EXERCICES – CHAPITRE 7

PGCD

PGCD et algorithme d'Euclide

EXERCICE 1 ⋆

1. Déterminer à l'aide des règles de divisibilité :
   a) PGCD$(12, 42)$
   b) PGCD$(45, 105)$
   c) PGCD$(92, 69)$
   d) PGCD$(72, 108)$
2. Déterminer les entiers naturels n tels que :
   a) $n \leqslant 200$ et PGCD$(n, 324) = 12$
   b) $n \leqslant 500$ et PGCD$(n, 378) = 54$
   c) $n \leqslant 400$ et PGCD$(n, 150) = 6$

EXERCICE 2 ⋆

Trouver tous les couples d'entiers naturels (a, b) avec $a < b$ tels que :

1. $\begin{cases} ab = 432 \\ \text{PGCD}(a, b) = 6 \end{cases}$
2. $\begin{cases} ab = 7776 \\ \text{PGCD}(a, b) = 18 \end{cases}$
3. $\begin{cases} a + b = 24 \\ \text{PGCD}(a, b) = 4 \end{cases}$

EXERCICE 3 ⋆

1. Utiliser l'algorithme d'Euclide pour déterminer les PGCD suivants :
   a) PGCD$(144, 840)$
   b) PGCD$(202, 138)$
   c) PGCD$(441, 777)$
   d) PGCD$(2004, 9185)$
2. À l'aide de l'algorithme d'Euclide, dire si les couples d'entiers suivants sont premiers entre eux :
   a) $(4\,847\,;5\,633)$
   b) $(5\,617\,;813)$

EXERCICE 4 ⋆

1. À l'aide de l'algorithme d'Euclide, rendre irréductibles les fractions $\dfrac{3528}{3780}$ et $\dfrac{1071}{462}$.
2. Un carreleur doit recouvrir le sol d'une pièce rectangulaire de 3,36 m sur 2,40 m avec des dalles carrées identiques, sans découpe. Il souhaite utiliser les dalles les plus grandes possibles, dont le côté est un nombre entier de centimètres. Quel est le côté des dalles, et combien en faut-il ?

EXERCICE 5 ⋆⋆

Si on divise 4294 et 3521 par un même entier positif, on obtient respectivement 10 et 11 comme reste. Quel est cet entier ?

EXERCICE 6 ⋆⋆

Soit $n \in \mathbb{N}^*$. On note $d = \text{PGCD}(n, n + 6)$.

1. Montrer que d divise 6. Quelles sont les valeurs possibles de d ?
2. Déterminer d selon le reste de la division euclidienne de n par 6.
3. Vérifier le résultat avec $n = 9$, $n = 10$, $n = 11$ et $n = 12$.

EXERCICE 7 ⋆⋆

1. Soient a et b deux entiers naturels non nuls et k un entier relatif tel que $b - ka$ soit non nul. Montrer que a et b ont les mêmes diviseurs communs que a et $b - ka$, puis que $\text{PGCD}(a, b) = \text{PGCD}(a, b - ka)$.
2. En déduire, pour tout $n \in \mathbb{N}$, la valeur de $\text{PGCD}(3n + 5, n + 2)$.
3. Soit $n \in \mathbb{N}$. Vérifier que $n^2 + 3 = (n-1)(n+1) + 4$. En déduire que $\text{PGCD}(n^2 + 3, n + 1)$ divise 4, puis déterminer sa valeur selon le reste de la division euclidienne de n par 4.

EXERCICE 8 ⋆⋆

Soit $n \in \mathbb{N}^*$, on pose $a = 5n + 1$ et $b = 2n - 1$. On note $D = \text{PGCD}(a, b)$.

1. Démontrer que les valeurs possibles de D sont 1 ou 7.
2. Déterminer les valeurs de n pour lesquelles :
$$a \equiv 0\ [7] \text{ et } b \equiv 0\ [7]$$
3. En déduire, suivant les valeurs de n, la valeur de D.

EXERCICE 9 ⋆

1. Soit n un entier naturel, on pose $a = 7n + 4$ et $b = 5n + 3$. Montrer, pour tout n, que a et b sont premiers entre eux.
2. Montrer que deux entiers consécutifs non nuls sont premiers entre eux.
3. Montrer que deux entiers impairs consécutifs sont premiers entre eux.

EXERCICE 10 ⋆

Montrer que les fractions suivantes sont irréductibles pour tout entier naturel n :

a) $\dfrac{n}{2n+1}$ b) $\dfrac{9n+1}{6n+1}$ c) $\dfrac{14n+3}{5n+1}$

EXERCICE 11 ⋆⋆

Soit $n > 5$, on pose : $a = n^3 - n^2 - 12n$ et $b = 2n^2 - 7n - 4$.

1. Démontrer que a et b sont des entiers naturels divisibles par $n - 4$.
2. On pose $\alpha = 2n + 1$ et $\beta = n + 3$. On note $d = \text{PGCD}(\alpha, \beta)$.
   (a) Démontrer que d est un diviseur de 5.
   (b) Démontrer que α et β sont multiples de 5 si et seulement si $n - 2 \equiv 0\ [5]$.
3. Démontrer que $2n + 1$ et n sont premiers entre eux.
4. (a) Déterminer $\text{PGCD}(a, b)$ en fonction de n.
   (b) Vérifier les résultats obtenus dans les cas particuliers $n = 11$ et $n = 12$.

Théorème de Bézout et algorithme d'Euclide étendu

EXERCICE 12 ⋆

1. Montrer que 87 et 31 sont premiers entre eux à l'aide de l'algorithme d'Euclide, puis, en remontant cet algorithme, déterminer un couple d'entiers relatifs (x, y) tel que :

$$87x + 31y = 1$$

2. Montrer que 38 et 45 sont premiers entre eux à l'aide de l'algorithme d'Euclide, puis, en remontant cet algorithme, déterminer un couple d'entiers relatifs (x, y) tel que :

$$38x + 45y = 1$$

3. Montrer que 41 et 25 sont premiers entre eux à l'aide de l'algorithme d'Euclide, puis, en remontant cet algorithme, déterminer un couple d'entiers relatifs (x, y) tel que :

$$41x - 25y = 1$$

4. Montrer que 221 et 331 sont premiers entre eux à l'aide de l'algorithme d'Euclide, puis, en remontant cet algorithme, déterminer un couple d'entiers relatifs (x, y) tel que :

$$221x - 331y = 1$$

EXERCICE 13 : INVERSE MODULAIRE ET CHIFFREMENT AFFINE ⋆⋆

1. À l'aide de l'algorithme d'Euclide étendu, déterminer un couple d'entiers (u, v) tel que $11u + 26v = 1$. En déduire un entier $x_0 \in \{0, \dots, 25\}$ tel que $11x_0 \equiv 1\ [26]$. On dit que x_0 est un *inverse de* 11 *modulo* 26.
2. Résoudre dans $\mathbb{Z}$ la congruence $11x \equiv 5\ [26]$.
3. On numérote les lettres de l'alphabet de $A = 0$ à $Z = 25$. Pour coder une lettre de rang x, on calcule le reste y de la division euclidienne de $11x + 3$ par 26, et l'on remplace la lettre par celle de rang y.
   (a) Coder la lettre E.
   (b) Montrer que $y \equiv 11x + 3\ [26]$ équivaut à $x \equiv 19(y - 3)\ [26]$, puis décoder la lettre H.
   (c) Pourquoi ce procédé ne fonctionnerait-il pas avec la clé $y \equiv 13x + 3\ [26]$?

EXERCICE 14 ⋆

1. Déterminer les couples d'entiers relatifs (x, y) tels que : $33x - 45y = 0$.
2. En déduire les couples d'entiers relatifs (x, y) tels que : $33x + 45y = 12$.

EXERCICE 15 ⋆

1. Déterminer les couples d'entiers relatifs (x, y) tels que : $7(x - 3) = 5(y - 2)$.
2. En déduire les couples d'entiers relatifs (x, y) tels que : $7x \equiv 1\ [5]$.

Équations diophantiennes

EXERCICE 16 ⋆

Soit l'équation $4x - 3y = 2$.

1. Sans calcul, dire pourquoi cette équation admet des solutions entières.
2. Déterminer un couple d'entiers solution de cette équation.
3. Déterminer l'ensemble des couples d'entiers solutions de cette équation.

EXERCICE 17 ⋆

Soit l'équation $3x - 4y = 6$.

1. Déterminer un couple d'entiers solution de cette équation.
2. Déterminer l'ensemble des couples d'entiers solutions de cette équation.

EXERCICE 18 ⋆

Soit l'équation $5x + 8y = 2$.

1. Déterminer un couple d'entiers solution de cette équation.
2. Déterminer l'ensemble des couples d'entiers solutions de cette équation.

EXERCICE 19 ⋆

1. L'équation $6x + 9y = 20$ admet-elle des solutions entières ? Et l'équation $6x + 9y = 21$?
2. Résoudre dans $\mathbb{Z}^2$ l'équation $6x + 9y = 21$. On commencera par simplifier l'équation.

EXERCICE 20 ⋆

Soit l'équation $13x - 23y = 1$.

1. Déterminer un couple d'entiers solution de cette équation par l'algorithme d'Euclide.
2. Déterminer l'ensemble des couples d'entiers solutions de cette équation.

EXERCICE 21 : POINTS ENTIERS D'UNE DROITE ⋆⋆

Dans un repère orthonormé, on considère la droite $\mathcal{D}$ d'équation $7x - 4y = 3$.

1. Le point $A(1;1)$ appartient-il à $\mathcal{D}$?
2. Déterminer tous les points de $\mathcal{D}$ dont les deux coordonnées sont des entiers relatifs.
3. Quels sont ceux dont l'abscisse est comprise entre 0 et 20 et dont l'ordonnée est positive ? Représenter $\mathcal{D}$ et ces points pour $0 \leqslant x \leqslant 10$.
4. Que constate-t-on sur l'écart entre deux points consécutifs à coordonnées entières ?

EXERCICE 22 ⋆⋆

1. Démontrer que : $\forall n \in \mathbb{Z}$, $\text{PGCD}(14n + 3, 5n + 1) = 1$.
2. On considère l'équation diophantienne suivante : (E) $87x + 31y = 2$.
   (a) Vérifier, à l'aide de la question 1, que 87 et 31 sont premiers entre eux.
   (b) En déduire un couple (u, v) d'entiers relatifs tels que $87u + 31v = 1$ puis un couple (x_0, y_0) solution de (E).
   (c) Déterminer l'ensemble des solutions de (E).
3. **Application :** Trouver les points de la droite $87x - 31y - 2 = 0$ dont les coordonnées sont des entiers naturels et dont l'abscisse est comprise entre 0 et 10.

EXERCICE 23 ⋆⋆

1. On considère l'équation (E) : $8x + 5y = 1$, où (x, y) est un couple d'entiers.
   (a) Donner une solution particulière de l'équation (E).
   (b) Résoudre l'équation (E).
2. Soit $n \in \mathbb{N}$ tel qu'il existe un couple (a, b) d'entiers vérifiant : $\begin{cases} n = 8a + 1 \\ n = 5b + 2 \end{cases}$
   (a) Montrer que le couple $(a, -b)$ est solution de (E).

(b) Quel est le reste, dans la division de n par 40 ?

3. (a) Résoudre l'équation $8x + 5y = 100$, où (x, y) est un couple d'entiers.

   (b) Au VIIIe siècle, un groupe d'hommes et de femmes a dépensé 100 pièces de monnaie dans une auberge. Les hommes ont dépensé 8 pièces chacun et les femmes 5 pièces chacune. Combien pouvait-il y avoir d'hommes et de femmes dans le groupe ?

EXERCICE 24 : À LA FERME ⋆⋆

Un éleveur dépense exactement 200 € pour acheter des poules à 7 € pièce et des lapins à 11 € pièce. Il achète au moins un animal de chaque sorte.

1. Traduire la situation par une équation diophantienne d'inconnues x (nombre de poules) et y (nombre de lapins).
2. Déterminer un couple de Bézout pour 7 et 11, puis une solution particulière de l'équation.
3. Résoudre l'équation dans $\mathbb{Z}^2$, puis déterminer les achats possibles.

EXERCICE 25 ⋆⋆⋆

28 personnes participent à un repas gastronomique. Le prix normal est de 26€ sauf pour les étudiants et les enfants qui paient respectivement 17 et 13 euros. La somme totale recueillie est de 613€.

Calculer le nombre d'étudiants et d'enfants ayant participé au repas.

Approfondissements

EXERCICE 26 : THÉORÈME DES RESTES CHINOIS ⋆⋆

On veut déterminer l'ensemble S des entiers $n \in \mathbb{Z}$ vérifiant : $\begin{cases} n \equiv 9\ [17] \\ n \equiv 3\ [5] \end{cases}$

1. Recherche d'un élément de S.
   On désigne par (u, v) un couple d'entiers relatifs tel que : $17u + 5v = 1$.

   (a) Justifier l'existence d'un tel couple (u, v).

   (b) On pose $n_0 = 3 \times 17u + 9 \times 5v$. Démontrer que n_0 appartient à S.

   (c) Donner un exemple d'entier n_0 appartenant à S.

2. Caractérisation des éléments de S.

   (a) Soit n un entier relatif appartenant à S. Démontrer que $n - n_0 \equiv 0\ [85]$.

   (b) En déduire qu'un entier relatif n appartient à S si et seulement si n peut s'écrire sous la forme $n = 43 + 85k$ où k est un entier relatif.

3. **Application :** Zoé sait qu'elle a entre 300 et 400 jetons. Si elle fait des tas de 17 jetons, il lui en reste 9. Si elle fait des tas de 5 jetons, il lui en reste 3. Combien a-t-elle de jetons ?

EXERCICE 27 : RESTES CHINOIS AVEC DES MODULES NON PREMIERS ENTRE EUX ⋆⋆⋆

1. Montrer qu'aucun entier n ne vérifie à la fois $n \equiv 1\ [6]$ et $n \equiv 4\ [8]$.
2. On cherche les entiers n tels que $n \equiv 3\ [6]$ et $n \equiv 5\ [8]$.

   (a) Montrer que n convient si et seulement s'il existe deux entiers a et b tels que $n = 6a + 3 = 8b + 5$, et en déduire que $3a - 4b = 1$.

   (b) Résoudre l'équation $3a - 4b = 1$ dans $\mathbb{Z}^2$, et en déduire que les entiers cherchés sont ceux qui vérifient $n \equiv 21\ [24]$.

3. Comparer avec l'exercice 26 : pourquoi l'ensemble des solutions n'est-il pas formé des entiers congrus à un même nombre modulo $6 \times 8 = 48$?

EXERCICE 28 ⋆⋆

Soit (u_n) la suite définie sur $\mathbb{N}$ par : $\begin{cases} u_0 = 0 \\ u_{n+1} = 4u_n + 1 \end{cases}$

1. (a) Calculer u_1, u_2 et u_3.
   (b) Montrer que pour $n \in \mathbb{N}$, u_{n+1} et u_n sont premiers entre eux.
2. On pose pour $n \in \mathbb{N}$: $v_n = u_n + \dfrac{1}{3}$
   (a) Montrer que (v_n) est une suite géométrique.
   (b) En déduire l'expression de v_n puis celle de u_n en fonction de n.
3. Calculer $\text{PGCD}(4^{n+1} - 1, 4^n - 1)$.

EXERCICE 29 : PGCD ET PPCM ⋆⋆⋆

Soient a et b deux entiers naturels non nuls. On appelle *plus petit commun multiple* de a et b, noté $\text{PPCM}(a, b)$, le plus petit entier naturel non nul qui soit à la fois multiple de a et de b. On note $d = \text{PGCD}(a, b)$, et on écrit $a = da'$ et $b = db'$.

1. Justifier que a' et b' sont premiers entre eux.
2. On pose $m = da'b'$. Vérifier que m est un multiple commun de a et b.
3. Soit M un multiple commun de a et b non nul. En écrivant $M = ak$, montrer à l'aide du théorème de Gauss que b' divise k, puis que m divise M.
4. En déduire que $\text{PPCM}(a, b) = m$, puis que $\text{PGCD}(a, b) \times \text{PPCM}(a, b) = ab$.
5. **Application :** deux roues dentées engrènent l'une sur l'autre. La première a 36 dents, la seconde 60. On marque d'un point rouge les deux dents en contact au départ. Combien de tours doit faire chaque roue pour que les deux points rouges se retrouvent en contact pour la première fois ?

EXERCICE 30 : NOMBRES DE FERMAT ⋆⋆

1. (a) Montrer que pour tout $x \in \mathbb{N}$ et $k \in \mathbb{N}^*$:
   $$x^{2k+1} + 1 = (x + 1)(x^{2k} - x^{2k-1} + \cdots + x^2 - x + 1)$$
   (b) Montrer que si m est impair alors, $2^m + 1$ n'est pas premier.
   (c) Montrer que si m est un entier possédant un diviseur strict impair alors, $2^m + 1$ n'est pas premier.
   (d) En déduire que les seuls nombres premiers de la forme $(2^m + 1)$ sont de la forme $2^{2^n} + 1$.
2. On appelle **nombre de Fermat** tout nombre noté F_n tel que : $F_n = 2^{2^n} + 1$.
   (a) Calculer F_0, F_1, F_2, F_3, F_4 et vérifier qu'ils sont tous premiers.
   (b) Fermat pensait que F_5 était également premier. Qu'en pensez-vous ? On pourra utiliser un algorithme donnant la primalité d'un nombre.
   (c) Vérifier que pour tout $n \in \mathbb{N}$: $F_{n+1} = (F_n - 1)^2 + 1$. En déduire $\text{PGCD}(F_n, F_{n+1})$.
3. Montrer par récurrence que tout nombre de Fermat F_n pour $n \geqslant 2$ a une écriture décimale se terminant par 7.

EXERCICE 31 : CRYPTAGE RSA, TIRÉ DU BAC 2018 ⋆⋆

Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens **Ronald Rivest**, **Adi Shamir** et **Leonard Adleman**, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978. Les questions 1 et 2 sont des questions préparatoires, la question 3 aborde le cryptage, la question 4 le décryptage.

1. Cette question envisage de calculer le reste dans la division euclidienne par 55 de certaines puissances de l'entier 8.

   (a) Vérifier que $8^7 \equiv 2$ [55]. En déduire le reste de la division euclidienne par 55 du nombre 8^{21}.

   (b) Vérifier que $8^2 \equiv 9$ [55] puis en déduire à l'aide de la question a) le reste de la division euclidienne par 55 de 8^{23}.

2. Dans cette question, on considère l'équation (E) : $23x - 40y = 1$, dont les solutions sont des couples (x, y) d'entiers relatifs.

   (a) Justifier le fait que l'équation (E) admet au moins un couple solution.

   (b) Donner un couple, solution particulière de l'équation (E).

   (c) Déterminer tous les couples d'entiers relatifs solutions de l'équation (E).

   (d) En déduire qu'il existe un unique entier d vérifiant les conditions $0 \leqslant d < 40$ et $23d \equiv 1$ [40].

3. **Cryptage dans le système RSA.**
   Une personne A choisit deux nombres premiers p et q , puis calcule les produits $N = p \times q$ et $n = (p-1) \times (q-1)$. Elle choisit également un entier naturel c premier avec n. La personne publie le couple $(N; c)$ qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté. Les messages sont numérotés et transformés en une suite d'entiers compris entre 0 et $N - 1$.

   Pour crypter un entier a de cette suite, on procède ainsi : on calcule le reste b dans la division euclidienne par N du nombre a^c et le nombre crypté est l'entier b. Dans la pratique, cette méthode est sûre si la personne A choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres.

   On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 11$. La personne A choisit également $c = 23$.

   (a) Calculer les nombres N et n, puis justifier que c vérifie la condition voulue.

   (b) Un émetteur souhaite envoyer à la personne A le nombre $a = 8$. Déterminer la valeur du nombre crypté b.

4. **Décryptage dans le système RSA.**
   La personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions : $0 \leqslant d < n$ et $cd \equiv 1$ [n]. Elle garde secret le nombre d qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec la clé publique.

   Pour décrypter un nombre crypté b, la personne A calcule le reste de la division euclidienne par N du nombre b^d , et le nombre en clair (c'est-à-dire le nombre avant le cryptage) est le nombre a.

   On admet l'existence et l'unicité de l'entier d, et le fait que le décryptage fonctionne. Les nombres choisis par A sont encore $p = 5$, $q = 11$ et $c = 23$.

   (a) Quelle est la valeur de d ?

   (b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.

Pour aller plus loin

EXERCICE 32 ⋆⋆

Pour $n \in \mathbb{N}$, montrer que les nombres entiers $14n+3$ et $21n+4$ sont premiers entre eux. On explicitera une relation de Bézout.

EXERCICE 33 ⋆⋆

La suite de Fibonacci $(F_n)_{n \geqslant 0}$ est définie par $F_0 = 0$, $F_1 = 1$ et, pour tout $n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$. Pour $n \in \mathbb{N}$, calculer $\text{PGCD}(F_n, F_{n+1})$.

EXERCICE 34 ⋆⋆

Soit $n \geqslant 2$ un entier. On dit qu'un entier a admet un *inverse modulo* n s'il existe un entier x tel que $ax \equiv 1\ [n]$. Montrer que n est premier si et seulement si tout élément de $\{1, \dots, n-1\}$ admet un inverse modulo n.

EXERCICE 35 ⋆⋆⋆

Soient a et b deux éléments de $\mathbb{N}^*$. Montrer que a et b sont premiers entre eux si et seulement si $a+b$ et ab sont premiers entre eux.

EXERCICE 36 ⋆⋆⋆

Soient a et b deux entiers relatifs premiers entre eux, $(k, \ell) \in \mathbb{N}^{*2}$.

a) Montrer que a^k et b sont premiers entre eux. On déduira d'une relation de Bézout entre a et b une relation de Bézout entre a^k et b.

b) Montrer que a^k et b^ℓ sont premiers entre eux.

EXERCICE 37 ⋆⋆⋆

Soient u et v deux entiers supérieurs ou égaux à 2 et premiers entre eux. Montrer que le nombre $\dfrac{\ln(v)}{\ln(u)}$ est irrationnel.

EXERCICE 38 : RACINES RATIONNELLES D'UN POLYNÔME ⋆⋆⋆

Soient $n \in \mathbb{N}^*$, $a_0, \dots, a_n$ des entiers relatifs avec $a_0 a_n \neq 0$, et P la fonction polynomiale définie par $P(x) = \sum_{k=0}^{n} a_k x^k$.

a) Soit r une racine rationnelle de P. On écrit $r = \dfrac{p}{q}$ où $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ sont premiers entre eux. Montrer que q divise a_n et que p divise a_0. On pourra utiliser l'exercice 36.

b) En déduire que $\sqrt{2}$ est irrationnel.

c) Montrer que l'équation $x^5 - 5x + 7 = 0$ admet une unique solution réelle, puis que cette solution est un nombre irrationnel.

EXERCICE 39 : L'ÉQUATION DIOPHANTIENNE $ax + by = c$ ⋆⋆⋆⋆

Soient a et b deux éléments de $\mathbb{N}^*$ et $c \in \mathbb{Z}$. On note δ le PGCD de a et b. On se propose de déterminer l'ensemble E des couples $(x, y) \in \mathbb{Z}^2$ tels que $ax + by = c$. On écrit $a = \delta a'$, $b = \delta b'$ où a' et b' sont deux entiers premiers entre eux.

a) Montrer que E est non vide si et seulement si $\delta \mid c$.

On suppose dans la suite que $\delta \mid c$. On fixe un élément (x_0, y_0) de E.

b) Pour $(x, y) \in \mathbb{Z}^2$, vérifier que $(x, y) \in E \iff a'(x - x_0) = b'(y_0 - y)$.

c) Montrer que $E = \{(x_0 + tb',\ y_0 - ta')\ ;\ t \in \mathbb{Z}\}$.

EXERCICE 40 ⋆⋆⋆⋆

Selon la valeur de $n \in \mathbb{Z}$, déterminer le PGCD de $n^3 + n$ et $2n + 1$.

EXERCICE 41 ⋆⋆⋆⋆

En utilisant l'exercice 31 du chapitre 1, montrer que, si $a \geqslant 2$ est un entier, m et n deux éléments de $\mathbb{N}^*$, alors $a^m - 1$ et $a^n - 1$ ont pour PGCD $a^{\mathrm{PGCD}(m,n)} - 1$.

EXERCICE 42 : RELATION DE BÉZOUT À COEFFICIENTS DANS $\mathbb{N}$ ⋆⋆⋆⋆

Soient a et b deux éléments de $\mathbb{N}^*$ premiers entre eux.

a) Montrer que $ab - a - b$ n'est pas de la forme $au + bv$ avec u et v dans $\mathbb{N}$.

b) Montrer que si n est un entier $\geqslant ab - a - b + 1$ alors n s'écrit $au + bv$ où $(u, v) \in \mathbb{N}^2$. On pourra remarquer que les $n - au$ pour $u \in \{0, \ldots, b-1\}$ sont supérieurs ou égaux à $1 - b$ et ont des restes distincts dans la division euclidienne par b.

c) Application : avec des pièces de 5 et de 8 centimes, quel est le plus grand montant que l'on ne peut pas payer exactement ? Lister les montants impossibles, et comparer leur nombre à $\dfrac{(a-1)(b-1)}{2}$.