3. Énoncés des exercices

Exercice 7.1 PGCD et décomposition en facteurs premiers

1. Déterminer la décomposition en facteurs premiers des nombres 26460 et 34650.
2. En déduire $PGCD(26460; 34650)$
3. En déduire la forme irréductible de la fraction $\frac{26460}{34650}$

Exercice 7.2 Algorithme d'Euclide Algorithme d'Euclide pour la recherche de $PGCD(a, b)$ (on ne perd pas en généralité en supposant $a > b$).
Le PGCD de a et b est le dernier reste non nul dans la suite de divisions successives ci-dessous :

- On écrit la division euclidienne de a par b :

  $$a = b \times q_0 + r_0$$

  avec $0 \leqslant r_0 < b$
- Si $r_0 = 0$, $PGCD(a, b) = b$
  Sinon, $PGCD(a, b) = PGCD(b, r_0)$ et on écrit la division euclidienne de b par r_0 :

  $$b = r_0 \times q_1 + r_1$$

  avec $0 \leqslant r_1 < r_0$
- Si $r_1 = 0$, $PGCD(b, r_0) = r_0$
  Sinon, $PGCD(a, b) = PGCD(b, r_0) = PGCD(r_0, r_1)$ et on écrit la division euclidienne de r_0 par r_1 :

  $$r_0 = r_1 \times q_2 + r_2$$

  avec $0 \leqslant r_2 < r_1$
  etc... le dernier reste non nul est le PGCD cherché.

Application :
Utiliser l'algorithme d'Euclide pour calculer $PGCD(712; 114)$.

Exercice 7.3 Démonstration de la caractérisation du PGCD Soient $a, b \in \mathbb{N}^*$.

1. (a) On note D le PGCD de a et b. Justifier que $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers naturels non nuls.
   (b) Soit d le PGCD de $\frac{a}{D}$ et $\frac{b}{D}$. En utilisant la propriété d'homogénéité, montrer que $d = 1$.
2. Réciproquement, on suppose que $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers premiers entre eux. Montrer que $PGCD(a, b) = D$.

Exercice 7.4 Nombres de Fermat, infinité des nombres premiers (démonstration de George Polya, vers 1920) On appelle *nombres de Fermat* les nombres de la forme

$$F_n = 2^{2^n} + 1$$

1. Montrons que les nombres de Fermat, pris deux à deux, sont premiers entre eux. Soit $x \in \mathbb{Z}$.
   (a) Calculer
   $$(1 - x + x^2 - x^3 + ... + (-1)^{p-1}x^{p-1})(1 + x)$$
   (b) En déduire que si p est pair, alors il existe un entier N tel que $x^p - 1 = (1 + x) \times N$
   (c) Soit $k \in \mathbb{N}^*$. Montrer qu'il existe un entier N tel que $F_{n+k} - 2 = F_n \times N$
   (d) En déduire que F_{n+k} et F_n sont premiers entre eux.
2. En déduire qu'il existe une infinité de nombres premiers.
   Coup de pouce : *Si deux nombres sont premiers entre eux, alors les diviseurs premiers de l'un sont distincts des diviseurs premiers de l'autre. Ainsi, si deux nombres sont premiers entre eux, alors il existe au moins deux nombres premiers différents...*

Exercice 7.5 Unicité de la décomposition en facteurs premiers. Soit $n \in \mathbb{N}$, $n \geqslant 2$.
On va raisonner par l'absurde et supposer que n ait deux décompositions en facteurs premiers :

- $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_m^{\alpha_m}$, avec $\alpha_1, \alpha_2, ...\alpha_m \in \mathbb{N}^*$, et $p_1, p_2, ..., p_m$ premiers tels que $p_1 < p_2 < ... < p_m$;
- $n = q_1^{\beta_1} \times q_2^{\beta_2} \times ... \times q_r^{\beta_r}$, avec $\beta_1, \beta_2, ...\beta_r \in \mathbb{N}^*$, et $q_1, q_2, ..., q_r$ premiers tels que $q_1 < q_2 < ... < q_r$.

1. Soient $i \in [\![1; m]\!]$ et $j \in [\![1; r]\!]$.

(a) Montrer que si $p_i \neq q_j$, alors $p_i^{\alpha_i}$ et $q_j^{\beta_j}$ sont premiers entre eux.

(b) En déduire que $\forall i \in [\![1;m]\!]$, $\exists j \in [\![1;r]\!]$ t.q. $p_i = q_j$.

(c) En déduire que $m = r$, $p_1 = q_1$, $p_2 = q_2$,...,$p_m = q_m$.

2. Pour l'instant, on a donc : $p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_m^{\alpha_m} = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_m^{\beta_m}$.
Il reste à montrer que les exposants sont les mêmes. raisonnons par l'absurde et supposons par exemple que $\alpha_1 < \beta_1$.
S'inspirer de la question $1.a$ pour montrer que $p_1^{\beta_1 - \alpha_1}$ est premier avec chaque $p_i^{\alpha_i}$, $i \in [\![2;m]\!]$.
Conclure.
On raisonnerait de même pour montrer que $\beta_1 < \alpha_1$, conclure.
On raisonnerait de même avec α_2 et β_2, ... α_m et β_m. Conclure.

Exercice 7.6 Dans tout l'exercice, x et y désignent des entiers naturels non nuls vérifiant $x < y$. S est l'ensemble des couples $(x;y)$ tels que $pgcd(x,y) = y - x$.

1. (a) Calculer $pgcd(363;484)$

   (b) Le couple $(363;484)$ appartient-il à S ?

2. Soit n un entier naturel non nul ; le couple $(n;n+1)$ appartient-il à S ? Justifier votre réponse.

3. Montrer que $(x;y)$ appartient à S ssi il existe un entier naturel non nul k t.q. $x = k(y-x)$ et $y = (k+1)(y-x)$

Exercice 7.7 Soit n un entier naturel supérieur ou égal à 2.

1. Montrer que n et $2n+1$ sont premiers entre eux.

2. On pose $\alpha = n+3$ et $\beta = 2n+1$, et on note δ le pgcd de α et β.

   (a) Calculer $2\alpha - \beta$ et en déduire les valeurs possibles de δ

   (b) Démontrer que α et β sont multiples de 5 ssi $(n-2)$ est multiple de 5.

3. On considère les nombres a et b définis par : $a = n^3 + 2n^2 - 3n$ et $b = 2n^2 - n - 1$.
Montrer, après factorisation, que a et b sont des entiers naturels divisibles par $(n-1)$.

4. (a) On note d le pgcd de $n(n+3)$ et de $(2n+1)$.
   Montrer que δ divise d, puis que $\delta = d$.

   (b) En déduire le pgcd Δ de a et b en fonction de n.

   (c) Déterminer Δ pour $n = 2001$ puis pour $n = 2002$

Exercice 7.8

1. Déterminer le pgcd de 66 et 15 à l'aide de l'algorithme d'Euclide, en détaillant chaque étape.
2. A l'aide de la dernière division de reste non nul, trouver deux entiers a et b tels que $3 = 15 \times a + 6 \times b$ (E_1)
3. A l'aide de la division précédente, trouver a' et b' tels que $6 = 66 \times a' + 15 \times b'$ (E_2)
4. En remplaçant (E_2) dans (E_1), trouver une combinaison linéaire entre 15 et 66 qui donne 3.

Exercice 7.9

1. Soit x un entier naturel tel que $x \equiv 0\,[7]$ et $x \equiv 0\,[3]$.
Montrer que x est aussi congru à 0 modulo 21.
2. Cette propriété est-elle généralisable ? C'est-à-dire si $x \equiv 0\,[m]$ et $x \equiv 0\,[n]$, a-t-on $x \equiv 0\,[mn]$?

Exercice 7.10 On considère deux entiers naturels non nuls a et b tels que $a^2 = b^3$.
On note d la PGCD de a et b ; u et v désignent les entiers tels que $a = du$ et $b = dv$.

1. (a) Démontrer que $u^2 = dv^3$

   (b) en déduire que v divise u, puis que $v = 1$

2. Démontrer que $a^2 = b^3$ ssi a et b sont respectivement le cube et le carré d'un même entier.

. Équations diophantiennes (équations en entiers)

Exercice 7.11 Déterminer les couples d'entiers naturels $(x; y)$ tels que $x^2y + y = 102$

Exercice 7.12 Le but de cet exercice est de résoudre dans $\mathbb{Z}^2$ l'équation diophantienne $5x + 4y = 1$

1. Déterminer une solution particulière $(x_0; y_0)$
2. En déduire que $5(x - x_0) = 4(y_0 - y)$
3. En déduire tous les couples solutions.

Exercice 7.13 Le but de cet exercice est de résoudre dans $\mathbb{Z}^2$ l'équation diophantienne $35a + 8b = 4$

1. Déterminer une solution particulière.
   Aide : on cherchera d'abord à trouver une solution particulière de l'équation $35a + 8b = 1$.
2. déterminer alors tous les couples solutions de l'équation.

Exercice 7.14 La nouvelle lune tombe un lundi. Dans combien de jours la nouvelle lune aura-t-elle lieu à nouveau un lundi ?
(La lunaison, période entre deux nouvelles lunes, varie un peu mais on considèrera qu'elle est de 29 jours).

Exercice 7.15 Le but de cet exercice est de déterminer l'ensemble des entiers relatifs x, y, z avec x premier tels que : $z = x^2 + y^2$ et $z = xy + 2x$.
Cela correspond à chercher les points à coordonnées entières dans l'intersection entre une paraboloïde et un plan.

1. (a) Montrer que $y(y - x) = x(2 - x)$
   (b) En déduire que le nombre premier x divise y.
2. On pose $y = kx$, avec $k \in \mathbb{Z}$
   (a) Montrer que x divise 2, puis que $x = 2$.
   (b) En déduire les valeurs possibles de k.
3. Donner les solutions du système.

. Cryptographie

Exercice 7.16 Le chiffre de César Pendant la guerre des Gaules, au premier siècle av. J.C., Jules César codait ses messages par un décalage simple de trois caractères vers la droite : Le A est codé par D, le Y par B, le Z par C, etc...
Le but de cet exercice est de déterminer les fonctions permettant de coder et décoder le chiffrement de César.
A toute lettre de l'alphabet, on associe un entier compris entre 0 et 25 de la manière suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Appelons f la fonction permettant de coder ; la lettre associée à l'entier x sera alors codée par la lettre associée à l'entier $f(x)$.
On calcule d'abord $x + 3$, puis on prend le reste de la division euclidienne de $x + 3$ par 26 pour se ramener à un entier compris entre 0 et 25.
La fonction pour coder est donc $f(x) =$ reste de la division euclidienne de $x + 3$ par 26.
On a donc $f(x) \equiv x + 3\,[26]$, et $0 \leqslant f(x) < 26$.

1. Coder le mot ATTAQUE
2. Déterminer la fonction g de décodage
3. Décoder le mot IDFLOH

Dans chiffre de César, comme on décale de 3 rangs, on dira que la "clé" de chiffrement est 3.

Exercice 7.17 Un chiffrement affine La lettre associée à l'entier x est codée par la lettre associée à $f(x)$, reste de la division euclidienne de $21x + 11$ par 26.

1. Coder le mot RIGOLO
2. Soient x et x' des entiers compris entre 0 et 25 inclus, tels que $f(x) \equiv f(x')\,[26]$.
   (a) Montrer que$21(x - x') = 26k$, avec $k \in \mathbb{Z}$
   (b) En déduire que $x \equiv x'\,[26]$, puis que $x = x'$.

3. Déterminer la fonction g de décodage.
   (Aide : déterminer l'inverse de 21 modulo 26).
4. Décoder le mot GLB

Dans un chiffrement affine du type $f(x) = ax + b$, la "clé" est le couple $(a; b)$; ici, la clé est $(21; 11)$.

Exercice 7.18 PARTIE A :
On considère l'équation (E) : $11x - 26y = 1$, avec $x, y \in \mathbb{Z}$.

1. Vérifier que le couple $(-7, -3)$ est solution de (E).
2. Résoudre alors l'équation (E).
3. En déduire le couple $(u; v)$ d'entiers relatifs solution de (E) tel que $0 \leqslant u \leqslant 25$.

PARTIE B :
On assimile chaque lettre de l'alphabet à un entier, comme dans le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On "code" tout nombre entier x compris entre 0 et 25 de la façon suivante :
on calcule $11x + 8$;
on calcule le reste de la division euclidienne de $11x + 8$ par 26, que l'on appelle y ;
L'entier x est alors "codé" par y.
Ainsi par exemple, la lettre L est assimilée au nombre 11 ;
$11 \times 11 + 8 = 129 \equiv 25\,[26]$.
Au nombre 25 correspond la lettre Z.
La lettre L est donc codée par la lettre Z.

1. Coder la lettre W
2. le but de cette question est de déterminer la fonction de décodage.
   (a) Montrer que $\forall x, j \in \mathbb{Z}$, on a $11x \equiv j\,[26] \Leftrightarrow x \equiv 19j\,[26]$.
   (b) En déduire un procédé de décodage.
   (c) Décoder la lettre W.

Exercice 7.19 Le "petit théorème" de Fermat Théorème : Soient p un entier naturel premier, et a un entier. Si p ne divise pas a, alors p divise $a^{p-1} - 1$.

1. Démonstration. Pour chaque entier k compris entre 1 et $p - 1$, notons r_k le reste de la division euclidienne de $k \times a$ par p.
   Ainsi, $ka \equiv r_k\,[p]$, et $0 \leqslant r_k \leqslant p - 1$.
   (a) Justifier que $r_k \neq 0$.
   (b) Montrer que, pour deux entiers k et k' quelconques, compris entre 1 et $p - 1$, si $r_k = r_{k'}$, alors $k = k'$.
   En déduire que l'ensemble des restes $\{r_1, r_2, ..., r_{p-1}\}$ est confondu avec l'ensemble $\{1, 2, ..., p - 1\}$.
   (c) On note $(p - 1)!$ le produit des entiers de 1 à $(p - 1)$. Déduire de la question précédente que : $(p - 1)!a^{p-1} \equiv (p - 1)!\,[p]$.
   Aide : Si $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$, alors $ab \equiv a'b'\,[n]$.
2. Conséquence.
   Démontrer que pour tout entier naturel a et tout entier premier p, $a^p \equiv a\,[p]$.
3. Application.
   Soit p un entier premier supérieur ou égal à 3.
   Montrer que p divise $\sum_{k=0}^{p-2} 2^k$.
   Aide : penser à la somme $1 + q + q^2 + ... + q^n$ du cours sur les suites.