \wedge b \in \mathbb{N}$, on obtient $d = a \wedge b = (a'd) \wedge (b'd) = |d|(a' \wedge b') = d(a' \wedge b')$. Or $d \neq 0$, donc $a' \wedge b' = 1$.*
- *Soit $r \in \mathbb{Q}$.*

  Si $r = 0$, *alors on peut écrire $0 = \dfrac{0}{1}$ et $0 \wedge 1 = 1$.*

  Si $r \in \mathbb{Q}^*$, *alors il existe $(\alpha, \beta) \in (\mathbb{Z}^*)^2$ tel que $r = \dfrac{\alpha}{\beta}$.*

  Posons $d := \alpha \wedge \beta$. Alors il existe $(\alpha', \beta') \in (\mathbb{Z}^*)^2$ tel que $\alpha' \wedge \beta' = 1$, $\alpha = \alpha' d$ et $\beta = \beta' d$. Alors, $r = \dfrac{\alpha}{\beta} = \dfrac{\alpha'}{\beta'}$, où cette dernière fraction est irréductible.

3. **Lemme de Gauss** : $(a|bc \text{ et } a \wedge b = 1) \Longrightarrow a|c$.

Correction. *Supposons $a|bc$ et $a \wedge b = 1$.*
Bien sûr $a|ac$, donc $a|(ac \wedge bc)$. Or, par homogénéité du PGCD, on a $(ac) \wedge (bc) = |c|(a \wedge b) = |c|$.
Ainsi, a divise $|c|$ puis $\boxed{a|c}$.

4. $(a \wedge b = 1 \text{ et } a \wedge c = 1) \Longrightarrow a \wedge (bc) = 1$.

Correction. *Montrons que si a est premier avec b et c, alors a est premier avec le produit bc.*
Méthode 1. *L'hypothèse signifie que si a n'a pas de facteur premier en commun avec b et c alors il n'en a pas non plus avec le produit bc (en effet, on rappelle que si un nombre premier divise un produit, alors il divise l'un des facteurs du produit d'après le lemme d'Euclide).*
Méthode 1 bis (par contraposée). *Supposons $a \wedge (bc) \neq 1$. Alors il existe un diviseur premier p commun à a et bc. L'entier p est premier et divise bc donc d'après le lemme d'Euclide, p divise b ou c.*
Si p divise b, comme p divise aussi a, on en déduit que $a \wedge b \neq 1$; sinon, p divise c et a donc de même $a \wedge c \neq 1$.
On a donc montré que $a \wedge (bc) \neq 1 \Longrightarrow (a \wedge b \neq 1 \text{ ou } a \wedge c \neq 1)$.
Par contraposée, on a : $\boxed{(a \wedge b = 1 \text{ et } a \wedge c = 1) \Longrightarrow a \wedge (bc) = 1}$.
Méthode 2 (directe). *Supposons que $a \wedge b = 1$ et $a \wedge c = 1$. Soit $d \in \mathbb{Z}$ un diviseur commun à a et bc. Montrons que $d \in \{\pm 1\}$. A fortiori, $d|ac$ et $d|bc$ donc $d|(ac \wedge bc)$.*
Or, $(ac) \wedge (bc) = |c|(a \wedge b) = |c|$ donc d divise $|c|$ puis d divise c. De plus, d divise a donc d divise leur PGCD, qui vaut 1 par hypothèse. Ainsi, $d \in \{\pm 1\}$, et donc $\boxed{a \wedge (bc) = 1}$.

5. $(a|c \text{ et } b|c \text{ et } a \wedge b = 1) \Longrightarrow (ab)|c$.

Montrons que si a et b sont premiers entre eux et divisent tous les deux c, alors leur produit ab divise encore c.
Supposons que $a|c$ et $b|c$ et $a \wedge b = 1$.

- ***Méthode 0.*** *Conséquence du Théorème de Bézout (HP).*

Comme $a \wedge b = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. En multipliant par c, on obtient $acu + bcv = c$.
Or, $b|c$ donc on peut écrire $c = bb'$ avec $b' \in \mathbb{Z}$ et de même, on peut écrire $c = aa'$ avec $a' \in \mathbb{Z}$. Ainsi, $ab(b'u + a'v) = c$ avec $b'u + a'v \in \mathbb{Z}$ d'où $\boxed{ab|c}$.

- ***Méthode 1.*** *$a|c$ et $b|c$ impliquent que c est un multiple commun à a et b, donc $|c|$ est un multiple positif commun à a et b, et $a \vee b$ est le plus petit au sens de $\cdot|\cdot$ (et $\leq$), donc $(a \vee b)||c|$. Or, $a \wedge b = 1$ donc $a \vee b = |ab|$.*
Ainsi, ab divise $|ab|$, qui lui-même divise $|c|$, donc par transitivité ab divise $|c|$. En particulier $\boxed{ab|c}$.
- ***Méthode 2.*** *$a|c$ donc $ab|bc$. De même, $b|c$ donc $ab|ac$. Puis ab est un diviseur commun à ac et bc donc $(ab)|(ac \wedge bc)$. Par homogénéité du PGCD, on a : $ac \wedge bc = |c|(a \wedge b) = |c|$. Donc ab divise $|c|$ puis $\boxed{ab|c}$.*
- ***Méthode 3.*** *$a|c$ et $b|c$ donc il existe $(k, \ell) \in \mathbb{Z}^2$ tel que $c = ak$ et $c = b\ell$. Donc $c = ak = b\ell$. Ainsi, $a|b\ell$. Mais comme $a \wedge b = 1$, d'après le lemme de Gauss, on en déduit que $a|\ell$ donc $\ell = aq$, avec $q \in \mathbb{Z}$. Ainsi, $c = b\ell = abq$ donc $\boxed{(ab)|c}$.*
- ***Méthode 4 (avec des produits de facteurs premiers).***

6. **Homogénéité du PPCM** *: $(ac) \vee (bc) = |c|(a \vee b)$.*

Méthode 1. *D'après le cours,*

$$(ac \wedge bc)(ac \vee bc) = |a||b||c|^2 = |c|^2(a \wedge b)(a \vee b).$$

Or, par homogénéité du PGCD, on a : $ac \wedge bc = |c|(a \wedge b)$. On obtient alors :

$$|c|(a \wedge b)(ac \vee bc) = |c|^2(a \wedge b)(a \vee b).$$

Comme $|c|(a \wedge b) \neq 0$, on en déduit que $\boxed{ac \vee bc = |c|(a \vee b)}$.
Méthode 2 (décomposition en facteurs premiers).

- *Si $(a, b, c) \in (\mathbb{N}^*)^3$, alors il existe $r \in \mathbb{N}$ et des nombres premiers $p_1 < \cdots < p_r$ tels que :*

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}, \ b = \prod_{i=1}^{r} p_i^{\beta_i} \quad et \quad c = \prod_{i=1}^{r} p_i^{\gamma_i},$$

avec pour tout $i \in [\![1, r]\!]$, $\alpha_i, \beta_i, \gamma_i \in \mathbb{N}$. Alors :

$$(ac) \vee (bc) = \prod_{i=1}^{r} p_i^{\max(\alpha_i+\gamma_i, \beta_i+\gamma_i)} = \prod_{i=1}^{r} p_i^{\gamma_i+\max(\alpha_i,\beta_i)} = \prod_{i=1}^{r} p_i^{\gamma_i} \times \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)} = c(a \vee b).$$

- *Dans le cas général, $(ac) \vee (bc) = |a||c| \vee |b||c| = |c|(|a| \vee |b|) = |c|(a \vee b)$.*

7. $\forall (m, n) \in \mathbb{N}^2, \ (a \wedge b = 1 \Longrightarrow a^m \wedge b^n = 1)$.

Soit $(m, n) \in \mathbb{N}^2$. Par contraposée : Si $a^m \wedge b^n \neq 1$, alors a^m et b^n possèdent un diviseur premier p en commun. Comme p divise a^m et p est premier, on a que p divise a (lemme d'Euclide). De

même, p divise b. Ainsi p est un diviseur commun à a et b, donc $a \wedge b \neq 1$.

Exercice 10. Calculs de PGCD, PPCM.

1. *Pour $k \in \mathbb{N}$, déterminer $(2k+1) \wedge (9k+4)$.*
2. *Pour $n \in \mathbb{N}^*$, déterminer $n \vee (2n+1)$.*
3. *Pour $n > 2$, déterminer $(n-1) \vee (2n+1)$.*

Correction.

1. *Soit $k \in \mathbb{N}$. On écrit :*
$$9k+4 = (2k+1) \times 4 + k$$
$$2k+1 = k \times 2 + \boxed{1},$$
(la deuxième égalité n'est pas nécessairement une D.E. si $k \in \{0,1\}$, mais ce n'est pas grave...). Par théorème, on sait que $\boxed{(9k+4) \wedge (2k+1) = (2k+1) \wedge k = k \wedge 1 = 1}$.

2. *Soit $n \in \mathbb{N}^*$.*
• *Déterminons d'abord le PGCD.*
Méthode 1. *Un diviseur commun à $2n+1$ et n divise $2n+1-2n = 1$ donc vaut ± 1. Ainsi, $2n+1$ et n sont premiers entre eux donc $n \wedge (2n+1) = 1$.*
Méthode 2. *On écrit $2n+1 = n \times 2 + 1$ (si $n \geq 2$ il s'agit de la D.E. de $2n+1$ par n, si $n = 1$, non, mais ce n'est pas grave...). On sait alors que $(2n+1) \wedge n = n \wedge 1 = 1$.*
• *De plus, comme n et $2n+1$ sont non nuls, on sait que $\underbrace{(n \wedge (2n+1))}_{=1} \times (n \vee (2n+1)) = |\underbrace{n(2n+1)}_{\geq 0}|$,*
donc $\boxed{n \vee (2n+1) = n(2n+1)}$.

3. *Soit $n \geq 3$. Déterminons d'abord le PGCD. De l'égalité $2n+1 = 2(n-1)+3$, on déduit*
$$(n-1) \wedge (2n+1) = (n-1) \wedge 3 \in \{1, 3\}.$$
De plus, comme $(n-1) \wedge (2n+1) \neq 0$ et $(n-1)(2n+1) \geq 0$, on a
$$(n-1) \vee (2n+1) = \frac{(n-1)(2n+1)}{(n-1) \wedge (2n+1)}.$$
Distinguons deux cas.
   - *Si $n-1$ est multiple de 3, alors $(n-1) \wedge (2n+1) = 3$, ce qui donne :*
   $$\boxed{(n-1) \vee (2n+1) = \frac{(n-1)(2n+1)}{3}}.$$
   - *Sinon, $(n-1) \wedge (2n+1) = 1$, et donc $\boxed{(n-1) \vee (2n+1) = (n-1)(2n+1)}$.*

Exercice 11. PGCD. *Soit $(a,b) \in (\mathbb{Z}^*)^2$. Montrer que :*

1. $a \wedge b = 1 \implies (a+b) \wedge (ab) = 1$.
2. $(a^2+b^2) \wedge (ab) = (a \wedge b)^2$.

Correction.

1. *Par contraposée. Supposons que $a+b$ et ab ne soient pas premiers entre eux.*
Alors il existe un nombre premier p qui divise ab et $a+b$.
p est premier et divise ab, donc d'après le lemme d'Eucide, p divise a ou b.
Sans perte de généralité, supposons que p divise a. Comme p divise aussi $a+b$, p divise $(a+b)-a$ donc b. Donc $a \wedge b \neq 1$. On a montré que $(a+b) \wedge ab \neq 1 \implies a \wedge b \neq 1$ donc la contraposée est vraie.

2. - *On normalise le problème en posant $d := a \wedge b \neq 0$ (car $a \neq 0$). Dès lors, on peut écrire $a = a'd$, $b = b'd$, avec $a', b' \in \mathbb{Z}^*$ tels que $a' \wedge b' = 1$.*
   - *Par homogénéité du PGCD, on a :*

$$(a^2+b^2) \wedge ab = d^2(a'^2+b'^2) \wedge d^2a'b' = d^2[(a'^2+b'^2) \wedge a'b'].$$

Il suffit donc de montrer que $d' := (a'^2+b'^2) \wedge a'b' = 1$ pour conclure.

Première méthode. *Par définition, $d' | (a'^2+b'^2)$ et $d' | (a'b')$ donc aussi $d' | (a'b')^2$, donc d' divise $(a'^2+b'^2) \wedge (a'b')^2$.*
Or, $a' \wedge b' = 1$ donc $a'^2 \wedge b'^2 = 1$ et d'après la question 1 appliquée à a'^2 et b'^2, on a $(a'^2+b'^2) \wedge (a'b')^2 = 1$. Ainsi, d' divise 1 donc $d' = \pm 1$, mais comme $d' \geq 0$, on a finalement $d' = 1$, ce qui permet de conclure l'exercice.
Sinon : *considérer δ un diviseur commun à $(a'^2+b'^2)$ et $(a'b')$. Par les mêmes arguments, δ divise 1 donc $\delta = \pm 1$, ce qui prouve que $(a'^2+b'^2)$ et $a'b'$ sont premiers entre eux et conclut.*

Deuxième méthode.
- *D'après la question précédente, $(a'+b') \wedge a'b' = 1$ puis par application de l'exercice 9.7., on a : $(a'+b')^2 \wedge a'b' = 1$.*
- *Soit δ un diviseur commun à $a'^2+b'^2$ et $a'b'$. Puisque $(a'+b')^2 = (a'^2+b'^2)+2a'b'$, on en déduit que δ divise $(a'+b')^2$. Ainsi, δ divise $(a'+b')^2$ et $a'b'$ donc δ divise leur PGCD i.e. 1. Ainsi, $\delta = \pm 1$, ce qui prouve que $(a'^2+b'^2) \wedge a'b' = 1$.*

- *En conclusion : $(a^2+b^2) \wedge ab = d^2 = (a \wedge b)^2$.*

Exercice 12. Devinette. *Déterminer tous les entiers naturels non nuls a et b tels que $a+b = 4(a \wedge b)$.*

Correction. *Procédons par analyse-synthèse.*

- *Soit $(a,b) \in (\mathbb{N}^*)^2$ tel que $a+b = 4(a \wedge b)$.*
On normalise le problème, en introduisant $d = a \wedge b$ et $a' = \dfrac{a}{d}$ et $b' = \dfrac{b}{d}$. Alors $a' \wedge b' = 1$.
Le problème revient donc à : $a+b = 4(a \wedge b) \iff a'+b' = 4$ (car $d \neq 0$ vu que $a \neq 0$).
Or, $a', b' \in \mathbb{N}^*$ et ils sont donc ≤ 3. Ainsi, $a', b' \in \{1,2,3\}$. Comme $a' \wedge b' = 1$, le cas $(a',b') = (2,2)$ est impossible. Ainsi, $(a',b') = (1,3)$ ou $(a',b') = (3,1)$.
Puis, $(a,b) = (d,3d)$ ou $(a,b) = (3d,d)$, avec $d \in \mathbb{N}^*$.

- *Réciproquement, supposons que $(a,b) = (d,3d)$ ou $(a,b) = (3d,d)$, avec $d \in \mathbb{N}^*$.*

Dans chacun des cas, on a bien $\begin{cases} a+b=4d \\ a\wedge b=d \end{cases}$ *donc* $a+b=4(a\wedge b)$.

- *En conclusion,* $\boxed{\{(a,b)\in(\mathbb{N}^*)^2 \mid a+b=4(a\wedge b)\}=\{(d,3d) \mid d\in\mathbb{N}^*\}\cup\{(3d,d) \mid d\in\mathbb{N}^*\}}$.

Exercice 13. *Montrer que l'équation* $x^3+x^2+2x+1=0$ *n'a pas de solution dans* $\mathbb{Q}$.

Correction. *Raisonnons par l'absurde et supposons que l'équation admette une solution rationnelle. On pourrait donc trouver* $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$ *tel que* $a\wedge b=1$ *et* $\frac{a}{b}$ *est solution de l'équation. Alors :* $\left(\frac{a}{b}\right)^3+\left(\frac{a}{b}\right)^2+2\frac{a}{b}+1=0$. *En multipliant par* b^3, *on obtient*

$$a^3+ba^2+2ab^2+b^3=0.$$

En écrivant $b^3=a\underbrace{(-a^2-ab-2b^2)}_{\in\mathbb{Z}}$, *on remarque que* $a|b^3$, *donc* a *divise* $a\wedge b^3$. *Or,* $a\wedge b=1$ *donc* $a\wedge b^3=1$.
On en déduit que $a|1$, *d'où* $a\in\{\pm1\}$.
De même, en écrivant $a^3=b\underbrace{(-a^2-2ab-b^2)}_{\in\mathbb{Z}}$, *on a bien* b *divise* a^3, *donc* b *divise* $a^3\wedge b$ *qui vaut 1.*
Donc $b\in\pm1$, *et comme* $b\in\mathbb{N}^*$, *on a* $b=1$.
Ainsi, $\frac{a}{b}\in\{pm1\}$.
Or, un simple calcul montre que -1 *et* 1 *ne sont pas solution de l'équation. Contradiction.*
On en déduit que $\boxed{\text{l'équation n'admet pas de solution rationnelle}}$.

Remarques. *Notons* $f:x\mapsto x^3+x^2+2x+1$.

- f *est une fonction polynomiale de degré impair donc admet au moins une racine dans* $\mathbb{R}$ *(conséquence du TVI généralisé car* $\lim\limits_{-\infty}f<0$ *et* $\lim\limits_{+\infty}f>0$ *et* f *est continue sur* $\mathbb{R}$*).*
- $f':x\mapsto 3x^2+2x+2>0$ *(équation du second degré sans racine réelle et de coefficient dominant positif) donc* f *est strictement croissante sur* $\mathbb{R}$, *donc injective, donc l'équation admet au plus une solution dans* $\mathbb{R}$.
- $f(0)=1>0$ *et* $f(-1)=-1<0$ *donc* $0\in]f(-1),f(0)[$ *et* f *est continue donc d'après le corollaire du TVI, l'équation admet exactement une solution dans* $\mathbb{R}$, *et elle se trouve dans* $]-1,0[$. *D'après cet exercice, cette solution est irrationnelle !*

Exercice 14. Nombres de Mersenne. *Pour tout* $n\in\mathbb{N}$, *on note* $M_n=2^n-1$.

1. *Soit un entier* $a\geq 2$. *Montrer que si* M_a *est un nombre premier, alors* a *est un nombre premier.*

   Correction. *Supposons* M_a *premier. Soit* d *un diviseur positif de* a. *Alors il existe* $q\in\mathbb{N}$ *tel que* $a=dq$.

   $$M_a=2^a-1=2^{dq}-1=(2^d)^q-1=(2^d-1)(1+2^d+2^{2d}+\cdots+2^{(q-1)d}).$$

   Ainsi, $M_d=2^d-1$ *divise* M_a *et* $M_d\geq 0$. *Or* M_a *est premier donc* $M_d=2^d-1=1$ *ou* $M_d=$

$2^d - 1 = M_a$ *d'où* $d = 1$ *ou* $d = a$. *Cela signifie que* a *est premier*.

2. *Soient* $a, b \in \mathbb{N}^*$ *tels que* $a > b$.

(a) *En notant* r *et* q *le reste (resp. le quotient) de la division euclidienne de* a *par* b, *montrer que*

$$M_a = 2^{bq} M_r + M_b \sum_{k=0}^{q-1} 2^{bk}.$$

Correction. *On sait que* $a = bq + r$. *Par définition, on a :*

$$\begin{aligned} M_a &= 2^a - 1 = 2^{bq+r} - 1 \\ &= 2^{bq} \times 2^r - 1 \\ &= 2^{bq} M_r + 2^{bq} - 1 \\ &= 2^{bq} M_r + (2^b)^q - 1 \\ &= 2^{bq} M_r + (2^b - 1) \left(\sum_{k=0}^{q-1} (2^b)^k \right) \\ M_a &= 2^{bq} M_r + M_b \sum_{k=0}^{q-1} 2^{bk}. \end{aligned}$$

On obtient bien la formule recherchée.

(b) *En déduire que* $\text{pgcd}(M_a, M_b) = \text{pgcd}(M_b, M_r)$.

Correction.

- *Soit* d *un diviseur de* M_a *et de* M_b. *Alors d'après l'égalité précédente,* d *divise* $2^{bq} M_r$. *Remarquons que nécessairement* d *est impair* *(en effet,* M_a *est impair car* $a \neq 0$*) donc* $d \wedge 2^{bq} = 1$. *Par application du lemme de Gauss, on en déduit que* $d | M_r$. *Ainsi,* $d | \text{pgcd}(M_b, M_r)$. *En particulier,* $\text{pgcd}(M_a, M_b) | \text{pgcd}(M_b, M_r)$.
- *Soit* d *un diviseur commun à* M_b *et* M_r. *Alors* $d \left| \left(2^{bq} M_r + M_b \sum_{k=0}^{q-1} 2^{bk} \right) \right.$ *i.e.* $d | M_a$. *Ainsi,* $d | \text{pgcd}(M_a, M_b)$. *En particulier,* $\text{pgcd}(M_b, M_r) | \text{pgcd}(M_a, M_b)$.

Ainsi, $\text{pgcd}(M_a, M_b) = \pm \text{pgcd}(M_b, M_r)$. *Or, des PGCD sont positifs donc* $\text{pgcd}(M_a, M_b) = \text{pgcd}(M_b, M_r)$.
Variante : *avec la notation du cours, on peut montrer de même que* $D_{M_a, M_b} = D_{M_b, M_r}$.

(c) *Conclure que* $\text{pgcd}(M_a, M_b) = M_{\text{pgcd}(a,b)}$.

Correction. *On applique l'algorithme d'Euclide au couple* (a, b) *en commençant par la division euclidienne de* a *par* b. *On note* $r_0, \ldots, r_m$ *les restes des divisions euclidiennes successives, tels que* $r_{m-1} \neq 0$ *et* $r_m = 0$. *Alors* $r_{m-1} = \text{pgcd}(a, b)$ *est le dernier reste non nul.*

D'après la question précédente,

$$\begin{aligned}\operatorname{pgcd}(M_a, M_b) &= \operatorname{pgcd}(M_b, M_{r_0}) = \operatorname{pgcd}(M_{r_0}, M_{r_1}) = \cdots = \operatorname{pgcd}(M_{r_{m-1}}, M_{r_m}) \\ &= \operatorname{pgcd}(M_{r_{m-1}}, M_0) = \operatorname{pgcd}(M_{r_{m-1}}, 0) = |M_{r_{m-1}}| = M_{r_{m-1}} \\ \operatorname{pgcd}(M_a, M_b) &= M_{\operatorname{pgcd}(a,b)},\end{aligned}$$

ce qui est la formule souhaitée.

Exercice 15. Petit théorème de Fermat. *Soit p un nombre premier.*

1. *Montrer que p est premier avec tout entier qu'il ne divise pas. En particulier :*

$$\forall k \in [\![1, p-1]\!],\ k \wedge p = 1.$$

Correction. *Soit k un entier non multiple de p. Montrons que k et p sont premiers entre eux. Soit d un diviseur commun à k et p et positif. d divise p et p est premier, donc $d = 1$ ou $d = p$. Si $d = p$, alors k serait un multiple de p, ce qui contredirait l'hypothèse. D'où $d = 1$ et donc $k \wedge p = 1$.*

2. *Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.*

Correction. *Soit $k \in [\![1, p-1]\!]$.*

Méthode 1. *On a : $k!\binom{p}{k} = p\underbrace{(p-1)\dots(p-k+1)}_{\in\mathbb{N}}$ donc $p | k!\binom{p}{k}$.*

Or, p est premier donc d'après le lemme d'Euclide, on en déduit que : $p | k!$ ou $p | \binom{p}{k}$.
Supposons, par l'absurde, que $p | k!$. Comme $k! = k \times (k-1) \dots 1$ et que p est premier, p diviserait au moins un des facteurs de $k!$. Ainsi, il existerait $i \in [\![1, k]\!]$ tel que $p | i$. En particulier, comme $i \neq 0$, on aurait $p \leq i \leq k$. Or par hypothèse, $k \leq p - 1 < p$, ce qui est absurde d'après la question 1. Ainsi, $p \left| \binom{p}{k} \right.$.

Méthode 2. *On a : $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$ donc $p \left| k\binom{p}{k} \right.$. Or d'après 1., $p \not| k$ et p est premier donc $p \left| \binom{p}{k} \right.$.*

3. *Montrer $\forall a \in \mathbb{N},\ p | (a^p - a)$.*

Correction. *Montrons ce résultat par récurrence sur a. Pour tout $a \in \mathbb{N}$, notons $\mathscr{P}(a)$:« $p | (a^p - a)$ ».*

- *Puisque $p \geq 2$, on a $0^p - 0 = 0$ donc $p | 0^p - 0$. Ainsi, $\mathscr{P}(0)$ est vraie.*
- *Soit $a \in \mathbb{N}$ tel que $\mathscr{P}(a)$.*

  D'après la formule du binôme de Newton, $(a+1)^p - (a+1) = a^p - a + \sum_{k=1}^{p-1} \binom{p}{k} a^k$.

Or, par hypothèse de récurrence, $p|(a^p - a)$ et d'après la question 2., $p\left|\sum_{k=1}^{p-1}\binom{p}{k}a^k\right.$.

Ainsi, $p|[(a+1)^p - (a+1)]$, ce qui prouve $\mathscr{P}(a+1)$.

- *Par récurrence, $\mathscr{P}(a)$ est vraie pour tout $a \in \mathbb{N}$.*

Autrement dit, $\boxed{\text{si } p \text{ est premier, alors pour tout } a \in \mathbb{N}, \text{ on a : } a^p \equiv a \quad [p]}$ **: petit Théorème de Fermat**.

4. *Soit $a \in \mathbb{N}$ tel que $a \wedge p = 1$. Montrer que p divise $(a^{p-1} - 1)$.*

Correction. *D'après la question précédente, $p|(a^p - a)$ donc p divise $a(a^{p-1} - 1)$. Comme $a \wedge p = 1$, d'après le lemme de Gauss, on en déduit que* $\boxed{p|(a^{p-1} - 1)}$.

Autrement dit, $\boxed{\text{si } p \text{ est premier, alors pour tout } a \in \mathbb{N} \text{ tel que } a \wedge p = 1, \text{ on a : } a^{p-1} \equiv 1 \quad [p]}$.

Exercice 16. Application du théorème de Fermat. *Soit $a \in \mathbb{N}^*$. Montrer que $a^{13} - a$ est divisible par 546.*

Correction.

- *La décomposition en nombres premiers donne :* $546 = 2 \times 273 = 2 \times 3 \times 91 = \boxed{2 \times 3 \times 7 \times 13}$.
- *On rappelle le théorème de Fermat : si p est un nombre premier, alors :* $\forall x \in \mathbb{N},\ p|(x^p - x)$ *et* $\forall x \in \mathbb{N},\ x \wedge p = 1 \Longrightarrow p|(x^{p-1} - 1)$.
- *13 est premier donc* $\boxed{13|(a^{13} - a)}$.
- *On écrit :*

$$a^{13} - a = a(a^{12} - 1) = a(a^6 - 1)(a^6 + 1) = (a^7 - a)(a^6 + a).$$

On sait que $7|(a^7 - a)$ et $(a^7 - a)|(a^{13} - a)$ donc par transitivité $\boxed{7|(a^{13} - a)}$.

- *D'après l'écriture précédente, on a :*

$$\begin{aligned} a^{13} - a &= a(a^{12} - 1) = a(a^6 - 1)(a^6 + 1) \\ &= a((a^2)^3 - 1)(a^6 + 1) \\ &= a(a^2 - 1)((a^2)^2 + a^2 + 1)(a^6 + 1) \qquad \text{(somme géom./Bernoulli)} \\ &= (a^3 - a)(a^4 + a^2 + 1)(a^6 + 1). \end{aligned}$$

Comme 3 est premier, on sait que $3|(a^3 - a)$ donc par transitivité $\boxed{3|(a^{13} - a)}$.

- *On écrit :*

$$a^{13} - a = \underbrace{a(a-1)}_{\text{2 entiers consécutifs}}(a+1)(a^4 + a^2 + 1)(a^6 + 1)$$

donc $\boxed{2|(a^{13} - a)}$.

- *Ainsi, 2,3,7, 13 sont des nombres premiers distincts qui divisent $a^{13}-a$ donc leur produit divise $a^{13}-a$ (conséquence de la décomposition en facteurs premiers, ou de la question 5. de l'exercice 9) :* $\boxed{546|a^{13}-a.}$

Exercice 17. *On pose* $\mathbb{Z}[\sqrt{3}]=\{z\in\mathbb{R}\mid \exists(a,b)\in\mathbb{Z}^2,\ z=a+b\sqrt{3}\}$

1. *Montrer que* $\sqrt{3}$ *est irrationnel.*

   Correction. *On raisonne par l'absurde. Supposons que* $\sqrt{3}=\dfrac{p}{q}$ *avec* $(p,q)\in(\mathbb{N}^*)^2$ *et* $\text{pgcd}(p,q)=1$.
   En élevant au carré, on a : $p^2=3q^2$ *i.e.* $3|p^2$. *Or 3 est premier donc* $3|p$ *ou* $3|p$ *d'où* $3|p$.
   Ainsi, $p=3r$ *avec* $r\in\mathbb{N}^*$. *Puis,* $p^2=9r^2=3q^2$ *donc* $q^2=3r^2$. *Ainsi,* $3|q^2$ *donc* $3|q$.
   En résumé, $3|q$ *et* $3|p$ *donc* $3|\text{pgcd}(p,q)$, *ce qui absurde puisque* $\text{pgcd}(p,q)=1$. *Donc,* $\boxed{\sqrt{3}\in\mathbb{R}\setminus\mathbb{Q}}$.

2. *Montrer* $\forall n\in\mathbb{N},\ \exists!(a_n,b_n)\in\mathbb{N}^2\mid(2+\sqrt{3})^n=a_n+b_n\sqrt{3}$.

   Correction.

   Unicité *Soit* $n\in\mathbb{N}$. *Supposons qu'il existe* $(a_n,b_n,c_n,d_n)\in\mathbb{N}^4$ *tel que*

   $$(2+\sqrt{3})^n=a_n+b_n\sqrt{3}=c_n+d_n\sqrt{3}.$$

   Alors $a_n-c_n=\sqrt{3}(d_n-b_n)$.
   Si $d_n\neq b_n$, *alors* $\sqrt{3}\in\mathbb{Q}$, *ce qui est absurde, donc* $\underline{d_n=b_n}$, *puis* $\underline{a_n=c_n}$. *On a donc l'unicité.*

   Existence
   - **Méthode 1.** *On procède par récurrence. On trouve que les suites* (a_n) *et* (b_n) *sont définies par récurrences, via :*

     $$a_0=1,b_0=0\ \text{ et }\ \forall n\in\mathbb{N},\ a_{n+1}=2a_n+3b_n\ \text{ et }\ b_{n+1}=a_n+2b_n.$$

   - **Méthode 2.** *On le montre directement à l'aide du binôme de Newton, en distinguant les puissances paires et impaires de* $\sqrt{3}$ *pour enlever la racine carrée. Avec cette méthode, on trouve les expressions explicites des suites* (a_n) *et* (b_n) *:*

     $$\boxed{a_n=\sum_{p=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2p}3^p\,2^{n-2p}}\qquad\text{et}\qquad\boxed{b_n=\sum_{p=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2p+1}3^p\,2^{n-2p-1}}.$$

3. *Montrer* $\forall n\in\mathbb{N},\ \text{pgcd}(a_n,b_n)=1$.

   Correction.

   - **Méthode 1.** *On procède par récurrence (si on a procédé par récurrence à la question précédente).*
     Initialisation : $a_0=1$ *et* $b_0=0$ *et* $1\wedge 0=1$, *donc* $\text{pgcd}(a_0,b_0)=1$.

Hérédité : Soit $n \in \mathbb{N}$ tel que $a_n \wedge b_n = 1$. Soit d un diviseur commun à a_{n+1} et b_{n+1}. On a :

$$\begin{cases} 2a_n + 3b_n &= a_{n+1} \\ a_n + 2b_n &= b_{n+1} \end{cases} \iff \begin{cases} a_n &= 2a_{n+1} - 3b_{n+1} \\ b_n &= 2b_{n+1} - a_{n+1} \end{cases}.$$

Alors d divise a_n et b_n donc divise leur PGCD i.e. 1, d'où $d = \pm 1$. Ainsi, $a_{n+1} \wedge b_{n+1} = 1$.
Conclusion : Par théorème de récurrence, on en déduit que : $\boxed{\forall n \in \mathbb{N},\ a_n \wedge b_n = 1}$.

- **Méthode 2.** *On le montre directement.*
Soit $n \in \mathbb{N}$. On écrit : $1 = 4 - 3 = (2 - \sqrt{3})(2 + \sqrt{3})$ donc

$$1 = 1^n = (2 - \sqrt{3})^n (2 + \sqrt{3})^n.$$

Or, d'après la question 2 (méthode 2), on sait qu'il existe $(a_n, b_n) \in \mathbb{N}^2$ tel que $(2 + \sqrt{3})^n = a_n + \sqrt{3} b_n$ et on peut montrer de la même manière que $(2 - \sqrt{3})^n = a_n - \sqrt{3} b_n$.
Ainsi,

$$1 = (a_n + \sqrt{3} b_n)(a_n - \sqrt{3} b_n) = a_n^2 - 3b_n^2.$$

Cette relation (de la forme $1 = a_n u + b_n v$ avec $(u, v) \in \mathbb{Z}^2$) assure que $\boxed{a_n \wedge b_n = 1}$ (d'après le théorème de Bézout), et peut être remontrée rapidement, comme suit.

> *Considérons d un diviseur commun à a_n et b_n.*
> *Alors $d | (a_n^2 - 3b_n^2)$, donc $d | 1$, puis $d = \pm 1$.*
> *Ainsi, $a_n \wedge b_n = 1$.*

Divisions euclidiennes

Exercice 18. *Trouver le nombre d'entiers naturels qui, dans la division euclidienne par 23, ont un quotient égal au reste.*

Correction. *Les entiers qui conviennent sont ceux de la forme $n = 23q + q = 24q$, avec $0 \leq q < 23$ i.e. $q \in [\![0, 22]\!]$. Il y a donc 23 possibilités pour q, donc $\boxed{23 \text{ solutions}}$.*

Exercice 19. Division euclidienne dans $\mathbb{Z}$. *Montrer que :*

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*,\ \exists ! (q,r) \in \mathbb{Z}^2,\ \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

Correction. *Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$.*
Unicité. *Soient deux couples (q,r) et (q',r') vérifiant les conclusions de l'énoncé. On a donc $bq + r = bq' + r'$, donc $|r' - r| = |b||q - q'|$ $(*)$.*
L'inégalité sur r entraîne que $-|b| < r' - r < |b|$ i.e. $|r' - r| < |b|$. Puis, $|b||q - q'| < |b|$ donc $|b|(|q - q'| - 1) < 0$ et comme $|b| > 0$, $|q - q'| < 1$. Or, $|q - q'| \in \mathbb{N}$ donc $|q - q'| = 0$ i.e. $\boxed{q = q'}$. En reportant dans $(*)$, il vient : $\boxed{r = r'}$.
Existence.

- *Premier cas. Si $b \in \mathbb{N}^*$, on est dans le cas du cours et $q = \left\lfloor \dfrac{a}{b} \right\rfloor$ et $r = a - bq$ conviennent.*
- *Deuxième cas. Si $b \in \mathbb{Z} \setminus \mathbb{N}^*$, alors $-b \in \mathbb{N}^*$. D'après le premier cas, il existe $(q',r') \in \mathbb{Z}^2$ tel que $a = (-b)q' + r'$ et $0 \leq r' < -b$.*
  Ainsi, $a = b(-q') + r'$, avec $(-q', r') \in \mathbb{Z}^2$ et $0 \leq r' < |b|$.
- *L'existence est donc acquise dans tous les cas.*

Exercice 20. Division euclidienne dans $\mathbb{R} \times \mathbb{R}_+^*$. *Montrer que :*

$$\forall x \in \mathbb{R},\ \forall T > 0,\ \exists ! (q,r) \in \mathbb{Z} \times [0,T[,\ x = qT + r.$$

Que dire dans le cas où $T = 1$?

Correction. *Soit $x \in \mathbb{R}$ et soit $T > 0$.*

- *Pour l'existence, posons $q = \left\lfloor \dfrac{x}{T} \right\rfloor \in \mathbb{Z}$ et $r = x - qT$. On a bien $x = qT + r$, $q \in \mathbb{Z}$. Pour la dernière condition, remarquons que $\dfrac{x}{T} - \left\lfloor \dfrac{x}{T} \right\rfloor \in [0,1[$, i.e. $\dfrac{r}{T} \in [0,1[$ donc $r \in [0,T[$.*
- *Pour l'unicité, soient (q,r) et (q',r') deux couples de $\mathbb{Z} \times [0,T[$ tels que $x = qT + r = q'T + r'$. On a alors*

  $$T(q - q') = r' - r,$$

  qui est donc un multiple de T appartenant à $]-T,T[$. Le seul tel multiple étant 0, on a bien $q = q'$ et $r = r'$, ce qui prouve le résultat.
- *Si $T = 1$, le quotient de x est la partie entière $\lfloor x \rfloor$ et le reste en est la partie fractionnaire.*