15. Arithmétique, méthodologie

I. Divisibilité dans $\mathbb{Z}$

I.1. Premières propriétés

Définition. Soient $a, b \in \mathbb{Z}$. On dit que a divise b et on note $a|b$ si il existe $n \in \mathbb{Z}$ tel que $b = an$.

Proposition. Soient $a, b, c \in \mathbb{Z}$. Alors :
- $(a|b \text{ et } b|c) \Rightarrow a|c$.
- $(a|b \text{ et } a|c) \Rightarrow \forall p, q \in \mathbb{Z},\ a|(pb + qc)$.

I.2. Division euclidienne

Théorème. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $r \in [\![0, b-1]\!]$. On dit que q est le quotient de la division euclidienne de a par b et r le reste.

Exercice d'application 1.

1) Effectuer la division euclidienne de 71 par 22 et de -71 par 22. Comparer les quotients/restes de ces deux divisions euclidiennes.

2) Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Déterminer le quotient et le reste de la division euclidienne de $-a$ par b en fonction de q et de r, le quotient et le reste de la division euclidienne de a par b. *On séparera les cas $r = 0$ et $r \neq 0$.*

I.3. Congruences

Définition. Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que a est congru à b modulo n et on note $a \equiv b\ [n]$ si $n|(a - b)$.

Proposition. « $.\ \equiv .\ [n]$ » est une relation d'équivalence sur $\mathbb{Z}$.

Proposition. « $.\ \equiv .\ [n]$ » est compatible avec l'addition et la multiplication, c'est à dire que si $a_1 \equiv b_1\ [n]$ et $a_2 \equiv b_2\ [n]$, alors $a_1 + a_2 \equiv b_1 + b_2\ [n]$ et $a_1 a_2 \equiv b_1 b_2\ [n]$.

(m) Utiliser des congruences permet de trouver très rapidement les restes des divisions euclidiennes puisque si on note r le reste de la division euclidienne de a par n, on a $a \equiv r\ [n]$ (et le reste est l'unique entier de $[\![0, n-1]\!]$ vérifiant ceci). Si on ne cherche pas le quotient, il est donc préférable de passer par les congruences.

(m) Utiliser des congruences permet de tester rapidement la divisibilité puisque $a \equiv 0\ [n] \Leftrightarrow n|a$. Pour le calcul de $a\ [n]$, si a est défini avec des sommes/produits/puissances, on travaille sur les modulos

qui sont compris entre 0 et $n-1$ et on utilise les tables de puissances modulo n, ce qui rend le calcul plus simple.

Exercice d'application 2. Déterminer le reste de la division euclidienne de 852×493 par 7. 852×493 est-il divisible par 7 ?

Exercice d'application 3. Soit $n \geq 3$ un entier. Déterminer le reste de la division euclidienne de $u_n = (n+3)^2 - (n^2 - 3n + 2)^3 + (n-1)^n$ par n. Pour quelles valeurs de n l'entier u_n est-il divisible par n ?

Exercice d'application 4. Montrer par récurrence et en utilisant les congruences que pour tout $n \in \mathbb{N}$, 9 divise $4^n - 1 - 3n$.

Exercice d'application 5. Déterminer toutes les possibilités pour a^4 [5] en fonction de $a \in \mathbb{Z}$. En déduire que $\forall a, b, c \in \mathbb{Z}$, $a^4 + b^4 + c^4 + 1$ n'est jamais divisible par 5.

II. Plus Grand Diviseur Commun

II.1. Définition

Définition. Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$ ou $b \neq 0$. Alors, l'ensemble $\{k \in \mathbb{Z} \ / \ k|a \text{ et } k|b\}$ admet un maximum, que l'on note $a \wedge b$. C'est le **plus grand diviseur commun** (abrégé en PGCD) à a et b et on a $a \wedge b \in \mathbb{N}^*$. On pose $0 \wedge 0 = 0$ pour étendre la propriété à tous les entiers relatifs.

II.2. Algorithme d'Euclide

Proposition. Lemme d'Euclide. $\forall a, b, q \in \mathbb{Z}$, $a \wedge b = (a + bq) \wedge b$.

(m) Pour calculer $a \wedge b$ où $a, b \in \mathbb{N}^*$, on effectue donc des divisions euclidiennes successives en utilisant le lemme d'Euclide précédent :

1. On calcule la division euclidienne de a par b ce qui donne $a = q_1 b + r_1$ avec $r_1 \in [\![0, b-1]\!]$. Si $r_1 = 0$, alors $a \wedge b = b$.
2. Si $r_1 \neq 0$, alors on a $a \wedge b = b \wedge r_1$ d'après le lemme d'Euclide. On effectue donc la division euclidienne de b par r_1 ce qui donne $b = q_2 r_1 + r_2$ avec $r_2 \in [\![0, r_1 - 1]\!]$. Si $r_2 = 0$, alors $a \wedge b = r_1$.
3. Si $r_2 \neq 0$, alors on a $b \wedge r_1 = r_1 \wedge r_2$ d'après le lemme d'Euclide. On effectue donc la division euclidienne de r_1 par r_2 ce qui donne $r_1 = q_3 r_2 + r_3$ avec $r_3 \in [\![0, r_2 - 1]\!]$. Si $r_3 = 0$, alors $a \wedge b = r_2$.
4. etc. On continue l'algorithme jusqu'à obtenir un reste nul. Le PGCD de a et b est alors égal au dernier reste non nul obtenu.

Exercice d'application 6. Déterminer le pgcd de 846 et 153.

II.3. Propriétés du PGCD

Proposition. Soient $a, b \in \mathbb{Z}$ et $d \in \mathbb{Z}$. Alors :

$$(d|a \text{ et } d|b) \Leftrightarrow d|(a \wedge b).$$

Exercice d'application 7. Déterminer tous les entiers $n \in \mathbb{N}^*$ tels que $99 \equiv 0\ [n]$ et $23 \equiv 0\ [n]$.

Proposition. Soient $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}$. Alors, $(ka) \wedge (kb) = k(a \wedge b)$.

(m) Ainsi, si deux entiers ont un facteur commun, on peut d'abord le mettre en facteur et ensuite calculer le pgcd, ce qui permettra de le calculer en partant de nombres moins grands.

III. Théorèmes de Bezout et de Gauss

III.1. Identité de Bezout

Proposition. Soient $a, b \in \mathbb{Z}$. Alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$. On dit que (u, v) est un couple de Bezout associé à a et b.

(m) Pour obtenir un tel couple, on utilise l'algorithme d'Euclide pour calculer $a \wedge b$ et on remonte les calculs en exprimant les restes en fonction des restes précédents ce qui permet d'obtenir une expression ne dépendant que de a et b.

Exercice d'application 8. Déterminer un couple de Bezout associé à 846 et 153.

III.2. Entiers premiers entre eux

Définition. Soient $a, b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Théorème. De Bezout. Soient $a, b \in \mathbb{Z}$. Alors, $a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2 \ / \ au + bv = 1$.

Exercice d'application 9.

1) Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Montrer qu'il existe $c \in \mathbb{Z}$ tel que $ac \equiv 1\ [n]$ si et seulement si $a \wedge n = 1$. *On dit que c est un inverse modulo n de a.*

2) En appliquant l'algorithme d'Euclide à 99 et 23, déterminer $c \in [\![0, 98]\!]$ tel que $23 \times c \equiv 1\ [99]$

3) En déduire l'ensemble des entiers $k \in \mathbb{Z}$ tels que $23k \equiv 3\ [99]$.

III.3. Théorème de Gauss

Théorème. De Gauss. Soient $a, b, c \in \mathbb{Z}$ tels que $a|bc$ et $a \wedge b = 1$. Alors, $a|c$.

Proposition. Corollaires du théorème de Gauss. Soient $a, b, c \in \mathbb{Z}$. Alors :

- Si $a|c$, $b|c$ et $a \wedge b = 1$, alors $ab|c$.
- Si $a \wedge c = 1$ et $b \wedge c = 1$, alors $(ab) \wedge c = 1$.

Proposition. Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge b = 1$. Alors, $a \wedge (bc) = a \wedge c$.

IV. Applications et généralisations du PGCD

IV.1. Résolution d'équations du type $ax + by = c$

(m) Soient $a, b \in \mathbb{Z}$ non nuls et $c \in \mathbb{Z}$. On cherche tous les couples $(x, y) \in \mathbb{Z}^2$ tels que $ax + by = c$. On procède toujours de la même façon pour résoudre ce type d'équations :

1. On commence par calculer $a \wedge b$ en utilisant l'algorithme d'Euclide.
2. Si $a \wedge b \not| c$, alors il n'y a pas de solutions. Sinon, on divise l'équation de départ par $a \wedge b$ ce qui donne une équation du type $a'x + b'y = c'$ avec $a' \wedge b' = 1$.
3. On utilise les calculs réalisés à l'étape 1 pour trouver $(u_0, v_0) \in \mathbb{Z}^2$ tels que $a'u_0 + b'v_0 = 1$ (il suffit de tout diviser par $a \wedge b$ et de remonter l'algorithme d'Euclide). On multiplie alors par c' pour obtenir $(x_0, y_0) = (c'u_0, c'v_0)$ comme solution particulière de l'équation.
4. On raisonne ensuite par analyse/synthèse pour démontrer que les solutions sont de la forme $(x, y) = (x_0 + kb', y_0 - ka')$ avec $k \in \mathbb{Z}$. Pour la partie analyse, on suppose (x, y) solution, on écrit $a'x + b'y = a'x_0 + b'y_0$, on rassemble les termes en a' et les termes en b' ensemble et on utilise le théorème de Gauss. Une fois x obtenu, on obtient y et on passe à la synthèse.

Exercice d'application 10. Déterminer tous les couples $(x, y) \in \mathbb{Z}^2$ tels que $26x - 16y = 4$.

IV.2. Calcul du PGCD

(m) Quand on ne peut pas appliquer l'algorithme d'Euclide explicitement pour calculer un PGCD, on utilise le lemme d'Euclide qui permet, lorsque que l'on calcule $a \wedge b$ d'ajouter à a n'importe quel multiple de b et à b n'importe quel multiple de a en conservant le PGCD. On essaye alors d'utiliser plusieurs fois ce lemme jusqu'à avoir une expression simple sur laquelle on peut conclure.

Exercice d'application 11. Soit $k \in \mathbb{N}$.

1) Montrer que $2k + 1$ et $9k + 4$ sont premiers entre eux.

2) En vous inspirant de la méthode de l'algorithme d'Euclide, déterminer une relation de Bezout associée à ces deux entiers.

3) Calculer le pgcd de $2k - 1$ et $9k + 4$.

IV.3. PGCD de plusieurs entiers

Proposition. Le PGCD est associatif, autrement dit $\forall a, b, c \in \mathbb{Z},\ a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Définition. Soient $a_1, \ldots, a_n \in \mathbb{Z}$ non tous nuls. Alors, l'ensemble $\{k \in \mathbb{Z} \,/\, k|a_1 \text{ et } k|a_2 \text{ et } \ldots \text{ et } k|a_n\}$ admet un maximum, que l'on note $a_1 \wedge a_2 \wedge \ldots \wedge a_n$. C'est le **plus grand diviseur commun** (abrégé en PGCD) à $a_1, a_2, \ldots, a_n$ et on a $a_1 \wedge a_2 \wedge \ldots \wedge a_n \in \mathbb{N}^*$. On pose $0 \wedge 0 \wedge \ldots \wedge 0 = 0$ pour étendre la propriété à tous les entiers relatifs.

Proposition. Soient $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ et $k \in \mathbb{N}$. Alors $(ka_1) \wedge (ka_2) \wedge \ldots \wedge (ka_n) = k(a_1 \wedge a_2 \wedge \ldots \wedge a_n)$.

Définition. Soient $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. On dit que :

- $a_1, a_2, \ldots, a_n$ sont premiers entre eux deux à deux si $\forall i, j \in [\![1, n]\!]$, $(i \neq j \Rightarrow a_i \wedge a_j = 1)$.
- $a_1, a_2, \ldots, a_n$ sont premiers entre eux dans leur ensemble si $a_1 \wedge a_2 \wedge \ldots \wedge a_n = 1$.

Exercice d'application 12.

1) Donner un exemple de trois entiers premiers entre eux dans leur ensemble mais non premier entre eux deux à deux.

2) Montrer que si $a_1, a_2, \ldots, a_n$ sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble.

Théorème. De Bezout généralisé. Soient $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Alors, $a_1 \wedge a_2 \wedge \ldots \wedge a_n = 1 \Leftrightarrow \exists (u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n \ / \ a_1u_1 + a_2u_2 + \ldots + a_nu_n = 1$.

V. Plus Petit Multiple Commun

Définition. Soient $a, b \in \mathbb{Z}$. Alors, l'ensemble des entiers naturels multiples de a et b ($\{k \in \mathbb{N} \ / \ a|k \text{ et } b|k\}$) admet un minimum, noté $a \vee b$. C'est le plus petit multiple commun à a et b (abrégé en PPCM).

Proposition. Soient $a, b \in \mathbb{Z}$. Alors :
- $a \vee b = b \vee a$.
- $a \vee b = (-a) \vee b = a \vee (-b) = (-a) \vee (-b)$.
- $a \vee 1 = |a|$.
- $a \vee a = |a|$.
- $a|a \vee b$ et $b|a \vee b$.

Proposition. Soient $a, b \in \mathbb{Z}$ et $m \in \mathbb{Z}$. Alors :

$$a|m \text{ et } b|m \Leftrightarrow (a \vee b)|m.$$

Proposition. Soient $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}$. Alors, $(ka) \vee (kb) = k(a \vee b)$.

Proposition. Soient $a, b \in \mathbb{Z}$. Alors, $(a \wedge b) \times (a \vee b) = |ab|$.

(m) En général, on utilise la relation précédente pour traduire toute information sur le ppcm en information sur le PGCD. En effet, connaitre les diviseurs communs à des entiers donne souvent plus d'informations car on peut alors les factoriser par leur PGCD et manipuler ensuite des entiers premiers entre eux.

Exercice d'application 13. Résoudre dans $\mathbb{N}^2$ le système $\begin{cases} x \wedge y = 5 \\ x \vee y = 60 \end{cases}$.

VI. Nombres premiers

VI.1. Définition

Définition. Soit $p \geq 2$. On dit que p est un **nombre premier** si ses seuls diviseurs positifs sont 1 et lui-même. On note $\mathbb{P}$ l'ensemble des nombres premiers.

(m) Ainsi, pour montrer qu'un entier $n \geq 2$ n'est pas premier, il suffit de réussir à l'écrire comme $n = ab$ avec $a >$ 1 et $b >$ des entiers .

Exercice d'application 14.

1) On pose pour $n \in \mathbb{N}^*$, $u_n = \sum_{k=0}^{n-1}(2k+1)$ la somme des n premiers nombres impairs. Montrer que u_n n'est jamais premier.

2) Montrer qu'une somme de nombres impairs consécutifs d'au moins deux termes n'est jamais un nombre premier.

VI.2. Recherche de nombres premiers

VI.3. Propriétés

Proposition. Soit $p \in \mathbb{P}$ un nombre premier et $a \in \mathbb{Z}$. Alors $p|a$ ou $a \wedge p = 1$.

Proposition. Soit $p \in \mathbb{P}$ un nombre premier et $a, b \in \mathbb{Z}$. Alors $p|(ab) \Rightarrow (p|a$ ou $p|b)$.

VI.4. Infinité des nombres premiers

Théorème. L'ensemble des nombres premiers $\mathbb{P}$ est infini.

VI.5. Petit théorème de Fermat

Théorème. Soit $p \in \mathbb{P}$ un nombre premier et $a \in \mathbb{Z}$. Alors :
- $a^p \equiv a\ [p]$.
- Si de plus $p \not| a$, $a^{p-1} \equiv 1\ [p]$.

(m) Ceci peut nous permettre de trouver rapidement des périodes dans les tables de congruence. Par exemple, si on étudie les puissances de 3 modulo 11, alors puisque 11 est premier et qu'il ne divise pas 2, on a $3^{10} \equiv 1\ [11]$ d'après le petit théorème de Fermat donc la table des puissances de 3 modulo 11 est automatiquement 10 périodique ! Attention, cela ne garantit pas de trouver la plus petite période ! En effet, on a $3^5 \equiv 1\ [11]$, et on peut vérifier que la plus petite période des puissances de 3 modulo 11 est 5.

VI.6. Valuation

Définition. Soit $p \in \mathbb{P}$ un nombre premier et $a \in \mathbb{N}^*$. Alors l'ensemble $\{k \in \mathbb{N}\ /\ p^k|a\}$ admet un maximum que l'on note $v_p(a)$. $v_p(a)$ est la valuation p-adique de a et c'est le plus grand entier k tel que p^k divise a.

Proposition. Soient $a, b \in \mathbb{N}^*$ et $p \in \mathbb{P}$. Alors $v_p(ab) = v_p(a) + v_p(b)$.

Proposition. Soient $a, b \in \mathbb{N}^*$. Alors $a|b$ si et seulement si $\forall p \in \mathbb{P},\ v_p(a) \leq v_p(b)$.

VI.7. Théorème de factorisation

Théorème. Décomposition en produits de facteurs premiers. Soit $a \in \mathbb{N}^*$. Alors :

$$a = \prod_{p \in \mathbb{P}} p^{v_p(a)}.$$

Cette écriture est de plus unique à l'ordre des facteurs près.

(m) Cette décomposition est très utile car elle permet de visualiser très rapidement les diviseurs d'un entier et de calculer des PGCDs/PPCMs. Ainsi par exemple, si $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$ et $b = \prod_{p \in \mathbb{P}} p^{v_p(b)}$, alors :

$$a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))} \text{ et } a \vee b = \prod_{p \in \mathbb{P}} p^{\max(v_p(a), v_p(b))}.$$

Le défaut de cette décomposition est qu'elle est en général difficile à trouver dans des exemples concrets ce qui rend l'utilisation de la formule précédente beaucoup moins efficace que l'algorithme d'Euclide pour un calcul concret de PGCD. Elle permet cependant dans des exercices plus théoriques d'avoir une factorisation simple de n'importe quel entier (la décomposition existe toujours et est unique) ce qui permet d'avoir très rapidement des propriétés sur les diviseurs d'un entier.

Exercice d'application 15.

1) Factoriser 10! en produit de nombres premiers.
2) En déduire le nombre de diviseurs de 10! dans $\mathbb{N}^*$.

Exercice d'application 16. Soit $n \in \mathbb{N}^*$ tel que n soit un carré et un cube d'entiers (autrement dit, il existe $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ tels que $n = a^2$ et $n = b^3$). Montrer qu'il existe $c \in \mathbb{N}^*$ tel que $n = c^6$.

VII. Correction des exercices

Exercice d'application 1.

1) On a $71 = 3 \times 22 + 5$ donc le quotient vaut 3 et le reste vaut 5. On a $-71 = -4 \times 22 + 17$ donc le quotient vaut -4 et le reste 17. *Attention à bien avoir un reste compris entre 0 et 21 ici !*

On remarque ici que les quotients sont presque opposés (il y a « 1 » d'écart) et que si on additionne les restes, on obtient 22 (donc le nombre par lequel on fait la division euclidienne).

2) On a $a = bq + r$ avec $r \in [\![0, b-1]\!]$ et $q \in \mathbb{Z}$. En multipliant par -1, on obtient $-a = (-q)b - r$. On a alors deux cas :

- Si $r = 0$, alors on a $-a = (-q)b + 0$ et par **unicité du quotient et du reste dans la division euclidienne**, on a que le quotient de la division euclidienne de $-a$ par b vaut $-q$ et le reste vaut 0.
- Si $r \neq 0$, alors, on a $-a = (-q)b - r = (-q-1)b + b - r$. On a alors $b - r \in [\![1, b-1]\!]$ (puisque $0 < r < b$). On peut donc à nouveau utiliser l'unicité du quotient et du reste dans la division euclidienne pour affirmer que le quotient de la division euclidienne de $-a$ par b vaut $-q-1$ et le reste vaut $b - r$.

Exercice d'application 2. On a 852=700+140+7+5. On a donc $852 \equiv 5\ [7]$. On a $493 = 490 + 3$ donc $493 \equiv 3\ [7]$. Par produit, on en déduit que $852 \times 493 \equiv 5 \times 3\ [7] \equiv 1\ [7]$. Le reste de la division euclidienne de 852×493 par 7 est donc 1. Puisque ce reste est non nul, 852×493 n'est pas divisible par 7.

Exercice d'application 3. Soit $n \geq 3$ un entier. On a $n+3 \equiv 3\ [n]$ donc $(n+3)^2 \equiv 9\ [n]$. De même, on a $n^2 - 3n + 2 \equiv 2\ [n]$ donc $(n^2 - 3n + 2)^3 \equiv 8\ [n]$. Enfin, $n - 1 \equiv -1\ [n]$ donc $(n-1)^n \equiv (-1)^n\ [n]$. On a donc finalement :

$$u_n \equiv 9 - 8 + (-1)^n\ [n] \equiv 1 + (-1)^n\ [n].$$

Puisque $1 + (-1)^n$ vaut soit 0, soit 2 et que $n \geq 3$, on a bien un reste compris entre 0 et $n-1$. C'est donc le reste de la division euclidienne de u_n par n. u_n est divisible par n si et seulement si le reste trouvé avant est nul, autrement dit si et seulement si n est impair.

Exercice d'application 4. Pour $n \in \mathbb{N}$, on pose $\mathcal{P}(n)$: « $4^n - 1 - 3n \equiv 0\ [9]$ ».

- La propriété est vraie au rang 0 (on a $1 - 1 - 0 = 0 \equiv 0\ [9]$).
- Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$. On a alors :

$$\begin{aligned} 4^{n+1} - 1 - 3(n+1) &= 4 \times 4^n - 4 - 3n \\ &= 4 \times (4^n - 1 - 3n) + 9n. \end{aligned}$$

  On a $9n \equiv 0\ [9]$ et $4^n - 1 - 3n \equiv 0\ [9]$ par hypothèse de récurrence. Par produit et somme dans les modulos, on a donc notre hypothèse vraie au rang $n+1$.
- L'hypothèse étant initialisée et héréditaire, elle est vraie à tout rang.

Exercice d'application 5. Toutes les possibilités pour a modulo 5 sont $0, 1, 2, 3, 4$. En élevant à la puissance quatrième chacun de ces nombres, on trouve que les possibilités pour a^4 modulo 5 sont 0 (si $a \equiv 0\ [5]$) et 1 dans tous les autres cas. *On aurait pu retrouver ce résultat directement avec le petit théorème de Fermat. En effet, si $a \not\equiv 0\ [5]$, alors a n'est pas divisible par 5, ce qui implique d'après le petit théorème de Fermat (puisque 5 est premier) que $a^{5-1} \equiv 1\ [5]$.*

Si $a, b, c \in \mathbb{Z}$, on en déduit que $a^4 + b^4 + c^4 + 1\ [5]$ appartient à $[\![1, 4]\!]$ (on a toutes les combinaisons possibles avec $a^4\ [5]$ pouvant valoir 0 ou 1, idem pour $b^4\ [5]$ et $c^4\ [5]$. Ceci entraine, le reste n'étant jamais nul, que $a^4 + b^4 + c^4 + 1$ n'est jamais divisible par 5.

Exercice d'application 6. On réalise l'algorithme d'Euclide. On a :

- $846 = 5 \times 153 + 81$.
- $153 = 1 \times 81 + 72$.
- $81 = 1 \times 72 + 9$.
- $72 = 8 \times 9 + 0$.

On en déduit que $846 \wedge 153 = 9$ (le dernier reste non nul).

Exercice d'application 7. On a $99 \equiv 0\ [n]$ et $23 \equiv 0\ [n]$ si et seulement si $n|99$ et $n|23$, et donc si et seulement si $n|(99 \wedge 23)$. Or, on a $99 \wedge 23 = 1$ (en utilisant l'algorithme d'Euclide : $99 = 4 \times 23 + 7$, $23 = 3 \times 7 + 2$, $7 = 3 \times 2 + 1$ et $2 = 2 \times 1 + 0$ donc le dernier reste non nul est 1). On a donc $99 \equiv 0\ [n]$ et $23 \equiv 0\ [n]$ si et seulement si $n|1$. Puisque $n \in \mathbb{N}^*$, on en déduit que le seul entier vérifiant la propriété est $n = 1$.

Exercice d'application 8. On remonte les calculs de l'exercice 7. On a :

$$\begin{aligned} 9 &= 81 - 72 \\ &= 81 - (153 - 81) \\ &= 2 \times 81 - 153 \\ &= 2 \times (846 - 5 \times 153) - 153 \\ &= 2 \times 846 - 11 \times 153. \end{aligned}$$

Un couple de Bezout associé à 846 et 153 est donc $(2, -11)$.

Exercice d'application 9.

1) Procédons par double implication :
   - ($\Rightarrow$) Si il existe $c \in \mathbb{Z}$ tel que $ac \equiv 1\ [n]$, alors par définition du modulo, il existe $k \in \mathbb{Z}$ tel que $ac = 1 + kn \Leftrightarrow ac - kn = 1$. On a donc d'après le théorème de Bezout que $a \wedge n = 1$.
   - ($\Leftarrow$) Si $a \wedge n = 1$, alors d'après le théorème de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $au + nv = 1$. En considérant cette égalité modulo n, on obtient $au \equiv 1\ [n]$ d'où l'existence du $c = u \in \mathbb{Z}$ demandé.

2) On a $99 \wedge 23 = 1$. On déterminer alors un couple de Bezout associé à 99 et 23 (qui sont premiers entre eux). On a $99 = 4 \times 23 + 7$, $23 = 3 \times 7 + 2$, $7 = 3 \times 2 + 1$ donc en remontant :

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - 3 \times (23 - 3 \times 7) \\ &= 10 \times 7 - 3 \times 23 \\ &= 10 \times (99 - 4 \times 23) - 3 \times 23 \\ &= 10 \times 99 - 43 \times 23. \end{aligned}$$

D'après la question précédente, on a donc $23 \times (-43) \equiv 1\ [99]$. Puisque l'on veut $c \in [\![0, 98]\!]$, il suffit de prendre 56 (car $56 \equiv -43\ [99]$). On a donc $23 \times 56 \equiv 1\ [99]$.

3) On a $23k \equiv 3\ [99] \Leftrightarrow k \equiv 3 \times 56\ [99]$. En effet, l'implication $\Rightarrow$ est vraie en multipliant par 56 l'égalité de gauche et l'implication $\Leftarrow$ est vraie en multipliant par 23 l'égalité de gauche (et dans les deux cas en utilisant le fait que $23 \times 56 \equiv 1\ [99]$). Puisque $3 \times 56 = 168 \equiv 69\ [99]$, on en déduit que l'ensemble des solutions sont les entiers de la forme $69 + 99k$ avec $k \in \mathbb{Z}$. *Il est important ici de justifier l'équivalence entre les deux propriétés sinon l'ensemble des solutions pourrait ne pas être le même...*

Exercice d'application 10. On a :

- $26 = 1 \times 16 + 10$.
- $16 = 1 \times 10 + 6$.
- $10 = 1 \times 6 + 4$.
- $6 = 1 \times 4 + 2$.

- $4 = 2 \times 2 + 0$.

On a donc $26 \wedge 16 = 2$. L'équation étudiée est donc équivalente à $13x - 8y = 2$. En divisant par 2 nos calculs précédents, on obtient :

- $13 = 1 \times 8 + 5$.
- $8 = 1 \times 5 + 3$.
- $5 = 1 \times 3 + 2$.
- $3 = 1 \times 2 + 1$.

On trouve alors un couple de Bezout :

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2 \times 3 - 5 \\ &= 2 \times (8 - 5) - 5 \\ &= 2 \times 8 - 3 \times 5 \\ &= 2 \times 8 - 3 \times (13 - 8) \\ &= 5 \times 8 - 3 \times 13. \end{aligned}$$

Pour obtenir une solution particulière, on multiplie par 2 ce qui donne $x_0 = -6$ et $y_0 = -10$. On montre ensuite par analyse/synthèse que l'ensemble des solutions est de la forme $\{(x_0+8k, y_0+13k),\ k \in \mathbb{Z}\}$.

Analyse : Soit $(x, y) \in \mathbb{Z}^2$ solution. On a alors $13x - 8y = 13x_0 - 8y_0 \Leftrightarrow 13(x - x_0) = 8(y - y_0)$. Puisque $13 \wedge 8 = 1$, on en déduit d'après le théorème de Gauss que $13|(y - y_0)$. Il existe donc $k \in \mathbb{Z}$ tel que $y - y_0 = 13k$. En réinjectant dans l'égalité précédente, on obtient $13(x - x_0) = 8 \times 13k$, soit $x - x_0 = 8k$. On a donc qu'il existe $k \in \mathbb{Z}$ tel que $x = x_0 + 8k$ et $y = y_0 + 13k$.

Synthèse : En réinjectant dans l'équation, on vérifie que tous ces couples sont bien solutions.

Exercice d'application 11. Soit $k \in \mathbb{N}$.

1) On utilise le lemme d'Euclide :

$$\begin{aligned} (9k + 4) \wedge (2k + 1) &= (9k + 4 - 4(2k + 1)) \wedge (2k + 1) \\ &= k \wedge (2k + 1) \\ &= k \wedge (2k + 1 - 2k) \\ &= k \wedge 1 \\ &= 1. \end{aligned}$$

Ceci entraine que $9k + 4$ et $2k + 1$ sont premiers entre eux.

2) En reprenant les calculs ci-dessus, on a $9k + 4 = 4(2k + 1) + k$ puis $2k + 1 = 2k + 1$. On a donc :

$$\begin{aligned} 1 &= (2k + 1) - 2 \times (k) \\ &= (2k + 1) - 2 \times ((9k + 4) - 4(2k + 1)) \\ &= 9 \times (2k + 1) - 2 \times (9k + 4). \end{aligned}$$

On a ainsi obtenu une relation de Bezout associée à $2k + 1$ et $9k + 4$.

3) On utilise le lemme d'Euclide. On a :

$$\begin{aligned} (2k - 1) \wedge (9k + 4) &= (2k - 1) \wedge (9k + 4 - 4(2k - 1)) \\ &= (2k - 1) \wedge (k + 8) \\ &= (2k - 1 - 2(k + 8)) \wedge (k + 8) \\ &= (-17) \wedge (k + 8). \end{aligned}$$

Puisque 17 est premier, on en déduit que le pgcd vaut 17 si $17|(k + 8)$, autrement dit si $(k + 8) \equiv 0\ [17]$, c'est à dire si $k \equiv 9\ [17]$, et que dans tous les autres cas, le pgcd vaut 1.

Exercice d'application 12.

1) Les entiers $6, 10$ et 15 par exemple sont premiers entre eux dans leur ensemble puisque :

$$6 \wedge 10 \wedge 15 = (6 \wedge 10) \wedge 15 = 2 \wedge 15 = 1.$$

Ils ne sont pas premiers entre eux deux à deux (par exemple $6 \wedge 10 = 2 \neq 1$). *Il n'y a même ici aucun des coupls qui sont premiers entre eux.*

2) Soient $a_1, \ldots, a_n$ premiers entre eux deux à deux. On a alors par exemple $a_1 \wedge a_2 = 1$. On a donc :

$$\begin{aligned} a_1 \wedge a_2 \wedge \ldots \wedge a_n &= (a_1 \wedge a_2) \wedge \ldots \wedge a_n \\ &= 1 \wedge \ldots \wedge a_n. \end{aligned}$$

Or, le PGCD de 1 avec n'importe quel entier vaut 1. On a donc bien $a_1, \ldots, a_n$ premiers entre eux dans leur ensemble.

Exercice d'application 13. Analyse : Si $(x, y) \in \mathbb{N}^2$ est un couple solution, on a $x \wedge y = 5$ donc il existe $x', y' \in \mathbb{N}$ tels que $x = 5x'$ et $y = 5y'$ avec $x' \wedge y' = 1$. On a alors $x \vee y = 5x' \vee y' = 5x'y'$ car x' et y' sont premiers entre eux. On a donc finalement le système :

$$\begin{cases} x' \wedge y' = 1 \\ x'y' = 12 \end{cases}$$

Puisque $12 = 2^2 \times 3$ et que l'on veut x' et y' premiers entre eux, on en déduit que les solutions sont les couples (x', y') égaux à $(1, 12)$, $(3, 4)$, $(4, 3)$ et $(12, 1)$ (les couples $(6, 2)$ et $(2, 6)$ sont à exclure car 2 et 6 ne sont pas premiers entre eux).

Synthèse : Les couples solutions sont donc $(5, 60)$, $(15, 20)$, $(20, 15)$ et $(60, 5)$.

Exercice d'application 14.

1) Pour $n \in \mathbb{N}$, on a $u_n = 2\sum_{k=0}^{n} k + \sum_{k=0}^{n} 1 = 2\dfrac{n(n+1)}{2} + n + 1 = (n+1)^2$. Si $n = 0$, ce nombre vaut 1 qui n'est pas premier. Si $n \geq 1$, alors $n + 1 \geq 2$ et on a bien u_n non premier.

2) On considère ici le nombre $\sum_{k=n_1}^{n_2} (2k+1)$ avec $n_1, n_2 \in \mathbb{N}$ et $n_2 > n_1$. On a alors :

$$\sum_{k=n_1}^{n_2} (2k+1) = u_{n_2} - u_{n_1-1} = (n_2+1)^2 - n_1^2 = (n_2 + 1 - n_1)(n_2 + 1 + n_1).$$

On a alors $n_2 + 1 + n_1 > 0$ (puisque $n_2 > n_1 \geq 0$) et $n_2 - n_1 > 0$ donc $n_2 - n_1 + 1 > 1$. Cet entier n'est donc pas premier puisqu'il se factorise comme produit d'entiers strictement plus grands que 1.

Exercice d'application 15.

1) On a :

$$\begin{aligned} 10! &= 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \\ &= 2 \times 3 \times 2^2 \times 5 \times 2 \times 3 \times 7 \times 2^3 \times 3^2 \times 2 \times 5 \\ &= 2^8 \times 3^4 \times 5^2 \times 7. \end{aligned}$$

2) Les diviseurs de 10! sont de la forme $2^x \times 3^y \times 5^z \times 7^t$ avec $x, y, z, t \in \mathbb{N}$ tels que $0 \leq x \leq 8$, $0 \leq y \leq 4$, $0 \leq z \leq 2$ et $0 \leq t \leq 1$. On a donc exactement $9 \times 5 \times 3 \times 2 = 270$ diviseurs de 10! dans $\mathbb{N}^*$ (9 possibilités pour la valeur de x, 5 pour y de manière indépendante, 3 pour z de manière indépendante et 2 pour t de manière indépendante).

Exercice d'application 16. On utilise la décomposition en produits de facteurs premiers de a et b. On écrit $a = \prod_{p\in\mathbb{P}} p^{v_p(a)}$ et $b = \prod_{p\in\mathbb{P}} p^{v_p(b)}$. Alors, puisque $a^2 = b^3$, on a :

$$\left(\prod_{p\in\mathbb{P}} p^{v_p(a)}\right)^2 = \left(\prod_{p\in\mathbb{P}} p^{v_p(b)}\right)^3$$

$$\Leftrightarrow \prod_{p\in\mathbb{P}} p^{2v_p(a)} = \prod_{p\in\mathbb{P}} p^{3v_p(b)}$$

Par unicité de la décomposition en produits de facteurs premiers, on a pour tout $p \in \mathbb{P}$, $2v_p(a) = 3v_p(b)$. Utilisons alors le théorème de Gauss. Puisque $2 \wedge 3 = 1$, on a $2|v_p(b)$. Il existe donc $\alpha_p \in \mathbb{N}$ tel que $v_p(b) = 2\alpha_p$. En reprenant alors l'écriture $n = b^3$, on a que :

$$n = \left(\prod_{p\in\mathbb{P}} p^{2\alpha_p}\right)^3 = \left(\left(\prod_{p\in\mathbb{P}} p^{\alpha_p}\right)^2\right)^3 = \left(\prod_{p\in\mathbb{P}} p^{\alpha_p}\right)^6.$$

En posant $c = \prod_{p\in\mathbb{P}} p^{\alpha_p} \in \mathbb{N}^*$, on a bien montré que n s'écrit comme une puissance 6-ième d'entier.