**Chapitre :** Arithmétique

# 1 Divisibilité et division euclidienne

**Exercice 1** ★ **Comprendre la division euclidienne** –

1. Déterminer les entiers positifs $a$ et $b$ sachant que $a < 4000$ et que la division euclidienne de $a$ par $b$ donne un quotient de 82 et un reste de 47.

2. Déterminer le quotient et le reste de la division euclidienne de $2^{2013} + 562$ par 4.

3. Quand on divise un nombre par 12, le reste est 8. Quand on divise ce même nombre par 10, on augmente le quotient de 1 et le reste devient 2. Quel est ce nombre ?

4. Démontrer que sur la droite $y = \frac{3}{4}x + \frac{1}{8}$, il n'y a pas de points à coordonnées entières.

Indication ▼ Correction ▼ [672]

**Exercice 2** ★★ **Divisibilité et identité remarquable** –

Démontrer que, pour tous $x, y \in \mathbb{R}^*$ et tout $n \in \mathbb{N}\backslash\{0\}$, on a

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

En déduire que $609 | 5^{4n} - 2^{4n}$.

Indication ▼ Correction ▼ [2280]

**Exercice 3** ★★ **Une relation de divisibilité** –

Déterminer les entiers relatifs $n$ tels que $n-4$ divise $3n-17$.

Indication ▼ Correction ▼ [673]

**Exercice 4** ★★ –

Soit $n \geq 1$ un entier. Déterminer le reste dans la division euclidienne par $n$ de la somme des $n$ premiers entiers strictement positifs.

Indication ▼ Correction ▼ [674]

**Exercice 5** ★★ **Division euclidienne avec de grands nombres** –

Soient $a, b, n$ trois entiers supérieurs ou égaux à 1. On note $q$ le quotient de la division euclidienne de $a-1$ par $b$, et $r$ le reste. Déterminer le quotient et le reste de la division euclidienne de $ab^n - 1$ par $b^{n+1}$.

Indication ▼ Correction ▼ [676]

**Exercice 6** ★★★ **Grands nombres divisibles** –

Montrer que pour tout entier $n \geq 1$, $40^n n! | (5n)!$.

Indication ▼ Correction ▼ [675]

**Exercice 7** ★★ **Équations diophantiennes du second degré résolues par factorisation** –

Résoudre les équations d'inconnues $(x, y) \in \mathbb{N}^2$ :

1. $x^2 - y^2 = 7$ ;

2. $9x^2 - y^2 = 32$.

Indication ▼ Correction ▼ [3169]

**Exercice 8** ★★★ **Écriture en base $b$** –

Soit $b \geq 2$ un entier. On souhaite démontrer que tout entier $n \geq 1$ s'écrit uniquement

$$n = \sum_{k=0}^{p} a_k b^k$$

avec $p \geq 0$, $a_k \in \{0, \dots, b-1\}$ et $a_p \geq 1$.

1. Existence : démontrer l'existence en procédant par récurrence forte. Pour l'hérédité, on pourra utiliser la division euclidienne de $n$ par $b$.

2. Unicité : on suppose que $n$ admet deux décompositions distinctes

$$n = \sum_{k=0}^{p} a_k b^k \text{ et } n = \sum_{k=0}^{p'} a'_k b^k.$$

On peut supposer $p \geq p'$. Quitte à compléter la suite $a'_k$ par $a'_{p'+1} = \cdots = a'_p = 0$, on peut supposer que $p = p'$. Soit $\ell \in \{0, \dots, p\}$ le plus grand possible tel que $a_\ell \neq a'_\ell$.

Vérifier que $(a_\ell - a'_\ell)b^\ell = \sum_{k=0}^{\ell-1}(a'_k - a_k)b^k$. Démontrer que, pour toute suite finie $c_0, \dots, c_{\ell-1}$ avec $0 \leq c_k \leq b-1$, on a

$$\sum_{k=0}^{\ell-1} c_k b^k < b^\ell.$$

Conclure.

3. Vérifier que $(a_\ell - a'_\ell)b^\ell = \sum_{k=0}^{\ell-1}(a'_k - a_k)b^k$.

4. Démontrer que, pour toute suite finie $c_0, \dots, c_{\ell-1}$ avec $0 \leq c_k \leq b-1$, on a

$$\sum_{k=0}^{\ell-1} c_k b^k < b^\ell.$$

5. Conclure.

6. Donner l'écriture de 37 (écrit en base 10) en base 2, puis en base 3.

Indication ▼ Correction ▼ [2891]

**Exercice 9** ★★★★ **Une équation de type Fermat –**

Soit $k \in \mathbb{N}^*$. Le but de l'exercice est de déterminer les entiers $a, b \in \mathbb{N}^*$ solutions de $a^2 + b^2 = 2^k$.

1. Démontrer que si $N, a$ et $b$ sont des entiers tels que $N = a^2 + b^2$ et $N$ est un multiple de 4, alors $a$ et $b$ sont pairs.

2. En déduire que l'équation $2^{2n} = a^2 + b^2$, $n \in \mathbb{N}$, $a, b \in \mathbb{N}^*$ n'admet pas de solutions.

3. Démontrer que l'équation $2^{2n+1} = a^2 + b^2$, $n \in \mathbb{N}$, $a, b \in \mathbb{N}^*$ admet une unique solution que l'on précisera.

Indication ▼ Correction ▼ [690]

## 2 Pgcd, ppcm et nombres premiers entre eux

**Exercice 10** ★ **Pour bien commencer... –**

1. Quels sont les diviseurs positifs communs à 390 et 525 ?

2. Calculer $(3^{123} - 5) \wedge 25$.

3. Soit $n \in \mathbb{Z}$. Démontrer que $6 | n(n+1)(n+2)$.

Indication ▼ Correction ▼ [692]

**Exercice 11** ★ **Des équations de Bezout –**

Résoudre les équations suivantes dans $\mathbb{Z}^2$ :

1. $2x + 5y = 3$ ;

2. $323x - 391y = 612$ ;

3. $162x + 207y = 27$ ;

4. $221x+247y=15$.

Indication ▼ Correction ▼ [693]

**Exercice 12** **Irrationnalité d'un quotient de logarithmes** –

Soit $a,b\geq 2$ deux entiers premiers entre eux. Démontrer que $\ln(a)/\ln(b)$ est irrationnel.

Indication ▼ Correction ▼ [3165]

**Exercice 13** **Rationnels qui sont entiers** –

Soient $a$ et $b$ deux rationnels tels que $a+b$ et $a\times b$ sont des entiers. Prouver que $a$ et $b$ sont des entiers.

Indication ▼ Correction ▼ [694]

**Exercice 14** **Points à coordonnées entières sur une droite rationnelle** –

Le plan est muni d'un repère $(O,\vec{i},\vec{j})$. On considère 4 entiers relatifs non nuls $m,n,p$ et $q$ tels que $\text{pgcd}(m,n)=\text{pgcd}(p,q)=1$. Le but de l'exercice est de déterminer une condition nécessaire et suffisante portant sur $m,n,p,q$ pour que la droite $\Delta$ d'équation $y=\frac{m}{n}x-\frac{p}{q}$ comporte au moins un point dont les coordonnées sont deux entiers relatifs.

1. On suppose dans cette question que la droite $\Delta$ comporte un point de coordonnées $(x_0,y_0)$ où $x_0$, $y_0$ sont des entiers relatifs.

Démontrer que $q$ divise le produit $np$. En déduire que $q$ divise $n$.

2. Démontrer que $q$ divise le produit $np$.

3. En déduire que $q$ divise $n$.

4. Réciproquement, on suppose que $q$ divise $n$ et on souhaite trouver un couple $(x_0,y_0)$ d'entiers relatifs tels que $y_0=\frac{m}{n}x_0-\frac{p}{q}$.

On pose $n=qr$, où $r$ est un entier relatif non nul. Démontrer que l'on peut trouver deux entiers relatifs $u$ et $v$ tels que $qru-mv=1$. En déduire qu'il existe un couple $(x_0,y_0)$ d'entiers relatifs tels que $y_0=\frac{m}{n}x_0-\frac{p}{q}$.

5. On pose $n=qr$, où $r$ est un entier relatif non nul. Démontrer que l'on peut trouver deux entiers relatifs $u$ et $v$ tels que $qru-mv=1$.

6. En déduire qu'il existe un couple $(x_0,y_0)$ d'entiers relatifs tels que $y_0=\frac{m}{n}x_0-\frac{p}{q}$.

7. On donne l'algorithme suivant : Variables : m,n,p,q entiers relatifs non nuls tels que pgcd(m,n)=pgcd(p,q)=1 x entier naturel Algorithme Si q divise n alors x prend la valeur 0 Tant que (mx/n - p/q) n'est pas un entier et (-mx/n-p/q) n'est pas un entier faire x prend la valeur x+1 Fin Tant Que Si (mx/n-p/q) est entier alors Afficher x, mx/n-p/q Sinon Afficher -x,-mx/n-p/q Fin Si Sinon Afficher "Pas de solutions" Fin Si.

Justifier que cet algorithme se termine. Que permet-il d'obtenir ?

Indication ▼ Correction ▼ [2213]

**Exercice 15** **Calculs de pgcd** –

Soient $n\in\mathbb{Z}$. Calculer les pgcd suivants :

**1.** $(n^2+n)\wedge(2n+1)$ **2.** $(15n^2+8n+6)\wedge(30n^2+21n+13)$

Indication ▼ Correction ▼ [706]

**Exercice 16** **Pile de livres** –

J'ai une pile de livres. Lorsque je les range par 10, il m'en reste 3. Lorsque je les range par 17, il m'en reste 2. Quel est le nombre minimum de livres que je possède ? Quels sont tous les nombres possibles ?

Indication ▼ Correction ▼ [2332]

**Exercice 17** **Pas de solutions rationnelles** –

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

Indication ▼ Correction ▼ [699]

**Exercice 18** ★★★ **Termes consécutifs d'une suite** –

Soit $(u_n)$ la suite d'entiers définie par $u_0 = 14$ et $u_{n+1} = 5u_n - 6$. Démontrer que le pgcd de deux termes consécutifs de la suite est constant. Préciser sa valeur.

Indication ▼ Correction ▼ [700]

**Exercice 19** ★★★ **pgcd et somme ou produit prescrits** –

1. Déterminer les couples d'entiers naturels de pgcd 18 et de somme 360.
2. Déterminer les couples d'entiers naturels de pgcd 18 et de produit 6480.

Indication ▼ Correction ▼ [2279]

**Exercice 20** ★★★★ **Équation avec pgcd et ppcm** –

Trouver tous les couples d'entiers $(x,y) \in \mathbb{N}^2$ tels que $x \vee y + 11(x \wedge y) = 203$.

Indication ▼ Correction ▼ [702]

**Exercice 21** ★★★★★ **Liens entre deux pgcd** –

Soient $a,m,n \in \mathbb{N}^*$ avec $a \geq 2$ et $m \leq n$. On note $d = (a^n - 1) \wedge (a^m - 1)$ et $r$ le reste dans la division euclidienne de $n$ par $m$.

1. Montrer que $a^n \equiv a^r \ [a^m - 1]$.
2. En déduire que $d = (a^r - 1) \wedge (a^m - 1)$, puis que $d = a^{n \wedge m} - 1$.
3. A quelle condition $a^m - 1 | a^n - 1$ ?

Indication ▼ Correction ▼ [703]

# 3 Nombres premiers et décomposition en produit de facteurs premiers

**Exercice 22** ★ **Algorithme pour compter le nombre de nombres premiers inférieurs à un entier** $n$ –

1. Écrire une fonction divise$(p,q)$ d'argument deux entiers naturels non nuls $p$ et $q$ et renvoyant True si $p$ divise $q$, et False sinon.
2. Écrire une fonction estpremier$(p)$ d'argument un entier naturel $p$, renvoyant 1 si $p$ est premier, et renvoyant 0 sinon.
3. Écrire une fonction $\phi(n)$ d'argument un entier naturel $n$ et renvoyant le nombre de nombres premiers inférieurs ou égaux à $n$.

Indication ▼ Correction ▼ [2533]

**Exercice 23** ★★ **Nombres de Fermat** –

1. Soit $q$ un entier impair. Démontrer que, pour tout $x \in \mathbb{R}$,

$$x^q + 1 = (x+1)(x^{q-1} - x^{q-2} + \cdots + 1).$$

2. Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit premier. Montrer que $m = 2^n$, où $n \in \mathbb{N}$.

Indication ▼ Correction ▼ [708]

**Exercice 24** ★★★ **Nombres de Mersenne** –

Soient $a,n \geq 2$ des entiers.

1. Montrer que si $a^n - 1$ est premier, alors $a = 2$ et $n$ est premier.
2. On note $M_n = 2^n - 1$ le $n$-ième nombre de Mersenne. Vérifier que $M_{11}$ n'est pas premier.

Indication ▼ Correction ▼ [711]

**Exercice 25** ★★★★ **Une version faible du théorème de la progression arithmétique** –

1. Démontrer que si un entier naturel est congru à 3 modulo 4, il admet un facteur premier congru à 3 modulo 4.

2. Démontrer qu'il existe une infinité de nombres premiers de la forme $4k+3$.

Indication ▼ Correction ▼ [712]

**Exercice 26** ★★★★★ **Intervalles sans nombres premiers** –

Soit $q \geq 1$ un entier. Trouver un intervalle de longueur $q$ ne contenant pas de nombres premiers.

Indication ▼ Correction ▼ [715]

**Exercice 27** ★ **Divisibilité et puissance** –

Soit $a, b \in \mathbb{N}^*$ tels que $a^2 | b^2$. Démontrer que $a|b$.

Indication ▼ Correction ▼ [3162]

**Exercice 28** ★ **Puissances égales** –

1. Montrer qu'un entier naturel qui est à la fois un carré et un cube est aussi un entier à la puissance 6.

2. Généralisation : soient $a, b, p, q, n$ des entiers naturels avec $p \wedge q = 1$ et $n = a^p = b^q$. Montrer qu'il existe un entier naturel $c$ tel que $n = c^{pq}$.

Indication ▼ Correction ▼ [704]

**Exercice 29** ★★ **Le produit est un carré parfait** –

Soient $a$ et $b$ deux entiers premiers entre eux tels que leur produit $ab$ est un carré parfait. Montrer que $a$ et $b$ sont deux carrés parfaits.

Indication ▼ Correction ▼ [705]

**Exercice 30** ★★★ **Application au calcul de pgcd** –

Soient $a, b, c \in \mathbb{N}^*$ et soit $n \in \mathbb{N}^*$.

1. Démontrer que $c|ab \implies c|(a \wedge c)(b \wedge c)$.

2. Démontrer que $(a \wedge b)^n = a^n \wedge b^n$.

3. (Plus difficile) Calculer $(a^2 + ab + b^2) \wedge ab$.

Indication ▼ Correction ▼ [707]

**Exercice 31** ★★★★ **Nombre de diviseurs d'un entier** –

Soit $n$ un nombre entier, $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en produit de facteurs premiers. On note $d(n)$ le nombre de diviseurs de $n$.

1. Montrer que $d(n) = \prod_{i=1}^{r} (\alpha_i + 1)$.

2. Montrer que $n$ est un carré parfait si et seulement si $d(n)$ est impair.

3. Montrer que $\prod_{d|n} d = \sqrt{n}^{d(n)}$.

Indication ▼ Correction ▼ [709]

**Exercice 32** ★★★★ **Formule de Legendre** –

Soit $n \geq 1$ un entier et $p \geq 2$ un nombre premier. Soit aussi $N$ tel que $p^N \geq n$.

1. Soit $u \geq 1$ un entier. Combien-y-a-t-il de multiples de $u$ dans $\{1, \dots, n\}$ ?

2. Soit $k \geq 1$ et $A_k = \{l \in \{1, \dots, n\} : \ v_p(l) = k\}$. Calculer le cardinal de $A_k$.

3. En déduire la formule de Legendre :

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

4. Par combien de zéros se termine le nombre 1000! ?

Indication ▼ Correction ▼ [3170]

**Exercice 33** ★★★★★ **Produit des diviseurs d'un entier** –

Déterminer tous les entiers naturels dont le produit des diviseurs (positifs) est égal à $45^{42}$.

Indication ▼ Correction ▼ [714]

# 4 Congruences

**Exercice 34** ★ **Puissances itérées** –

1. Déterminer, suivant les valeurs de $n \in \mathbb{N}$, le reste de la division euclidienne de $2^n$ par 5.
2. Quel est le reste de la division par 5 de $1357^{2013}$ ?

Indication ▼ Correction ▼ [677]

**Exercice 35** ★ **Un entier divisible par** 6 –

Démontrer que pour tout $n \in \mathbb{Z}$, $n(n+2)(7n-5)$ est divisible par 6.

Indication ▼ Correction ▼ [3163]

**Exercice 36** ★ **Divisible par** 30**.** –

Soit $n \in \mathbb{N}$ et $a = n^5 - n$.

1. Démontrer que $a$ est divisible par 5.
2. En remarquant que $a = n(n-1)(n+1)(n^2+1)$, démontrer que $a$ est divisible par 2 et par 3.
3. Démontrer que $a$ est divisible par 30.

Indication ▼ Correction ▼ [3164]

**Exercice 37** ★★ **Somme de trois cubes consécutifs** –

Démontrer que la somme de trois cubes consécutifs est toujours divisible par 9.

Indication ▼ Correction ▼ [678]

**Exercice 38** ★★ **Deux équations avec des congruences** –

1. Déterminer les entiers naturels $n$ tels que $5^n \equiv -1\ [13]$.
2. Déterminer les entiers naturels $n$ tels que 13 divise $5^{2n} + 5^n$.

Indication ▼ Correction ▼ [2562]

**Exercice 39** ★ **Puissance et congruence** –

Soit $a, b \in \mathbb{Z}$ et $n \geq 2$. On suppose que $a \equiv b\ [n]$. Démontrer que $a^n \equiv b^n\ [n^2]$.

Indication ▼ Correction ▼ [3166]

**Exercice 40** ★★ **La preuve par neuf** –

Montrer que tout entier naturel est congru modulo 9 à la somme des chiffres de son écriture décimale. En déduire que, quels que soient les entiers naturels $x = \overline{a_n \dots a_0}$, $y = \overline{b_m \dots b_0}$ et $z = \overline{c_p \dots c_0}$, si $xy = z$, alors $\left(\sum_{i=0}^{n} a_i\right)\left(\sum_{i=0}^{m} b_i\right) \equiv \left(\sum_{i=0}^{p} c_i\right)\ [9]$.

Indication ▼ Correction ▼ [679]

**Exercice 41** ★★ **Résolution d'équations diophantiennes en raisonnant modulo un entier** –

Résoudre les équations suivantes dans $\mathbb{Z}^2$ :
1. $x^2 - 5y^2 = 3$ (on raisonnera modulo 5) ;
2. $15x^2 - 8y^2 = 9$ (on raisonnera modulo 5).

Indication ▼ Correction ▼ [3168]

**Exercice 42** ★★★ **Divisible par 7** –

Démontrer que, pour tout entier naturel $n$, $3^{2n+1} + 2^{4n+2}$ est divisible par 7.

Indication ▼ Correction ▼ [2431]

**Exercice 43** ★★★ **Théorème de Pascal** –

Soit $m$ un entier naturel non-nul, et soit $(r_i)$ la suite d'entiers définie par $r_0 = 1$ et $r_{i+1}$ est le reste de la division euclidienne de $10r_i$ par $m$.

1. Démontrer que, pour tout entier naturel $a = \overline{a_n \dots a_0}$ en écriture décimale, on a $a \equiv \sum_{i=0}^{n} a_i r_i \ [m]$.
2. En déduire des critères simples permettant de reconnaitre sur l'écriture décimale d'un réel s'il est ou non divisible par 3, par 9, par 10, par 11.

Indication ▼ Correction ▼ [680]

**Exercice 44** ★★ **Équations de congruence du premier degré** –

Résoudre les équations suivantes :
1. $5x \equiv 3\ [17]$ ;
2. $10x \equiv 6\ [34]$ ;
3. $10x \equiv 5\ [34]$.

Indication ▼ Correction ▼ [3161]

**Exercice 45** ★★ **Un système de congruences** –

Résoudre le système suivant, d'inconnue $x \in \mathbb{Z}$ :

$$\begin{cases} x & \equiv & 1\ [5] \\ x & \equiv & 2\ [11]. \end{cases}$$

Indication ▼ Correction ▼ [3167]

**Exercice 46** ★★★ **Nombres palindromes** –

Un nombre palindrome est un nombre qui se lit indifféremment de gauche à droite ou de droite à gauche. Par exemple, 2002, 12321 sont des nombres palindromes. Prouver qu'un nombre palindrome ayant un nombre pair de chiffres est divisible par 11

Indication ▼ Correction ▼ [682]

**Exercice 47** ★★ **Une équation diophantienne** –

Le but de l'exercice est de déterminer tous les couples d'entiers $(m,n) \in \mathbb{N}^2$ tels que $2^m - 3^n = 1$.
1. Déterminer le reste de la division euclidienne de $3^n$ par 8 (on distinguera les cas $n$ pair et $n$ impair).
2. En déduire que si $(m,n) \in \mathbb{N}^2$ est solution de $2^m - 3^n = 1$, alors $m \leq 2$.
3. Déterminer toutes les solutions de l'équation.

Indication ▼ Correction ▼ [2378]

**Exercice 48** **Somme de deux carrés divisible par 7 –**

Soit $a$ et $b$ deux entiers tels que $a^2+b^2$ soit divisible par 7. Démontrer que $a$ et $b$ sont divisibles par 7.

Indication ▼ Correction ▼ [2282]

**Exercice 49** **Coefficients binomiaux –**

1. Soit $n \geq 1$. Montrer que $(n+1) | \binom{2n}{n}$.
2. Soit $p \geq 2$ premier. Montrer que $p | \binom{p}{k}$ pour $k \in \{1, \ldots, p-1\}$.
3. En déduire une preuve du petit théorème de Fermat : si $n \geq 1$ et $p$ est premier, $n^p \equiv n \ [p]$.

Indication ▼ Correction ▼ [688]

**Indication pour l'exercice 1 ▲**

1. Écrire la division euclidienne. Quelle est la valeur minimale de $b$ ?
2. Commencer par faire la division euclidienne de chaque terme de la somme.
3. Écrire deux fois la division euclidienne.
4. Raisonner par l'absurde et multiplier l'équation par 8 !

**Indication pour l'exercice 2 ▲**

Développer le membre de droite.

**Indication pour l'exercice 3 ▲**

Si $n-4$ divise $3n-17$, il divise aussi toute combinaison $a(n-4)+b(3n-17)$, avec $a$ et $b$ des entiers.

**Indication pour l'exercice 4 ▲**

Distinguer les cas $n$ pair et $n$ impair.

**Indication pour l'exercice 5 ▲**

Écrire la division euclidienne, puis tout multiplier par $b^n$.

**Indication pour l'exercice 6 ▲**

Raisonner par récurrence sur $n$.

**Indication pour l'exercice 7 ▲**

Factoriser puis résoudre, dans le premier cas, $uv = 7$ et dans le deuxième cas, $uv = 32$, avec $u, v$ des entiers naturels.

**Indication pour l'exercice 8 ▲**

1. Dans l'hérédité, on pourra distinguer le cas $n+1 \geq b$ du cas $n+1 < b$.
2. Écrire $n = n$ avec les deux décompositions possibles pour $n$. Se ramener à une somme géométrique.
3. Écrire $n = n$ avec les deux décompositions possibles pour $n$.
4. Se ramener à une somme géométrique.
5. 
6. Reprendre le schéma de l'existence, en faisant des divisions euclidiennes successives.

**Indication pour l'exercice 9 ▲**

1. Distinguer toutes les possibilités de parité possibles pour $a$ et $b$.
2. Considérer une solution à l'équation avec $n$ le plus petit possible, et fabriquer une solution encore plus petite.
3. Procéder par récurrence.

**Indication pour l'exercice 10 ▲**

1. Chercher le pgcd de ces deux nombres.
2. Pourquoi le pgcd de ces deux nombres est 1, 5 ou 25 ? Pourquoi est-ce forcément 1 ?
3. Démontrer que $2|n(n+1)(n+2)$ et $3|n(n+1)(n+2)$.

**Indication pour l'exercice 11 ▲**

1. Chercher une solution particulière, puis déterminer toutes les solutions en retranchant cette solution particulière et en utilisant le théorème de Gauss.

2. Commencer par chercher le pgcd de 323 et 391. Puis simplifier l'équation en la divisant par ce pgcd. Procéder alors comme d'ordinaire.

3. Exactement comme ci-dessus.

4. Il y a un piège !

**Indication pour l'exercice 12 ▲**

Procéder par l'absurde.

**Indication pour l'exercice 13 ▲**

Écrire $a$ et $b$ sous forme de fraction irréductible et commencer, en utilisant $a+b$, par démontrer que les dénominateurs sont égaux.

**Indication pour l'exercice 14 ▲**

1. Remarquer que le nombre $ny_0 - mx0$ est un entier relatif. Théorème de Gauss.
2. Remarquer que le nombre $ny_0 - mx0$ est un entier relatif.
3. Théorème de Gauss.
4. Théorème de Bézout. Chercher $x_0$ et $y_0$ de sorte que $(x_0, y_0)$ soit solution de

$$\frac{-np}{q} = ny_0 - mx_0.$$

5. Théorème de Bézout.
6. Chercher $x_0$ et $y_0$ de sorte que $(x_0, y_0)$ soit solution de

$$\frac{-np}{q} = ny_0 - mx_0.$$

7.

**Indication pour l'exercice 15 ▲**

On pourra utiliser une astuce (relation entre $n^2+n$ et $2n+1$ par exemple) ou l'algorithme d'Euclide.

**Indication pour l'exercice 16 ▲**

Se ramener à résoudre une équation de Bézout...

**Indication pour l'exercice 17 ▲**

Raisonner par l'absurde et imaginer qu'une solution $x = p/q$ existe, avec $p \wedge q = 1$. Remettre tout au même dénominateur, et montrer que $q = 1$.

**Indication pour l'exercice 18 ▲**

Démontrer que le pgcd de $u_n$ et $u_{n+1}$ est dans $\{1,2,3,6\}$. Puis démontrer que 3 ne divise aucun $(u_n)$.

**Indication pour l'exercice 19 ▲**

Écrire $x = 18x'$ et $y = 18y'$ avec $x' \wedge y' = 1$. On trouve une équation facile pour $x'+y'$ (ou pour $x'y'$) qu'on peut résoudre de façon exhaustive en tenant bien compte du fait que $x'$ et $y'$ sont premiers entre eux.

**Indication pour l'exercice 20 ▲**

Écrire $x = dx'$, $y = dy'$ avec $x' \wedge y' = 1$. On obtient $d|203 = 7 \times 29$. Que peut valoir $d$ ? Etudier tous les cas.

**Indication pour l'exercice 21 ▲**

1. Écrire $a^n - a^r = a^r\left((a^m)^q - 1\right)$ puis utiliser une identité remarquable.
2. Faire l'algorithme d'Euclide sur les exposants de $a$.
3. $b|c \iff b \wedge c = b$.

**Indication pour l'exercice 22 ▲**

**Indication pour l'exercice 23 ▲**

1. Il suffit de développer.
2. Par l'absurde

**Indication pour l'exercice 24 ▲**

Utiliser l'identité remarquable

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

**Indication pour l'exercice 25 ▲**

1. Utiliser la décomposition de $n$ en produits de facteurs premiers.
2. Démarrer comme la démonstration d'Euclide de l'existence d'une infinité de nombres premiers, c'est-à-dire supposer qu'il en existe simplement un nombre fini, considérer leur produit $n$ et surtout $m = 4n-1$. A quoi $n$ est-il congru modulo 4 ?

**Indication pour l'exercice 26 ▲**

Considérer des intervalles du type $[n!+2, n!+n]$.

**Indication pour l'exercice 27 ▲**

Utiliser une décomposition en produit de facteurs premiers.

**Indication pour l'exercice 28 ▲**

Décomposer $a$ et $b$ en facteur premiers, identifier les puissances des exposants, puis utiliser le théorème de Gauss.

**Indication pour l'exercice 29 ▲**

Décomposer $a, b$ et $ab$ en produit de facteurs premiers, $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \dots p_r^{\beta_r}$, $ab = p_1^{2\gamma_1} \dots p_r^{2\gamma_r}$, et se rappeler que, pour tout $j$, $\alpha_j \neq 0 \implies \beta_j = 0$.

**Indication pour l'exercice 30 ▲**

A chaque fois, on utilisera une décomposition en facteurs premiers des entiers concernés, et la caractérisation du pgcd à l'aide de cette décomposition.

**Indication pour l'exercice 31 ▲**

1. Un diviseur de $n$ s'écrit de façon unique sous la forme $d = p_1^{\beta_1} \dots p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$ pour $i = 1, \dots, r$.
2. Un produit de nombres entiers est pair si et seulement si un de ses facteurs est pair. Ou encore, un produit de nombres entiers est impair si et seulement si tous ses facteurs sont impairs.
3. Regrouper $n$ et $n/d$.

**Indication pour l'exercice 32 ▲**

1.
2. On a $v_p(l) = k$ si et seulement si $p^k | l$ mais $p^{k+1}$ ne divise pas $l$.
3. Écrire $v_p(n!) = \sum_{l=1}^{n} v_p(l)$ puis regrouper les éléments de $\{1, \ldots, n\}$ suivant leur valuation $p$-adique.
4. Il suffit de calculer $v_2(1000!)$ et $v_5(1000!)$.

**Indication pour l'exercice 33 ▲**

Prouver d'abord que $n$ est de la forme $3^p 5^q$, puis faire le produit des diviseurs de ces nombres.

**Indication pour l'exercice 34 ▲**

1. Commencer par les petites valeurs de $n$ pour conjecturer que la suite des restes est périodique.
2. Commencer par étudier le reste de 1357 dans la division par 5.

**Indication pour l'exercice 35 ▲**

Il suffit de vérifier la divisibilité par 2 et par 3. On pourra faire un raisonnement par disjonction de cas.

**Indication pour l'exercice 36 ▲**

1. Petit théorème de Fermat.
2.
3. Appliquer un corollaire du théorème de Gauss.

**Indication pour l'exercice 37 ▲**

Développer $n^3 + (n+1)^3 + (n+2)^3$ et essayer de factoriser par 9. On pourra discuter suivant la congruence modulo 3 de $n$.

**Indication pour l'exercice 38 ▲**

1. Calculer $5^2$, $5^3$, $5^4$ etc... modulo 13.
2. Factoriser par $5^n$ et utiliser que $13 \wedge 5 = 1$.

**Indication pour l'exercice 39 ▲**

Traduire avec des quantificateurs $a \equiv b\ [n]$, mettre à la puissance $n$ et utiliser la formule du binôme.

**Indication pour l'exercice 40 ▲**

A quoi est congru 10 modulo 9 ?

**Indication pour l'exercice 41 ▲**

Écrire l'équation modulo 5 la simplifiera grandement. On peut ensuite faire un raisonnement par disjonction de cas pour prouver qu'il y aura peu de solutions...

**Indication pour l'exercice 42 ▲**

Raisonner par récurrence sur n, en testant la divisibilité par 7 grâce aux congruences modulo 7. Le point clé pour le passage du rang $n$ au rang $n+1$ est qu'à la fois $2^4$ et $3^2$ sont congrus à 2 modulo 7.

**Indication pour l'exercice 43 ▲**

1. Démontrer que $10^i \equiv r_i\ [m]$ pour chaque entier naturel $i$.
2. Pour chaque valeur (3,9,10,11), étudier le comportement de la suite $r_i$.

**Indication pour l'exercice 44 ▲**

1. Commencer par chercher un entier $a$ tel que $5a \equiv 1\ [17]$. En déduire une solution particulière de l'équation, puis toutes les solutions.
2. Se ramener à l'équation précédente.
3. Pourquoi n'y-a-t-il pas de solutions ?

**Indication pour l'exercice 45 ▲**

Commencer par résoudre $x \equiv 1\ [5]$, puis introduire le résultat dans la seconde équation.

**Indication pour l'exercice 46 ▲**

Écrire le nombre sous la forme $a_1 \dots a_p a_p \dots a_1$ et remarquer que $10^k$ est congru à 1 modulo 11 si $k$ est pair, à -1 si $k$ est impair.

**Indication pour l'exercice 47 ▲**

1. $3^2 \equiv 1\ [8]$.
2. Supposer l'existence d'une solution avec $m > 2$. On a alors $2^m \equiv 0\ [8]$.
3. Faire $m = 0$, $m = 1$ et $m = 2$.

**Indication pour l'exercice 48 ▲**

Commencer par écrire un tableau décrivant les carrés modulo 7.

**Indication pour l'exercice 49 ▲**

1. Utiliser la formule $(n+1)\binom{2n}{n+1} = n\binom{2n}{n}$.
2. Montrer que $k!(p-k)!|(p-1)!$.
3. Procéder par récurrence sur $n$.

**Correction de l'exercice 1 ▲**

1. On sait que $a = 82b+47$, et que $b > 47$. Mais si $b = 49$, alors $82\times 49+47 > 4000$. La seule possibilité est donc $b = 48$, et $a = 3983$.

2. On commence par remarquer que $2^{2013} = 4\times 2^{2011}$. Pour l'autre partie, $562 = 4\times 140+2$. On en déduit donc que

$$2^{2013}+562 = 4\times(2^{2011}+140)+2.$$

Ainsi, le quotient est $2^{2011}+140$ et le reste est 2.

3. On écrit deux fois la division euclidienne. Notons $a$ le nombre recherché, et $q$ le premier quotient, on trouve $a = 12q+8$ et $a = 10(q+1)+2$. Il s'agit maintenant d'un petit système à résoudre, et on trouve $a = 32$.

4. Supposons qu'il existe un point $(x,y)$ à coordonnées entières sur cette droite. Alors, multipliant l'équation de la droite par 8, on trouve que

$$8y = 6x+1.$$

Mais $2|8y$, $2|6x$ et donc $2|1$, ce qui n'est pas le cas.

---

**Correction de l'exercice 2 ▲**

Développons le membre de droite de l'identité que l'on nous demande de démontrer.

$$\begin{aligned}(x-y)\sum_{k=0}^{n-1}x^k y^{n-1-k} &= \sum_{k=0}^{n-1}x^{k+1}y^{n-1-k}-\sum_{k=0}^{n-1}x^k y^{n-k}\\ &= \sum_{k=1}^{n}x^k y^{n-k}-\sum_{k=0}^{n-1}x^k y^{n-k}\end{aligned}$$

en effectuant un changement d'indice dans la première somme. Mais les deux sommes sont identiques, à deux termes près, et on a donc

$$(x-y)\sum_{k=0}^{n-1}x^k y^{n-1-k} = x^n y^{n-n}-x^0 y^{n-0} = x^n-y^n.$$

Le fait que $609|5^{4n}-2^{4n}$ est alors une application immédiate de cette identité à $x = 5^4$ et $y = 2^4$, puisque dans ce cas $x-y = 609$.

---

**Correction de l'exercice 3 ▲**

Puisque $n-4$ divise $3n-17$ et que $n-4$ divise $n-4$, $n-4$ divise également $(3n-17)-3(n-4) = -5$. Or les diviseurs dans $\mathbb{Z}$ de $-5$ sont $-5,-1,1,5$. Les valeurs possibles de $n-4$ sont donc ces valeurs, et donc on a $n\in\{-1,3,5,9\}$. Réciproquement, si $n = -1$, alors $n-4 = -5$ divise $3n-17 = -20$. Si $n = 3$, $n-4 = -1$ divise $3n-17 = -8$. Si $n = 5$, $n-4 = 1$ divise $3n-17 = -2$. Si $n = 9$, $n-4 = 5$ divise $3n-17 = 10$. En conclusion, les valeurs de $n$ qui conviennent sont $-1,3,5$ et 9.

---

**Correction de l'exercice 4 ▲**

Soit $S_n$ la somme des $n$ premiers entiers. Elle vaut $\frac{n(n+1)}{2}$. Si $n$ est impair, autrement dit si $n+1$ est pair, alors $(n+1)/2$ est un entier, et $n|S_n$. Le reste est donc 0. Si maintenant $n = 2k$ est pair, alors

$$S_n = \frac{2k(2k+1)}{2} = \frac{(2k)^2}{2}+k = k\times 2k+k = k\times n+n/2$$

Le reste est donc $n/2$.

---

**Correction de l'exercice 5 ▲**

La division euclidienne s'écrit $a-1 = bq+r$, avec $0\leq r\leq b-1$. On multiplie ensuite tout par $b^n$ et on trouve $ab^n-b^n = b^{n+1}q+rb^n$, puis on se ramène à

$$ab^n-1 = b^{n+1}q+rb^n+b^n-1 = b^{n+1}q+r'$$

où $r' = rb^n + b^n - 1$. On remarque que $0 \leq r' \leq (b-1)b^n + b^n - 1 = b^{n+1} - 1$. On a donc écrit la division euclidienne de $ab^n - 1$ par $b^{n+1}$, le quotient est $q$ et le reste est $rb^n + b^n - 1$.

---

**Correction de l'exercice 6 ▲**

On raisonne par récurrence sur $n$. La propriété est clairement vérifiée si $n = 1$, car $5! = 120 = 40 \times 3$. Supposons la propriété vraie au rang $n$, et prouvons la au rang $n+1$. On a

$$\begin{aligned}(5n+5)! &= (5n)!(5n+1)(5n+2)(5n+3)(5n+4)(5n+5)\\ &= (5n)!5(n+1)(5n+1)(5n+2)(5n+3)(5n+4)\end{aligned}$$

et

$$40^{n+1}(n+1)! = 40^n n! \times 40(n+1).$$

Puisque par hypothèse de récurrence, $40^n n! | (5n)!$, il suffit de prouver que $40(n+1) | 5(n+1)(5n+1)(5n+2)(5n+3)(5n+4)$, ou encore $8 | (5n+1)(5n+2)(5n+3)(5n+4)$. Mais $5n+1, 5n+2, 5n+3, 5n+4$ sont quatre entiers consécutifs. Deux sont pairs, et l'un des ces deux entiers pairs est même divisible par 4. Donc 8 divise bien leur produit.

---

**Correction de l'exercice 7 ▲**

1. On factorise $x^2 - y^2 = (x-y)(x+y)$. Puisque les seuls diviseurs de 7 sont 1 et 7, et puisque $x+y \geq x-y$, $x$ et $y$ sont solutions du système

$$\begin{cases} x-y &= 1\\ x+y &= 7\end{cases}$$

dont la seule solution est $x = 4$ et $y = 3$. L'équation $x^2 - y^2 = 7$ admet donc pour unique solution le couple $(4,3)$.

2. On procède de la même façon en remarquant que $9x^2 - y^2 = (3x-y)(3x+y)$. Mais cette fois, 32 a beaucoup plus de diviseurs et on peut l'écrire sous la forme

$$32 = 32 \times 1 = 16 \times 2 = 8 \times 4.$$

Tenant compte de $x+y \geq x-y$, on trouve que $(x,y)$ est solution d'un des trois systèmes suivants :

$\begin{cases} 3x+y &= 32\\ 3x-y &= 1.\end{cases}$ Mais ce système n'a pas de solutions entières... $\begin{cases} 3x+y &= 16\\ 3x-y &= 2.\end{cases}$ Dans ce cas, on trouve $x = 3$ et $y = 7$. $\begin{cases} 3x+y &= 8\\ 3x-y &= 4.\end{cases}$ Dans ce cas, on trouve $x = 2$ et $y = 2$.

Finalement, on a prouvé que l'ensemble des solutions est $\{(3,7);(2,2)\}$.

3. $\begin{cases} 3x+y &= 32\\ 3x-y &= 1.\end{cases}$ Mais ce système n'a pas de solutions entières...

4. $\begin{cases} 3x+y &= 16\\ 3x-y &= 2.\end{cases}$ Dans ce cas, on trouve $x = 3$ et $y = 7$.

5. $\begin{cases} 3x+y &= 8\\ 3x-y &= 4.\end{cases}$ Dans ce cas, on trouve $x = 2$ et $y = 2$.

---

**Correction de l'exercice 8 ▲**

1. Pour $n \geq 1$, on note $H_n$ la propriété suivante :

$$H_n = \text{"}\exists p \geq 0, \exists (a_0, \ldots, a_p) \in \{0, \ldots, b-1\} \text{ avec } a_p \geq 1 \text{ tels que } n = \sum_{k=0}^{p} a_k b^k.\text{"}$$

Initialisation : $H_1$ est vraie, car $1 = 1 \times b^0$ (on a $p = 0$ et $a_0 = 1$). Hérédite : Soit $n \geq 1$ et supposons $H_1, \ldots, H_n$ vraies. Prouvons $H_{n+1}$. On distingue deux cas :

soit $n+1 < b$. Dans ce cas, on peut écrire $n+1 = (n+1)b^0$, et on a le résultat avec $p = 0$ et $a_0 = n+1$. soit $n+1 \geq b$. Dans ce cas, on réalise la division euclidienne de $n+1$ par $b$. On écrit donc

$$n+1 = bq + r,\ 0 \leq r \leq b-1.$$

On a alors $q \leq n$ et on peut appliquer l'hypothèse de récurrence à $q$ : $q$ s'écrit

$$q = \sum_{k=0}^{p} a_k b^k,\ 0 \leq a_k \leq b-1,\ a_p \geq 1.$$

On obtient alors

$$n+1 = \sum_{k=0}^{p} a_k b^{k+1} + r = r + \sum_{k=1}^{p+1} a_{k-1} b^k.$$

On obtient alors bien que $n+1$ s'écrit

$$n+1 = \sum_{k=0}^{p'} a'_k b^k, 0 \leq a'_k \leq b-1,\ a'_{p'} \geq 1$$

en posant $p' = p+1$, $a'_k = a_{k-1}$ pour $k = 1, \ldots, p'$ et $a'_0 = r$.

Dans tous les cas $H_{n+1}$ est vraie. Donc, par le principe de récurrence forte, $H_n$ est vraie pour tout entier $n \geq 1$.

2. soit $n+1 < b$. Dans ce cas, on peut écrire $n+1 = (n+1)b^0$, et on a le résultat avec $p = 0$ et $a_0 = n+1$.

3. soit $n+1 \geq b$. Dans ce cas, on réalise la division euclidienne de $n+1$ par $b$. On écrit donc

$$n+1 = bq + r,\ 0 \leq r \leq b-1.$$

On a alors $q \leq n$ et on peut appliquer l'hypothèse de récurrence à $q$ : $q$ s'écrit

$$q = \sum_{k=0}^{p} a_k b^k,\ 0 \leq a_k \leq b-1,\ a_p \geq 1.$$

On obtient alors

$$n+1 = \sum_{k=0}^{p} a_k b^{k+1} + r = r + \sum_{k=1}^{p+1} a_{k-1} b^k.$$

On obtient alors bien que $n+1$ s'écrit

$$n+1 = \sum_{k=0}^{p'} a'_k b^k, 0 \leq a'_k \leq b-1,\ a'_{p'} \geq 1$$

en posant $p' = p+1$, $a'_k = a_{k-1}$ pour $k = 1, \ldots, p'$ et $a'_0 = r$.

4. Il suffit d'écrire que

$$n = \sum_{k=0}^{p} a_k b^k = \sum_{k=0}^{p} a'_k b^k$$

ce qui s'écrit encore, par définition de $\ell$,

$$n = \sum_{k=0}^{\ell} a_k b^k = \sum_{k=0}^{\ell} a'_k b^k.$$

Ceci s'écrit à son tour

$$a_\ell b^\ell + \sum_{k=0}^{\ell-1} a_k b^k = a'_\ell b^\ell + \sum_{k=0}^{\ell-1} a'_k b^k$$

ce qui donne immédiatement le résultat voulu. On écrit simplement que

$$\sum_{k=0}^{\ell-1} c_k b^k \leq (b-1) \sum_{k=0}^{\ell-1} b^k = b^\ell - 1 < b^\ell$$

où on a reconnu une somme géométrique. Supposons par exemple que $a_\ell > a'_\ell$. On a alors, puisque $|a'_k - a_k| \leq b-1$,

$$\left| \sum_{k=0}^{\ell-1} (a'_k - a_k) b^k \right| \leq \sum_{k=0}^{\ell-1} |a'_k - a_k| b^k < b^\ell \leq (a_\ell - a'_\ell) b^\ell$$

ce qui contredit l'hypothèse faite. On a donc bien démontré l'unicité de la décomposition en base b.

5. Il suffit d'écrire que

$$n = \sum_{k=0}^{p} a_k b^k = \sum_{k=0}^{p} a'_k b^k$$

ce qui s'écrit encore, par définition de $\ell$,

$$n = \sum_{k=0}^{\ell} a_k b^k = \sum_{k=0}^{\ell} a'_k b^k.$$

Ceci s'écrit à son tour

$$a_\ell b^\ell + \sum_{k=0}^{\ell-1} a_k b^k = a'_\ell b^\ell + \sum_{k=0}^{\ell-1} a'_k b^k$$

ce qui donne immédiatement le résultat voulu.

6. On écrit simplement que

$$\sum_{k=0}^{\ell-1} c_k b^k \leq (b-1) \sum_{k=0}^{\ell-1} b^k = b^\ell - 1 < b^\ell$$

où on a reconnu une somme géométrique.

7. Supposons par exemple que $a_\ell > a'_\ell$. On a alors, puisque $|a'_k - a_k| \leq b-1$,

$$\left| \sum_{k=0}^{\ell-1} (a'_k - a_k) b^k \right| \leq \sum_{k=0}^{\ell-1} |a'_k - a_k| b^k < b^\ell \leq (a_\ell - a'_\ell) b^\ell$$

ce qui contredit l'hypothèse faite. On a donc bien démontré l'unicité de la décomposition en base b.

8. On va faire des divisions euclidiennes successives :

$$\begin{aligned} 37 &= 2 \times 18 + 1 \\ &= 2 \times (2 \times 9 + 0) + 1 \\ &= 2 \times (2 \times (2 \times 4 + 1)) + 1 \\ &= 2 \times (2 \times (2 \times 2^2 + 1)) + 1 \\ &= 2^5 + 2^2 + 2^0 \end{aligned}$$

37 s'écrit donc en base 2 : 100101. En base 3, on a

$$\begin{aligned} 37 &= 3 \times 12 + 1 \\ &= 3 \times (3 \times 4) + 1 \\ &= 3 \times (3 \times (3 + 1)) + 1 \\ &= 3^3 + 3^2 + 3^0. \end{aligned}$$

37 s'écrit donc en base 3 : 1101.

---

**Correction de l'exercice 9 ▲**

1. On distingue plusieurs cas. Si $a$ et $b$ sont tous deux impairs, $a = 2k+1$ et $b = 2l+1$, alors $a^2 + b^2 = 4(k^2 + l^2 + k + l) + 2$ n'est pas un multiple de 4. Si $a$ est pair et $b$ est impair, $a = 2k$ et $b = 2l+1$, alors $a^2 + b^2 = 4(k^2 + l^2 + l) + 1$ n'est pas un multiple de 4. Le raisonnement est identique si $a$ est impair et $b$ est pair. Dans tous les cas, pour que $a^2 + b^2$ soit un multiple de 4, il est nécessaire que $a$ et $b$ soient pairs.

2. Imaginons qu'il existe au moins une solution à l'équation, et choisissons une solution $2^{2n} = a^2 + b^2$ avec $n$ le plus petit possible. Alors $n \geq 1$, car l'équation $2^0 = 1 = a^2 + b^2$ n'admet pas de solutions avec $a \geq 1$ et $b \geq 1$. Donc, $2^{2n}$ est un multiple de 4. D'après la question précédente, $a = 2k$ et $b = 2l$ sont des nombres pairs. Ainsi, on a encore

$$2^{2n} = 4k^2 + 4l^2 \iff 2^{2(n-1)} = k^2 + l^2.$$

Ainsi, on a trouvé une solution à l'équation avec $n-1<n$, ce qui contredit la minimalité de $n$. Donc l'équation n'admet aucune solution.

3. Démontrons par récurrence sur $n$ que l'équation (portant sur $a,b\in\mathbb{N}^*$) $2^{2n+1}=a^2+b^2$ admet pour unique solution $a=b=2^n$. Pour $n=0$, on doit résoudre $2=a^2+b^2$ avec $a,b\in\mathbb{N}^*$, ce qui entraîne bien $a=b=1$. Soit $n\in\mathbb{N}$ et supposons que la propriété est vraie au rang $n$. Prouvons-la au rang $n+1$. Alors, $2^{2n+3}$ est un multiple de 4. D'après la première question, si $a^2+b^2=2^{2(n+1)+1}$, alors $a=2k$, $b=2l$ et donc

$$2^{2n+1}=k^2+l^2.$$

Par hypothèse de récurrence, $k=l=2^n$, et donc $a=b=2^{n+1}$. La propriété est donc vraie au rang $n+1$. Par le principe de récurrence, elle est vraie pour tout $n\geq 0$.

---

**Correction de l'exercice 10 ▲**

1. En utilisant l'algorithme d'Euclide par exemple, on trouve que le pgcd de 390 et 525 est égal à 15. Les diviseurs communs de 390 et 525 sont les diviseurs de 15. Ces diviseurs (positifs) sont donc 1, 3, 5 et 15.

2. Notons $d$ le pgcd à calculer. Puisqu'il divise les deux nombres, il divise 25 et $d$ est donc égal à 1, 5 ou 25. S'il est égal à 5 ou 25, ceci signifie que 5 divise $3^{123}-5$. Mais alors, puisque 5 divise $-5$, ceci entrainerait encore que 5 divise $3^{123}$, ce qui n'est pas vrai. Donc $d=1$.

3. $n$ et $n+1$ sont deux entiers consécutifs. L'un des deux au moins est pair, et donc $2|n(n+1)(n+2)$. De même, $n$, $n+1$ et $n+2$ sont trois entiers consécutifs. L'un au moins est un multiple de 3, et donc $3|n(n+1)(n+2)$. Par le théorème de Gauss, puisque 2 et 3 sont premiers entre eux, $6|n(n+1)(n+2)$.

---

**Correction de l'exercice 11 ▲**

1. Commençons par remarquer que $2\wedge 5=1$ et donc, d'après le théorème de Bézout, l'équation admet toujours une solution. Ici, il est facile de remarquer que $(-1,1)$ est une solution particulière de l'équation. Considérons maintenant un couple d'entiers $(x,y)\in\mathbb{Z}^2$ tel que $2x+5y=3$. Alors, puisque $2\times(-1)+5\times 1=3$, on en déduit en soustrayant ces deux équations que

$$2(x+1)+5(y-1)=0 \iff 2(x+1)=-5(y-1).$$

On a donc $2|-5(y-1)$ et donc, puisque $2\wedge 5=1$, le théorème de Gauss assure que $2|y-1$. On en déduit l'existence de $k\in\mathbb{Z}$ tel que $y=1+2k$. Si on reporte ceci dans l'équation $2(x+1)=-5(y-1)$, on trouve que $x=-1-5k$. Réciproquement, tout couple d'entiers de la forme $(-1-5k,1+2k)$ avec $k\in\mathbb{Z}$ est solution de l'équation. Ainsi, on a prouvé que l'ensemble des solutions est

$$\mathscr{S}=\{(-1-5k,1+2k);\ k\in\mathbb{Z}\}.$$

2. On commence par rechercher le pgcd de 323 et 391 en appliquant par exemple l'algorithme d'Euclide. On a :

$$\begin{aligned}
391 &= 323\times 1+68\\
323 &= 68\times 4+51\\
68 &= 51\times 1+17\\
51 &= 17\times 3
\end{aligned}$$

Ainsi, le pgcd de 391 et 323 est 17. On vérifie que 17 divise 612, car $612=17\times 36$. D'autre part, $391=17\times 23$ et $323=17\times 19$. L'équation est donc équivalente à

$$19x-23y=36.$$

D'après le théorème de Bezout, puisque 19 et 23 sont premiers entre eux, on sait qu'il existe $(x_0,y_0)$ solution de $19x-23y=1$. Multipliant tout par 36, $(36x_0,36y_0)$ est solution de l'équation. Soit $(x,y)$ une solution de l'équation. Alors on a

$$19(x-36x_0)-23(y-36y_0)=0.$$

Ainsi, 19 divise $23(y-36y_0)$. Mais puisque 19 et 23 sont premiers entre eux, 19 divise $(y-36y_0)$ et donc il existe un entier $k$ tel que $y=36y_0+19k$. Reportant cela dans l'équation, on trouve que $x=36x_0+23k$. Réciproquement, il est facile de vérifier que tout couple $(36x_0+23k,36y_0+19k)$ est solution. Il suffit donc de déterminer un couple $(x_0,y_0)$. On applique une nouvelle fois l'algorithme d'Euclide :

$$\begin{aligned} 23 &= 19+4 \\ 19 &= 4\times 4+3 \\ 4 &= 3+1 \end{aligned}$$

soit, en remontant les calculs :

$$1=4-(19-4\times 4)=5\times 4-19=5\times(23-19)-19=5\times 23-6\times 19.$$

On peut donc prendre $x_0=-6$ et $y_0=-5$. L'ensemble des solutions de l'équation est donc

$$\{(-216+23k,-180+19k),\ k\in\mathbb{Z}\}.$$

3. On procède exactement comme ci-dessus, cette fois-ci, $162\wedge 207=9$ et on peut simplifier par 9. On trouve que l'ensemble des solutions est

$$\{(27-23k,-21+18k);\ k\in\mathbb{Z}\}.$$

4. Le pgcd de 221 et 247 est 13. Or, 13 ne divise pas 15. L'équation n'admet donc pas de solutions !

---

**Correction de l'exercice 12 ▲**

Supposons que $\ln(a)/\ln(b)$ est rationnel et soit $p,q\geq 1$ avec $p\wedge q=1$ tel que $\frac{\ln(a)}{\ln(b)}=\frac{p}{q}$. Ceci entraîne que $\ln(a^q)=\ln(b^p)$ et donc, par injectivité de la fonction ln, que $a^q=b^p$. Ainsi, $a|b^p$. Mais ceci contredit que $a\wedge b=1$.

---

**Correction de l'exercice 13 ▲**

Remarquons d'abord que si $a$ ou $b$ est nul, c'est trivial. On suppose donc que $a\neq 0$ et $b\neq 0$, et on écrit ces réels sous forme de fraction irréductible, $a=\frac{p_1}{q_1}$ et $b=\frac{p_2}{q_2}$, avec $q_1,q_2>0$ et $p_1\wedge q_1=1$, $p_2\wedge q_2=1$. On a alors

$$a+b=\frac{p_1q_2+p_2q_1}{q_1q_2}\in\mathbb{Z}.$$

On en déduit que $q_1|(p_1q_2+p_2q_1)$. Or, on sait déjà que $q_1|p_2q_1$. On a donc $q_1|p_1q_2$. De plus, puisque $q_1\wedge p_1=1$, le théorème de Gauss nous dit que $q_1|q_2$. Par symétrie, on a aussi $q_2|q_1$, et donc $q_1=q_2=q$. Le produit $ab$ vaut alors

$$ab=\frac{p_1p_2}{q^2},$$

et donc $q|p_1p_2$. Ceci implique (toujours par le lemme de Gauss) que $q|p_1$ et comme $q\wedge p_1=1$, on a $q\wedge p_1=q=1$. Ainsi, $a$ et $b$ sont des entiers.

---

**Correction de l'exercice 14 ▲**

1. Multiplions la relation $y_0=\frac{m}{n}x_0-\frac{p}{q}$ par $n$. On obtient

$$ny_0-mx_0=\frac{-pn}{q}.$$

Mais $ny_0-mx_0$ est un entier relatif que nous notons $r$. Donc $q(-r)=pn$, ce qui dit bien que $q$ divise le produit $pn$. Puisque $q$ et $p$ sont premier entre eux, ceci est une conséquence du théorème de Gauss.

2. Multiplions la relation $y_0=\frac{m}{n}x_0-\frac{p}{q}$ par $n$. On obtient

$$ny_0-mx_0=\frac{-pn}{q}.$$

Mais $ny_0 - mx_0$ est un entier relatif que nous notons $r$. Donc $q(-r) = pn$, ce qui dit bien que $q$ divise le produit $pn$.

3. Puisque $q$ et $p$ sont premier entre eux, ceci est une conséquence du théorème de Gauss.

4. Puisque $m$ et $n$ sont premiers entre eux, le théorème de Bézout nous dit qu'il existe deux entiers $u$ et $v$ tels que $nu - mv = 1$. Remplaçant $n$ par $qr$, on obtient le résultat voulu. Multiplions l'équation précédente par $\frac{-np}{q} = -pr$. On trouve

$$\frac{-np}{q} = -pqr^2u - (-prmv) = n(-pru) - m(-prv).$$

Posons alors $x_0 = -prv$ et $y_0 = -pru$. $x_0$ et $y_0$ sont bien deux entiers naturels. De plus, ils satisfont

$$\frac{-np}{q} = ny_0 - mx_0$$

équation qui est équivalente à

$$y_0 = \frac{m}{n}x_0 - \frac{p}{q}.$$

Le point de coordonnées $(x_0, y_0)$ est donc bien un élément de $\Delta$.

5. Puisque $m$ et $n$ sont premiers entre eux, le théorème de Bézout nous dit qu'il existe deux entiers $u$ et $v$ tels que $nu - mv = 1$. Remplaçant $n$ par $qr$, on obtient le résultat voulu.

6. Multiplions l'équation précédente par $\frac{-np}{q} = -pr$. On trouve

$$\frac{-np}{q} = -pqr^2u - (-prmv) = n(-pru) - m(-prv).$$

Posons alors $x_0 = -prv$ et $y_0 = -pru$. $x_0$ et $y_0$ sont bien deux entiers naturels. De plus, ils satisfont

$$\frac{-np}{q} = ny_0 - mx_0$$

équation qui est équivalente à

$$y_0 = \frac{m}{n}x_0 - \frac{p}{q}.$$

Le point de coordonnées $(x_0, y_0)$ est donc bien un élément de $\Delta$.

7. L'algorithme permet de déterminer s'il y a un point à coordonnées entières sur la droite $\Delta$ et, le cas échéant, d'afficher les coordonnées d'un de ces points. Pour cela, il commence par étudier la condition nécessaire et suffisante d'appartenance d'un tel point en étudiant si $q$ divise $n$. Ensuite, si $q$ divise $n$, il regarde s'il existe un point à coordonnées entières sur $\Delta$ dont l'abscisse est 0, puis $\pm 1$, puis $\pm 2$. L'algorithme va terminer puisqu'on sait qu'un tel point existe et que toutes les valeurs successives possibles des abscisses sont prises. De plus, l'algorithme va produire un point à coordonnées entières $(x_0, y_0)$ sur $\Delta$ avec $|x_0|$ minimum.

---

**Correction de l'exercice 15 ▲**

1. On remarque que $4(n^2+n) = (2n+1)^2 - 1$. Ainsi, si $d|(n^2+n)$ et $d|2n+1$, $d|1$. On a donc $(n^2+n) \wedge (2n+1) = 1$.

2. Rappelons que si $a = bq + r$, on a $a \wedge b = b \wedge r$ et que $a \wedge b = a \wedge (a-b)$ (on écrit $a = b + (a-b)$). Ainsi, on trouve ici

$$30n^2 + 21n + 13 = 2(15n^2 + 8n + 6) + 5n + 1, \quad 15n^2 + 8n + 6 = 3n(5n+1) + 5n + 6.$$

On a donc

$$\begin{aligned}(30n^2 + 21n + 13) \wedge (15n^2 + 8n + 6) &= (15n^2 + 8n + 6) \wedge (5n+1) \\ &= (5n+1) \wedge (5n+6) \\ &= (5n+1) \wedge 5 \\ &= 1.\end{aligned}$$

**Correction de l'exercice 16 ▲**

Soit $N$ le nombre de livres. L'information que l'on donne est que le reste dans la division euclidienne de $N$ par 10 (respectivement par 17) vaut 3 (respectivement 2). Ainsi, il existe $a$ et $b$ des entiers naturels tels que $N = 10a+3$ et $N = 17b+2$. Faisant la différence, on trouve que $(a,b)$ est une solution de l'équation de Bézout $17b-10a = 1$. On résoud cette équation. Le couple $(a,b) = (5,3)$ est solution, et donc les couples solutions sont les couples $(a,b)$ avec $a = 5+17k$ et $b = 3+10k$, avec $k \in \mathbb{N}$ (il n'y a pas de $-$ car l'équation de Bézout comporte déjà un $-$). Ainsi, si $N$ est le nombre de livres, il existe $k \in \mathbb{N}$ (car le nombre de livres est positif !) tel que $N = 53+170k$. Réciproquement, on vérifie que $53+170k = 10\times(17k+5)+3 = 17\times(10k+3)+2$. Le nombre minimal de livres possible est 53, les nombres possibles sont ceux de la forme $53+170k$ avec $k \in \mathbb{N}$. Bien sûr, le nombre minimal de livres possibles aurait pu être trouvé à l'aide d'un tableur.

**Correction de l'exercice 17 ▲**

Admettons qu'il existe une solution rationnelle $x = p/q$, avec $p \wedge q = 1$ et $q > 0$. Alors, remplaçant $x$ par $p/q$ dans l'équation et multipliant tout par $q^3$, on obtient :

$$p^3 - p^2q + pq^2 + q^3 = 0.$$

Puisque $q|p^2q+pq^2+q^3$, on obtient $q|p^3$ et donc $q = 1$ puisque $p$ et $q$ sont premiers entre eux. En effectuant le même raisonnement avec $p$, on obtient $p = \pm 1$. Or 1 et $-1$ ne sont pas solutions de l'équation. Il y a donc contradiction.

**Correction de l'exercice 18 ▲**

De la relation $u_{n+1} = 5u_n - 6$, on tire que tout diviseur commun de $u_n$ et de $u_{n+1}$ divise aussi 6. Ainsi, le pgcd de $u_n$ et $u_{n+1}$ ne peut qu'être un élément de $\{1,2,3,6\}$. Par ailleurs, on va démontrer par récurrence sur $n$ que 2 divise $u_n$ et que 3 ne divise pas $u_n$. C'est bien le cas pour $u_0 = 14$, et considérons $n \in \mathbb{N}$ tel que 2 divise $u_n$ et 3 ne divise pas $u_n$. Alors, $2|5u_n$ et 2 divise 6, donc 2 divise $u_{n+1} = 5u_n - 6$. De plus, si on avait $3|u_{n+1}$, alors $3|u_{n+1}+6$ et donc $3|5u_n$. De plus, par le théorème de Gauss, puisque $3 \wedge 5 = 1$, on tire $3|u_n$, ce qui est une contradiction. Ainsi, pour tout entier $n$, on a prouvé que $2|u_n$ et 3 ne divise pas $u_n$. Ainsi, si $d_n$ est le pgcd de $u_n$ et $u_{n+1}$, $2|d_n$ et 3 ne divise pas $d_n$. Puisque l'on sait déjà que $d_n \in \{1,2,3,6\}$, on a nécessairement $d_n = 2$.

**Correction de l'exercice 19 ▲**

1. Soit $(x,y)$ un tel couple d'entiers naturels. On écrit que $x = 18x'$ et $y = 18y'$ avec $x' \wedge y' = 1$. Puisque $x+y = 360$, on doit avoir $x'+y' = 20$. Si $x' = 1$, alors $y' = 19$ et cette solution convient car 1 et 19 sont premiers entre eux. Si $x' = 2$, alors $y' = 18$ et cette solution ne convient pas car 2 et 18 ne sont pas premiers entre eux. On peut continuer ainsi à chercher de façon exhaustive toutes les solutions, et on trouve que les couples qui conviennent correspondent à $x' = 1,3,7,9,11,13,17,19$. Les couples solutions sont donc :

$$(18,342),\ (54,306)\,(126,234),\ (162,198)$$

ainsi que les couples symétriques.

2. On procède exactement de la même façon, et cette fois on a l'équation $x'y' = 20$. Les solutions qui vérifient en outre que $x' \wedge y' = 1$ correspondent à $x' = 1,4,5$ et 20. Les couples solutions sont donc

$$(18,360),\ (72,90),\ (90,72),\ (360,18).$$

**Correction de l'exercice 20 ▲**

On pose $d = x \wedge y$ et on écrit $x = dx'$, $y = dy'$ et $x' \wedge y' = 1$. L'équation devient

$$d(x'y'+11) = 203 = 7\times 29.$$

On a donc $d = 1, 7, 29$ ou 203 et on sépare les cas.

Les cas $d = 29$ et $d = 203$ ne conduisent pas à une solution, puisqu'on a alors $x'y' = 7 - 11 < 0$ ou $x'y' = 1 - 11 < 0$, ce qui est impossible puisque $x'$ et $y'$ sont positifs. Pour $d = 1$, on a $x'y' = 192 = 2^6 \times 3$. Puisque $x' \wedge y' = 1$, on obtient que $(x', y')$ est un des couples $(192, 1)$, $(3, 2^6)$, $(2^6, 3)$ ou $(1, 192)$. Pour $d = 7$, on a $x'y' = 18 = 2 \times 3^2$. Puisque $x' \wedge y' = 1$, on obtient que $(x', y')$ est un des couples $(18, 1)$, $(2, 9)$, $(9, 2)$ ou $(1, 18)$.

En remultipliant par $d$, on trouve que l'ensemble des solutions est constitué par les couples $(1, 192)$, $(3, 64)$, $(7, 126)$, $(14, 63)$ et leurs symétriques.

---

**Correction de l'exercice 21 ▲**

1. On écrit $n = mq + r$ puis

$$\begin{aligned} a^n - a^r &= a^r (a^{mq} - 1) = a^r ((a^m)^q - 1) \\ &= a^r (a^m - 1) \left( a^{m(q-1)} + a^{m(q-2)} + \cdots + 1 \right) \end{aligned}$$

ce qui prouve le résultat.

2. De la relation précédente, on tire

$$(a^n - 1) - (a^r - 1) = Q (a^m - 1)$$

où $Q \in \mathbb{N}$. Ainsi, si $s$ divise $a^r - 1$ et $a^m - 1$, il divise $a^n - 1$. Réciproquement si $s$ divise $a^n - 1$ et $a^m - 1$, alors il divise $a^r - 1$. Ainsi, $d = (a^m - 1) \wedge (a^r - 1)$ (on utilise ici le même raisonnement que pour prouver que si $a = bq + c$, alors $a \wedge b = b \wedge c$). Mais, poursuivant les divisions euclidiennes successives, en notant $(r_k)$ la suite des restes obtenus, on a $d = (a^{r_k} - 1) \wedge (a^{r_{k+1}} - 1)$, jusqu'à ce que $a^{r_{k+1}} = 1$, c'est-à-dire $r_{k+1} = 0$. On a donc $d = a^{r_{k_0}} - 1$, où $r_{k_0}$ est le dernier reste non-nul dans l'algorithme d'Euclide, c'est-à-dire que $r_{k_0}$ est le pgcd de $n$ et $m$.

3. On a la suite d'équivalences :

$$\begin{aligned} a^m - 1 | a^n - 1 &\iff d = a^m - 1 \\ &\iff n \wedge m = m \\ &\iff m | n. \end{aligned}$$

---

**Correction de l'exercice 22 ▲**

1. On utilise le fait que $p$ divise $q$ si et seulement si le reste dans la division euclidienne de $q$ par $p$ est nul. def divise(p,q) : if ( (q return True else : return False

2. Un entier naturel est premier si ses seuls diviseurs positifs sont 1 et lui-même, et s'il n'est pas égal à 1. On sépare donc le traitement de 1, et pour les autres, on regarde si un des entiers entre 2 et $p - 1$ divise $p$. def estpremier(p) : if (p<2) : return 0 for i in range(2,p) : if divise(i,p) : return 0 return 1

3. def phi(n) : total=0 for m in range(2,n+1) : total+=estpremier(m) return total

---

**Correction de l'exercice 23 ▲**

1. Il suffit de développer prudemment le membre de gauche et de constater que les termes se simplifient bien deux par deux. Remarquer qu'il faut que $q$ soit impair pour que le signe devant le dernier 1 soit bien "+".

2. Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit un nombre premier. Si $m$ n'est pas une puissance de 2, alors $m$ s'écrit $pq$ où $p = 2^\alpha$ est un entier (éventuellement égal à 0), et $q$ est un nombre impair strictement supérieur à 1 (on obtient cette écriture en regroupant les nombres premiers impairs dans l'écriture en produit de facteurs premiers de $m$). On a alors :

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

Puisque $1 < 2^p + 1 < 2^m + 1$, on a obtenu une factorisation non triviale de $2^m + 1$ qui n'est donc pas un nombre premier. C'est absurde, et donc $m$ est une puissance de 2.

---

**Correction de l'exercice 24 ▲**

1. Montrons d'abord que $a = 2$. Pour cela, on factorise $a^n - 1$ sous la forme

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

$a-1$ est un diviseur de $a^n - 1$, distinct de $a^n - 1$. Si on suppose que $a^n - 1$ est premier, on a donc nécessairement $a - 1 = 1$, c'est-à-dire $a = 2$. De même, si $n = pq$, alors

$$2^{pq} - 1 = (2^p)^q - 1 = (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + \cdots + 2^p + 1).$$

Donc $2^p - 1$ divise $2^n - 1$ qui est premier. On a donc ou bien $p = n$ (si $2^p - 1 = 2^n - 1$) ou bien $p = 1$ (si $2^p - 1 = 1$). Donc les seuls diviseurs de $n$ sont 1 et $n$, i.e. $n$ est premier.

2. On a $M_{11} = 2047 = 23 \times 89$. On a donc $M_p$ premier implique $p$ premier, mais la réciproque est fausse.

**Correction de l'exercice 25 ▲**

1. Décomposons $n$ en produit de facteurs premiers : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Si $n$ n'admet aucun facteur premier congru à 3 modulo 4, ceci signifie que l'on a $p_i \equiv 2\ [4]$ ou $p_i \equiv 1\ [4]$ pour tout $i = 1, \ldots, r$ (le cas $p_i \equiv 0\ [4]$ est exclu puisque $p_i$ est premier). D'autre part, puisque $n$ est congru à 3 modulo 4, il est impair et aucun des $p_i$ n'est pair. On a donc pour tout $i = 1, \ldots, r$, $p_i \equiv 1\ [4]$ et donc $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \equiv 1\ [4]$, une contradiction.

2. Supposons qu'il en existe simplement un nombre fini, notés $p_1, \ldots, p_k$ et posons $n$ le produit de tous ces nombres :

$$n = p_1 \times \cdots \times p_k = 3 \times 7 \times 11 \times 19 \times \ldots.$$

Considérons alors $m = 4n - 1$. Alors $m$ est congru à 3 modulo 4. Par la question précédente, $m$ admet un diviseur premier congru à 3 modulo 4 et donc il existe $i \in \{1, \ldots, k\}$ tel que $p_i | m = 4n - 1$. Écrivant $1 = 4n - m$, on trouve que $p_i | 1$ puisque $p_i | m$ et $p_i | n$, ce qui est une contradiction.

**Correction de l'exercice 26 ▲**

Soit $n \geq 1$ et $I = \{n! + 2, n! + 3, \ldots, n! + n\}$. Prenons un entier $m = n! + k$ dans $I$. Alors $k$ est un diviseur strict de $m$, puisque $1 < k < m$, et $k | k$, $k | n!$ puisque $k \leq n$, donc $k | m$. Ainsi, $I$ est un intervalle de $(n-1)$ entiers ne comportant pas de nombres premiers. Si on a choisi $n = q + 1$, alors on a répondu au problème posé par l'énoncé.

**Correction de l'exercice 27 ▲**

Décomposons $a$ et $b$ en produit de facteurs premiers :

$$a = \prod_{i=1}^{r} p_i^{\alpha_i},\ b = \prod_{i=1}^{r} p_i^{\beta_i}.$$

On a donc

$$a^2 = \prod_{i=1}^{r} p_i^{2\alpha_i},\ b^2 = \prod_{i=1}^{r} p_i^{2\beta_i}.$$

La condition $a^2 | b^2$ se traduit par, pour tout $i = 1, \ldots, r$, $2\alpha_i \leq 2\beta_i$. Mais ceci entraîne que $\alpha_i \leq \beta_i$ et donc que $a | b$.

**Correction de l'exercice 28 ▲**

1. Détaillons d'abord ce que signifie la question. Soit $n$ un entier qui est à la fois un carré et un cube, i.e. $n = a^2$ et $n = b^3$. On veut prouver que c'est le carré d'un cube, c'est-à-dire qu'il existe un entier $c$ tel que $n = (c^3)^2 = c^6$. Décomposons $n$, $a$ et $b$ en produit de facteurs premiers :

$$\begin{aligned} n &= p_1^{n_1} \ldots p_r^{n_r} \\ a &= p_1^{\alpha_1} \ldots p_r^{\alpha_r} \\ b &= p_1^{\beta_1} \ldots p_r^{\beta_r} \end{aligned}$$

Par unicité de la décomposition en produit de facteurs premiers, puisque $n = a^2$, on a $n_i = 2\alpha_i$, et puisque $n = b^3$, on a $n_i = 3\beta_i$ pour tout $i \in \{1,\dots,r\}$. Ainsi chaque $n_i$ est multiple de 2 et de 3. C'est donc aussi un multiple de 6 et $n_i = 6\gamma_i$. Posons alors

$$c = p_1^{\gamma_1} \dots p_r^{\gamma_r}.$$

Alors $c^6 = n$.

2. Décomposons $a$ et $b$ en produit de facteurs premiers, $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \dots p_r^{\beta_r}$. L'égalité $a^p = b^q$ se traduit par $p\alpha_j = q\beta_j$ pour tout $j = 1,\dots,r$. On a donc $q | p\alpha_j$ et puisque $p \wedge q = 1$, on obtient $q|\alpha_j$. Ecrivons $\alpha_j = q\gamma_j$ et reportons. On trouve $pq\gamma_j = q\beta_j$ soit $\beta_j = p\gamma_j$. Ainsi, si on pose $c = p_1^{\gamma_1} \dots p_r^{\gamma_r}$ on a bien $n = c^{pq}$.

---

**Correction de l'exercice 29 ▲**

Décomposons $a, b$ et $ab$ en produit de facteurs premiers, $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \dots p_r^{\beta_r}$, $ab = p_1^{2\gamma_1} \dots p_r^{2\gamma_r}$ (on a utilisé que $ab$ est un carré parfait). Bien sûr, pour tout $j$, on a la relation $2\gamma_j = \alpha_j + \beta_j$. De plus, puisque $a \wedge b = 1$, si $\alpha_j$ est non-nul, alors $\beta_j = 0$, et réciproquement. On a alors ou bien $\alpha_j = 2\gamma_j$ et $\beta_j = 0$, ou bien $\beta_j = 2\gamma_j$ et $\alpha_j = 0$. Dans tous les cas, $\alpha_j$ et $\beta_j$ sont tous les deux pairs. Ainsi, $a$ et $b$ sont des carrés parfaits.

---

**Correction de l'exercice 30 ▲**

1. On décompose $a$, $b$ et $c$ en produit de facteurs premiers :

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r},\ b = p_1^{\beta_1} \dots p_r^{\beta_r},\ c = p_1^{\gamma_1} \dots p_r^{\gamma_r}$$

(on s'autorise à ce que les $\alpha_i$, les $\beta_i$ et les $\gamma_i$ soient nuls). La condition $c|ab$ signifie que $\gamma_j \leq \alpha_j + \beta_j$ pour tout $j$. De plus, on a

$$a \wedge c = p_1^{\min(\alpha_1,\gamma_1)} \dots p_r^{\min(\alpha_r,\gamma_r)}$$
$$b \wedge c = p_1^{\min(\beta_1,\gamma_1)} \dots p_r^{\min(\beta_r,\gamma_r)}$$

et donc on a $c|(a \wedge c)(b \wedge c)$ si et seulement si, pour tout $j$ de $1,\dots,r$, on a

$$\gamma_j \leq \min(\alpha_j,\gamma_j) + \min(\beta_j,\gamma_j).$$

Mais si $\min(\alpha_j,\gamma_j) = \gamma_j$ ou $\min(\beta_j,\gamma_j) = \gamma_j$, c'est trivial. Sinon on a

$$\min(\alpha_j,\gamma_j) + \min(\beta_j,\gamma_j) = \alpha_j + \beta_j \geq \gamma_j$$

par hypothèse. Ceci prouve le résultat.

2. Écrivons à nouveau

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r},\ b = p_1^{\beta_1} \dots p_r^{\beta_r}$$

et posons $\gamma_j = \min(\alpha_j,\beta_j)$. Alors

$$a \wedge b = p_1^{\gamma_1} \dots p_r^{\gamma_r} \implies (a \wedge b)^n = p_1^{n\gamma_1} \dots p_r^{n\gamma_r}.$$

De même,

$$a^n = p_1^{n\alpha_1} \dots p_r^{n\alpha_r},\ b^n = p_1^{n\beta_1} \dots p_r^{n\beta_r}$$

de sorte que

$$a^n \wedge b^n = p_1^{\delta_1} \cdots p_r^{\delta_r}$$

avec $\delta_j = \min(n\alpha_j, n\beta_j) = n\min(\alpha_j,\beta_j) = n\gamma_j$.

3. Soit $d = (a^2 + ab + b^2) \wedge ab$. On peut commencer par remarquer que $d = (a^2 + b^2) \wedge ab$. Décomposons $a$, $b$ et $d$ en produits de facteurs premiers :

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r}, b = p_1^{\beta_1} \dots p_r^{\beta_r},\ d = p_1^{\gamma_1} \dots p_r^{\gamma_r}.$$

Puisque $d|ab$, on a $\gamma_j \leq \alpha_j + \beta_j$ pour tout $j$. Si $\alpha_j = \beta_j$, on en déduit que $\gamma_j \leq 2\min(\alpha_j,\beta_j)$. Si maintenant $\alpha_j \neq \beta_j$, on peut supposer $\alpha_j < \beta_j$, alors

$$a^2 + b^2 = p_j^{2\alpha_j}(q + p_j^{2\beta_j - 2\alpha_j} r)$$

avec $q \wedge p_j = 1$. En particulier, $(q + p_j^{2\beta_j - 2\alpha_j} r) \wedge p_j = 1$, et donc $\gamma_j \leq 2\alpha_j = 2\min(\alpha_j, \beta_j)$. Ceci démontre en particulier que $d | a^2 \wedge b^2$. Réciproquement, on va prouver que $a^2 \wedge b^2 | ab$. Puisqu'il est clair qu'on a aussi $a^2 \wedge b^2 | a^2 + b^2$, on pourra conclure que $d = a^2 \wedge b^2$. Mais

$$ab = p_1^{\alpha_1+\beta_1} \dots p_r^{\alpha_r+\beta_r} \text{ et } a^2 \wedge b^2 = p_1^{\min(2\alpha_1, 2\beta_1)} \dots p_r^{\min(2\alpha_r, 2\beta_r)}$$

ce qui prouve ce que l'on voulait.

---

**Correction de l'exercice 31 ▲**

1. Un diviseur de $n$ s'écrit de façon unique sous la forme $d = p_1^{\beta_1} \dots p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$ pour $i = 1, \dots, r$. Notant $I_i = \{0, \dots, \alpha_i\}$, on a donc une bijection de $I_1 \times \dots \times I_r$ sur $\{\text{diviseurs de n}\}$ donné par

$$(\beta_1, \dots, \beta_r) \mapsto p_1^{\beta_1} \dots p_r^{\beta_r}.$$

Les deux ensembles ont même cardinal, et donc $d(n) = \prod_{i=1}^r (\alpha_i + 1)$.

2. Rappelons qu'un produit de nombre entiers est impair si et seulement si tous ses facteurs sont impairs. On en déduit

$$\begin{aligned} d(n) \text{ est impair} &\iff \forall i \in \{1, \dots, r\}, \alpha_j + 1 \text{ est impair} \\ &\iff \forall i \in \{1, \dots, r\},\ \alpha_j \text{ est pair} \\ &\iff n \text{ est un carré parfait.} \end{aligned}$$

3. L'idée est de regrouper ensemble les facteurs $d$ et $n/d$. Si le premier est inférieur à $\sqrt{n}$, le second est supérieur à $\sqrt{n}$. Précisément, si $n$ n'est pas un carré parfait :

$$\prod_{d|n} d = \prod_{d|n, d<\sqrt{n}} d \times \frac{n}{d} = \prod_{d|n, d<\sqrt{n}} n = n^{d(n)/2}.$$

Si $n$ est un carré parfait, $n = m^2$, alors

$$\prod_{d|n} d = m \prod_{d|n, d<\sqrt{n}} d \times \frac{n}{d} = n^{1/2} n^{(d(n)-1)/2} = n^{d(n)/2}.$$

---

**Correction de l'exercice 32 ▲**

1. Un multiple de $u$ s'écrit $ku$. Soit $mu$ le plus grand multiple dans $\{1, \dots, n\}$. Alors $um \leq n < u(m+1)$ et donc

$$m \leq \frac{n}{u} < m + 1.$$

Puisque $m$ est un entier, on reconnait $m = \left\lfloor \frac{n}{u} \right\rfloor$. Les multiples de $u$ dans $\{1, \dots, n\}$ étant les entiers $ku$, avec $1 \leq k \leq m$, on déduit que leur nombre est égal à $\left\lfloor \frac{n}{u} \right\rfloor$.

2. Soit $l \in \{1, \dots, n\}$. Alors $\nu_p(l) = k$ si et seulement si $p^k$ divise $l$ mais $p^{k+1}$ ne divise pas $l$. D'après la question précédente, on déduit que

$$\text{card}(A_k) = \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor.$$

3. On commence par écrire

$$\begin{aligned} \nu_p(n!) &= \sum_{l=1}^{n} \nu_p(l) \\ &= \sum_{k=1}^{N} k \,\text{card}\left(\{l \in \{1, \dots, n\} :\ \nu_p(l) = k\}\right) \end{aligned}$$

où on a regroupé les éléments de $\{1,\dots,n\}$ suivant leur valuation $p$-adique. En utilisant le résultat de la question précédente,

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{N} k\left(\left\lfloor \frac{n}{p^k}\right\rfloor - \left\lfloor \frac{n}{p^{k+1}}\right\rfloor\right) \\ &= \sum_{k=1}^{N} k\left\lfloor \frac{n}{p^k}\right\rfloor - \sum_{k=1}^{N} k\left\lfloor \frac{n}{p^{k+1}}\right\rfloor \\ &= \sum_{k=1}^{N} k\left\lfloor \frac{n}{p^k}\right\rfloor - \sum_{k=2}^{N+1} (k-1)\left\lfloor \frac{n}{p^k}\right\rfloor \\ &= \sum_{k=1}^{N} \left\lfloor \frac{n}{p^k}\right\rfloor - N\left\lfloor \frac{n}{p^{N+1}}\right\rfloor \\ &= \sum_{k=1}^{N} \left\lfloor \frac{n}{p^k}\right\rfloor \end{aligned}$$

où la dernière ligne vient du fait que $p^{N+1} > n$.

4. Il suffit de calculer la plus grande puissance $N$ telle que $10^N | 1000!$. Comme $10 = 2\times 5$, on obtient $N = \min(v_2(1000!), v_5(1000!))$. En utilisant la formule de Legendre, on trouve

$$\begin{aligned} v_5(1000!) &= \left\lfloor \frac{1000}{5}\right\rfloor + \left\lfloor \frac{1000}{25}\right\rfloor + \left\lfloor \frac{1000}{125}\right\rfloor + \left\lfloor \frac{1000}{625}\right\rfloor \\ &= 249 \\ v_2(1000!) &\geq \left\lfloor \frac{1000}{2}\right\rfloor = 500. \end{aligned}$$

Ainsi, 1000! se termine par 249 zéros.

---

**Correction de l'exercice 33 ▲**

Remarquons d'abord que $45^{42}$ se décompose en facteurs premiers sous la forme $3^{84}5^{42}$. Ainsi, un entier $n$ dont le produit des diviseurs est égal à $45^{42}$ est forcément de la forme $3^p5^q$. Maintenant, les diviseurs d'un tel entier sont tous les nombres de la forme $3^k5^l$ avec $0\leq k\leq p$ et $0\leq l\leq q$. Ainsi, le produit de ces diviseurs est égal à

$$\begin{aligned} \prod_{k=0}^{p}\prod_{l=0}^{q} 3^k5^l &= \prod_{k=0}^{p}\left(3^{k(q+1)}\prod_{l=0}^{q}5^l\right) \\ &= \prod_{k=0}^{p}\left(3^{k(q+1)}5^{\frac{q(q+1)}{2}}\right) \\ &= 3^{\frac{p(p+1)(q+1)}{2}}5^{\frac{q(q+1)(p+1)}{2}}. \end{aligned}$$

$p$ et $q$ sont donc solutions du système

$$\begin{cases} p(p+1)(q+1) &= 168 \\ q(q+1)(p+1) &= 84. \end{cases}$$

Si on fait le quotient de ces deux équations, on obtient $p = 2q$, ce qui donne encore

$$q(q+1)(2q+1) = 84.$$

La seule solution est $q = 3$ et donc $p = 6$. Ainsi, il y a un unique entier naturel dont le produit des diviseurs est $45^{42}$. Il s'agit de $3^65^3$.

---

**Correction de l'exercice 34 ▲**

1. La méthode pour ce type d'exercice est toujours la même et est très importante à savoir. On commence par rechercher le premier entier $k \geq 1$ tel que $2^k \equiv 1\ [5]$. On va ensuite raisonner modulo $k$. On trouve successivement :

$$2^1 \equiv 2\ [5], \quad 2^2 \equiv 4\ [5], \quad 2^3 \equiv 3\ [5], \quad 2^4 \equiv 1\ [5].$$

On va donc classer les entiers $n$ modulo 4. En effet, si $n = 4q + r$, alors sachant que $2^{4q} \equiv 1^q\ [5]$ soit $2^{4q} \equiv 1\ [5]$, on trouve que

$$2^n \equiv 2^r\ [5].$$

Ainsi, on obtient

Si $n \equiv 0\ [4]$, alors $2^n \equiv 1\ [5]$ ; Si $n \equiv 1\ [4]$, alors $2^n \equiv 2\ [5]$ ; Si $n \equiv 2\ [4]$, alors $2^n \equiv 4\ [5]$ ; Si $n \equiv 3\ [4]$, alors $2^n \equiv 3\ [5]$ ;

2. Si $n \equiv 0\ [4]$, alors $2^n \equiv 1\ [5]$ ;
3. Si $n \equiv 1\ [4]$, alors $2^n \equiv 2\ [5]$ ;
4. Si $n \equiv 2\ [4]$, alors $2^n \equiv 4\ [5]$ ;
5. Si $n \equiv 3\ [4]$, alors $2^n \equiv 3\ [5]$ ;
6. On commence par effectuer la division euclidienne de 1357 par 5, et on trouve que $1357 \equiv 2\ [5]$, d'où $1357^{2013} \equiv 2^{2013}\ [5]$. De plus, $2013 \equiv 1\ [4]$. On en déduit que $1357^{2013} \equiv 2^1 \equiv 2\ [5]$.

---

**Correction de l'exercice 35 ▲**

Puisque $6 = 2 \times 3$ avec $2 \wedge 3 = 1$, il suffit de prouver que $n(n+2)(7n-5)$ est divisible par 2 et est divisible par 3. Commençons par la divisibilité par 2. On va raisonner par disjonction de cas. Si $n \equiv 0\ [2]$, alors clairement $n(n+2)(7n+5) \equiv 0\ [2]$. Si $n \equiv 1\ [2]$, alors $7n-5 \equiv 2\ [2]$ et donc $7n+5 \equiv 0\ [2]$. A nouveau, on a $n(n+2)(7n+5) \equiv 0\ [2]$. Étudions maintenant la divisibilité par 3. On raisonne encore par disjonction de cas, le cas $n \equiv 0\ [3]$ se traite comme précédemment. Si $n \equiv 1\ [3]$, on conclut en utilisant que $n+2 \equiv 0\ [3]$ et si $n \equiv 2\ [3]$, on conclut en remarquant que $7n-5 \equiv 9\ [3]$ et donc $7n-5 \equiv 0\ [3]$.

---

**Correction de l'exercice 36 ▲**

1. Le plus facile est de remarquer que, d'après le petit théorème de Fermat, $n^5 \equiv n\ [5]$, ce qui est exactement le résultat demandé.

2. La vérification est immédiate. On remarque alors que, parmi $n$ et $n-1$, l'un des deux entiers est pair, et donc $2|a$. De la même façon, parmi les 3 entiers consécutifs $n-1$, $n$ et $n+1$, l'un au moins est divisible par 3 et donc $3|a$.

3. Puisque $2 \wedge 3 = 1$, puisque $2|a$ et $3|a$, on sait que $6|a$. Puisque $5 \wedge 6 = 1$ et que $5|a$, $6|a$, on en déduit que $30|a$.

---

**Correction de l'exercice 37 ▲**

On développe $n^3 + (n+1)^3 + (n+2)^3$ :

$$n^3 + (n+1)^3 + (n+2)^3 = 3n^3 + 9n^2 + 15n + 9 = 9(n^2+1) + 3n(n^2+5).$$

Il suffit donc de démontrer que $9|3n(n^2+5)$ ou encore que $3|n(n^2+5)$. Si $n \equiv 0\ [3]$, c'est bien sûr vrai. Si $n \equiv 1\ [3]$, on a $n^2 \equiv 1\ [3]$ et donc $n^2+5 \equiv 6 \equiv 0\ [3]$. Si $n \equiv 2\ [3]$, alors $n^2+5 \equiv 4+5 \equiv 9 \equiv 0\ [3]$. Dans tous les cas, $3n(n^2+5)$ est divisible par 9.

---

**Correction de l'exercice 38 ▲**

1. On calcule les premiers termes et on trouve $5^0 \equiv 1\ [13]$, $5^1 \equiv 5\ [13]$, $5^2 \equiv -1\ [13]$, $5^3 \equiv -5\ [13]$, $5^4 \equiv 1\ [13]$, $5^5 \equiv 5\ [13]$, $5^6 \equiv -1\ [13]$,... On voit clairement apparaître le cycle $1, 5, -1, -5, 1, 5, -1$, ce qui nous incite à démontrer par récurrence sur $\sqrt{} \in \mathbb{N}$ la propriété $\mathscr{P}(p)$ suivante :

$$\mathscr{P}(p) = \text{"}5^{4p} \equiv 1\ [13],\ 5^{4p+1} \equiv 5\ [13],\ 5^{4p+2} \equiv -1\ [13],\ 5^{4p+3} \equiv -5\ [13]\text{"}.$$

La propriété $\mathscr{P}(0)$ est vraie comme le montre le calcul précédent. Soit $p \in \mathbb{N}$ tel que $\mathscr{P}(p)$ est vraie, et prouvons $\mathscr{P}(p+1)$. Alors on a

$$5^{4(p+1)} = 5^{4p}5^4 \equiv 1 \times 1 \equiv 1\ [13].$$

La démonstration pour les trois autres cas est exactement similaire. Donc $\mathscr{P}(p+1)$ est vraie. Ainsi, les entiers naturels solutions de $5^n \equiv -1\ [13]$ sont exactement les entiers de la forme $4p+2$, avec $p \in \mathbb{N}$.

2. Écrivons $5^{2n} + 5^n = 5^n(5^n+1)$. Si $13|5^{2n}+5^n$, puisque $5 \wedge 13 = 1$, le théorème de Gauss assure que $13|5^n+1$, autrement dit que $5^n \equiv -1\ [13]$. D'après la question précédente, ceci est équivalent à dire que $n = 4p+2$, avec $p \in \mathbb{N}$. Réciproquement, si $n = 4p+2$ pour un certain $p \in \mathbb{N}$, on sait que $13|5^n+1$ et donc $13|5^n(5^n+1) = 5^{2n}+5^n$. Les entiers $n$ solutions sont donc exactement ceux qui s'écrivent $4p+2$ avec $p \in \mathbb{N}$.

---

**Correction de l'exercice 39 ▲**

Puisque $a \equiv b\ [n]$, il existe $k \in \mathbb{Z}$ tel que $a = b+kn$. Mettons ceci à la puissance $n$. On en déduit que

$$\begin{aligned} a^n &= (b+kn)^n \\ &= \sum_{j=0}^{n} \binom{n}{j} b^{n-j}k^j n^j \\ &= b^n + \binom{n}{1} b^{n-1}kn + \sum_{j=2}^{n} \binom{n}{j} b^{n-j}k^j n^j \\ &= b^n + b^{n-1}kn^2 + n^2 \sum_{j=2}^{n} \binom{n}{j} b^{n-j}k^j n^{j-2}. \end{aligned}$$

Puisque pour tout $j \geq 2$, $\binom{n}{j} b^{n-j}k^j n^{j-2}$ est un entier, on en déduit que $a^n = b^n + \ell n^2$ avec $\ell \in \mathbb{Z}$ et donc que $a^n \equiv b^n\ [n^2]$.

---

**Correction de l'exercice 40 ▲**

Le point crucial est que 10 est congru à 1 modulo 9. Ainsi, $10^2 = 10 \times 10 \equiv 1 \times 1 = 1[9]$, et une récurrence facile montre que pour tout entier $k$, alors $10^k$ est congru à 1 modulo 9. Notons $x = \overline{a_n \ldots a_0}$. Alors on a :

$$\begin{aligned} x &\equiv 10^n a_n + 10^{n-1}a_{n-1} + \cdots + 10a_1 + a_0\ [9] \\ &\equiv a_n + a_{n-1} + \cdots + a_0\ [9]. \end{aligned}$$

La deuxième partie de l'exercice s'en déduit aisément. En effet, on écrit que

$$xy = z \implies xy \equiv z\ [9] \implies \left(\sum_{i=0}^{n} a_i\right)\left(\sum_{i=0}^{m} b_i\right) \equiv \left(\sum_{i=0}^{p} c_i\right)\ [9].$$

---

**Correction de l'exercice 41 ▲**

1. On écrit l'équations modulo 5, et on trouve que $x^2 \equiv 3\ [5]$. Or, si $x \equiv \pm 1\ [5]$, alors $x^2 \equiv 1\ [5]$ et si $x \equiv \pm 2\ [5]$, alors $x^2 \equiv 4\ [5]$ et donc l'équation $x^2 = 3\ [5]$ n'a pas de solutions. Ainsi, l'équation de départ n'a pas de solutions dans $\mathbb{Z}^2$.

2. On écrit l'équation modulo 5, et on trouve $-8y^2 \equiv 4\ [5]$ et donc $2y^2 \equiv 4\ [5]$ puisque $-8 \equiv 2\ [5]$. Mais : si $y \equiv 0\ [5]$, alors $2y^2 \equiv 0\ [5]$ ; si $y \equiv \pm 1\ [5]$, alors $2y^2 \equiv 2\ [5]$ ; si $y \equiv \pm 2\ [5]$, alors $2y^2 \equiv 8\ [5] \equiv 3\ [5]$. Dans tous les cas, il est impossible que $2y^2 \equiv 4\ [5]$. Ainsi, l'équation n'admet pas de solutions.

3. si $y \equiv 0\ [5]$, alors $2y^2 \equiv 0\ [5]$ ;

4. si $y \equiv \pm 1\ [5]$, alors $2y^2 \equiv 2\ [5]$ ;

5. si $y \equiv \pm 2\ [5]$, alors $2y^2 \equiv 8\ [5] \equiv 3\ [5]$.

---

**Correction de l'exercice 42 ▲**

Notons, pour $n \in \mathbb{N}$, la propriété $\mathscr{P}(n)$ ="$3^{2n+1}+2^{4n+2}$ est divisible par 7". Prouvons par récurrence que pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vérifiée. Initialisation : On a $3^1+2^2=7$ qui est bien divisible par 7. Hérédité : Soit $n \in \mathbb{N}$ tel que $\mathscr{P}(n)$ est vraie. Remarquons que $3^2 \equiv 2\ [7]$ et que $2^4 \equiv 2\ [7]$. Alors, on écrit (modulo 7) :

$$\begin{aligned} 3^{2n+3}+2^{4n+6} &\equiv 3^2 3^{2n+1}+2^4 2^{4n+2}\ [7] \\ &\equiv 2\times 3^{2n+1}+2\times 2^{4n+2}\ [7] \\ &\equiv 2\times(3^{2n+1}+2^{4n+2})\ [7] \\ &\equiv 2\times 0\ [7] \\ &\equiv 0\ [7]. \end{aligned}$$

Ainsi, 7 divise $3^{2n+3}+2^{4n+6}$ et donc $\mathscr{P}(n+1)$ est vraie. En conclusion, par le principe de récurrence, $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

---

**Correction de l'exercice 43 ▲**

1. Puisque $a$ s'écrit $a=\sum_{i=0}^{n} a_i 10^i$, il suffit de démontrer que pour tout $i \geq 0$, $10^i \equiv r_i\ [m]$. On va démontrer ce résultat par récurrence sur $i$. La propriété est clairement vérifiée pour $i=0$. Supposons qu'elle est vraie au rang $i$, à savoir $r_i \equiv 10^i\ [m]$, et prouvons-la au rang $i+1$. On a $10^{i+1} \equiv 10 r_i\ [m]$ et par définition de $r_{i+1}$, on a aussi $r_{i+1} \equiv 10 r_i\ [m]$. Ainsi, on a bien $10^{i+1} \equiv r_{i+1}\ [m]$, ce qui achève de prouver que, pour tout $i \geq 0$, on a $10^i \equiv r_i\ [m]$.

2. Pour chaque valeur proposée (3,6,9,10), on va étudier le comportement de la suite $r_i$ afin d'en déduire le critère de divisibilité proposé.

Pour 3, on va prouver que $r_i$ est toujours égal à 1. C'est vrai pour $i=0$, et si c'est vrai au rang $i$, alors

$$10^{r_i} = 10 = 3\times 3+1,$$

et donc $r_{i+1}=1$. On a donc prouvé qu'un nombre est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3. Pour 9, le raisonnement est similaire, et on prouve qu'un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9. Pour 10, on a $r_0=1$, $r_1=0$ et on prouve par une récurrence immédiate que $r_i=0$ pour $i \geq 1$. Un nombre est donc divisible par 10 si et seulement si son dernier chiffre est nul (bien sûr, on le savait déjà !). Pour 11, on remarque que $r_0=1$, que $r_1=10$, puisque que $r_2=1$, $r_3=10,\ldots$. On prouve donc par récurrence sur $k$ que $r_{2k}=1$ et $r_{2k+1}=10$. C'est vrai pour $k=0$, et si c'est vrai au rang $k$, alors

$$10 r_{2k+1} = 100 = 9\times 11+1,$$

ce qui prouve que $r_{2k+2}=1$. Il vient ensuite $r_{2k+3}=10$, ce qui prouve l'assertion par récurrence. Pour en déduire un critère de divisibilité commode, on remarque que $10 \equiv -1\ [11]$. $a$ est donc divisible par 11 si et seulement si $\sum_{k=0}^{n}(-1)^k a_k$ est divisible par 11.

3. Pour 3, on va prouver que $r_i$ est toujours égal à 1. C'est vrai pour $i=0$, et si c'est vrai au rang $i$, alors

$$10^{r_i} = 10 = 3\times 3+1,$$

et donc $r_{i+1}=1$. On a donc prouvé qu'un nombre est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

4. Pour 9, le raisonnement est similaire, et on prouve qu'un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9.

5. Pour 10, on a $r_0=1$, $r_1=0$ et on prouve par une récurrence immédiate que $r_i=0$ pour $i \geq 1$. Un nombre est donc divisible par 10 si et seulement si son dernier chiffre est nul (bien sûr, on le savait déjà !).

6. Pour 11, on remarque que $r_0=1$, que $r_1=10$, puisque que $r_2=1$, $r_3=10,\ldots$. On prouve donc par récurrence sur $k$ que $r_{2k}=1$ et $r_{2k+1}=10$. C'est vrai pour $k=0$, et si c'est vrai au rang $k$, alors

$$10 r_{2k+1} = 100 = 9\times 11+1,$$

ce qui prouve que $r_{2k+2}=1$. Il vient ensuite $r_{2k+3}=10$, ce qui prouve l'assertion par récurrence. Pour en déduire un critère de divisibilité commode, on remarque que $10 \equiv -1\ [11]$. $a$ est donc divisible par 11 si et seulement si $\sum_{k=0}^{n}(-1)^k a_k$ est divisible par 11.

**Correction de l'exercice 44 ▲**

1. On commence par rechercher un entier $a$ tel que $5a \equiv 1\ [17]$ (on dit que $a$ est un inverse de 5 modulo 17). On cherche donc $a \in \mathbb{Z}$ tel qu'il existe $k \in \mathbb{Z}$ avec $5a = 1 + 17k$. On cherche donc les coefficients d'une relation de Bézout. On peut bien sûr appliquer l'algorithme d'Euclide pour les déterminer, mais ici il est facile de constater que $5 \times 7 = 1 + 17 \times 2$. Autrement dit, $5 \times 7 \equiv 1\ [17]$. Soit maintenant $x \in \mathbb{Z}$ une solution de l'équation. Alors en multipliant l'équation $5x \equiv 3\ [17]$ par 7, on trouve $35x \equiv 21\ [17]$ et comme $35 \equiv 1\ [17]$ et $21 \equiv 4\ [17]$, on obtient finalement $x \equiv 4\ [17]$ c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $x = 4 + 17k$. Réciproquement, si $x$ s'écrit $4 + 17k$, alors $5x = 20 + 17 \times (5k)$ et donc

$$\begin{aligned} 5x &\equiv 20\ [17] \\ &\equiv 3\ [17]. \end{aligned}$$

L'ensemble des solutions est donc $\{4 + 17k :\ k \in \mathbb{Z}\}$.

2. On remarque que

$$\begin{aligned} 10x \equiv 6\ [34] &\iff \exists k \in \mathbb{Z},\ 10x = 6 + 34k \\ &\iff \exists k \in \mathbb{Z},\ 5x = 3 + 17k \\ &\iff 5x \equiv 3\ [17] \\ &\iff \exists k \in \mathbb{Z},\ x = 4 + 17k. \end{aligned}$$

3. Dans ce cas, l'équation n'admet pas de solutions. En effet, si $x$ est solution, alors il existe $k \in \mathbb{Z}$ tel que $10x = 5 + 34k$ soit $5 = 10x - 34k$. Mais ceci est impossible car 2 divise le membre de droite de l'égalité, mais pas le membre de gauche.

**Correction de l'exercice 45 ▲**

Soit $x$ une solution du système. Puisque $x \equiv 1\ [5]$, il existe $k \in \mathbb{Z}$ tel que $x = 1 + 5k$. Reportant dans la deuxième équation, on trouve $1 + 5k \equiv 2\ [11]$ soit $5k \equiv 1\ [11]$. Multiplions ceci par 2. Puisque $10 \equiv -1\ [11]$, on obtient

$$-k \equiv 2\ [11] \iff k \equiv -2\ [11].$$

Il existe donc $\ell \in \mathbb{Z}$ tel que $k = -2 + 11\ell$. Finalement, on a prouvé que si $x$ est solution, alors $x = 1 - 10 + 55\ell = -9 + 55\ell$, $\ell \in \mathbb{Z}$. Réciproquement, si $x = -9 + 55\ell$, $\ell \in \mathbb{Z}$, on écrit $x = 1 + 5 \times (-2 + 11\ell)$ puis $x = 2 + 11 \times (-1 + 5\ell)$ pour prouver que $x$ est bien solution du système.

**Correction de l'exercice 46 ▲**

Écrivons un tel nombre $n = a_1 \ldots a_p a_p \ldots a_1$, c'est-à-dire

$$\begin{aligned} n &= 10^{2p-1}a_1 + 10^{2p-2}a_2 + \cdots + 10^p a_p + 10^{p-1}a_p + 10a_2 + a_1 \\ &= \sum_{k=1}^{p} (10^{k-1} + 10^{2p-k})a_k. \end{aligned}$$

Remarquons ensuite que $10 = -1\ (\text{mod } 11)$, et donc $10^k = (-1)^k\ (\text{mod } 11)$. On obtient donc

$$\begin{aligned} 10^{k-1} + 10^{2p-k} &= (-1)^{k-1} + (-1)^{2p-k}\ (\text{mod } 11) \\ &= (-1)^{k-1} + (-1)^k\ (\text{mod } 11) \\ &= 0\ (\text{mod } 11) \end{aligned}$$

Ainsi, chaque terme $(10^{k-1} + 10^{2p-k})a_k$ est congru à 0 modulo 11. Il en est de même pour $n$.

**Correction de l'exercice 47 ▲**

1. On remarque que $3^2 = 9 \equiv 1\ [8]$. En utilisant les propriétés sur les congruences, on trouve que, si $n = 2k$ est pair,

$$3^{2k} = (3^2)^k \equiv 1^k\ [8] \equiv 1\ [8]$$

et si $n = 2k+1$ est impair,

$$3^{2k+1} = 3^{2k}3 \equiv 1 \times 3\ [8] \equiv 3\ [8].$$

Le reste de la division euclidienne de $3^n$ par 8 est donc égal à 1 si $n$ est pair et à 3 si $n$ est impair.

2. Supposons qu'il existe une solution avec $m \geq 3$. Alors $2^m = 2^{m-3}2^3 = 82^{m-3} \equiv 0\ [8]$. On en déduit que

$$2^m - 3^n \equiv 1\ [8] \implies -3^n \equiv 1\ [8].$$

Mais ceci est impossible, puisque si $n$ est pair, $-3^n \equiv -1\ [8]$ et $-1$ n'est pas congru à 1 modulo 8, et si $n$ est impair, $-3^n \equiv -3\ [8] \equiv 5\ [8]$ et 5 n'est pas congru à 1 modulo 8.

3. Pour $m = 0$, on a $2^m - 3^n = 1 \iff -3^n = 0$, ce qui n'est jamais le cas. Si $m = 1$, on a $2^m - 3^n = 1 \iff 3^n = 1 \iff n = 0$. Le couple $(1,0)$ est donc solution. Si $m = 2$, alors $2^m - 3^n = 1 \iff 3^n = 3 \iff n = 1$. Le couple $(2,1)$ est solution. Donc les solutions sont les couples $(1,0)$ et $(2,1)$.

---

**Correction de l'exercice 48 ▲**

Commençons par écrire un tableau décrivant les carrés modulo 7.

| $x\ [7]$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $x^2\ [7]$ | 0 | 1 | 4 | 2 | 2 | 4 | 1 |

On distingue alors 4 cas :

Si $a^2 = 0$ modulo 7, alors $a^2 + b^2 = 0$ modulo 7 si et seulement si $b = 0$ modulo 7 : c'est le cas où $a$ et $b$ sont tous les deux divisibles par 7. Si $a^2 = 1$ modulo 7, pour que $7|a^2 + b^2$, il faudrait que $b^2 = 6$ modulo 7, ce qui est impossible. Si $a^2 = 2$ modulo 7, pour que $7|a^2 + b^2$, il faudrait que $b^2 = 5$ modulo 7, ce qui est impossible. Si $a^2 = 4$ modulo 7, pour que $7|a^2 + b^2$, il faudrait que $b^2 = 3$ modulo 7, ce qui est impossible.

Ainsi la seule possibilité est bien que $a$ et $b$ soient divisibles par 7.

---

**Correction de l'exercice 49 ▲**

1. Il est clair que $(n+1)\binom{2n}{n+1} = n\binom{2n}{n}$. Maintenant, comme $(n+1) \wedge n = 1$, on en déduit que $(n+1)|\binom{2n}{n}$.

2. Puisque $\binom{p}{k}$ est entier, on sait que $k!(p-k)!|p! = p \times (p-1)!$. Maintenant, puisque $p$ est premier, on sait aussi que $k! \wedge p = 1$ et $(p-k)! \wedge p = 1$. Par le théorème de Gauss, $k!(p-k)!|(p-1)!$ et donc $\frac{(p-1)!}{k!(p-k)!}$ est un entier. Autrement dit, $p|\binom{p}{k}$.

3. Si $n = 1$, le résultat est trivial. Supposons le résultat établi au rang $n$ et prouvons le au rang $n+1$. On a

$$(n+1)^p = n^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} n^k \equiv n^p + 1\ [p]$$

d'après la question précédente. Par hypothèse de récurrence,

$$(n+1)^p \equiv n+1\ [p].$$

---