Théorèmes de Bezout et de Gauss – Exercices

PGCD

1 Déterminer sans calcul le PGCD des nombres suivants.
1. $a = 25 \times 8$ et $b = 25 \times 11$
2. $a = 2^4 \times 3 \times 5^2$ et $b = 2^2 \times 5^3$
3. $a = 5 \times 7^2 \times 24$ et $b = 35 \times 16$

2 Calculer le PGCD de 308 et 448 puis de 3020 et 2880.

3 Quel est le PGCD :
a. de deux entiers consécutifs ?
b. de deux entiers pairs consécutifs ?
c. de deux entiers impairs consécutifs ?

4 On note d un diviseur des entiers non nuls a et b.
1. Démontrer que d divise $4a + 3b$ et $5a + 4b$.
2. Réciproquement, démontrer que tout diviseur de $4a + 3b$ et $5a + 4b$ divise a et b.
3. En déduire que $(a; b)$ et $(4a + 3b; 5a + 4b)$ ont le même PGCD.

5 Pour tout entier naturel n, on pose $a = 4n + 1$ et $b = 5n + 3$.
1. Émettre une conjecture sur leur PGCD à l'aide d'un tableur.
2. Démontrer la conjecture.

6 Calculer, en fonction de n, le PGCD de
a. $a = 3n + 5$ et $b = 2n - 1$;
b. $a = 5n + 3$ et $b = 2n + 2$;
c. $a = 2n - 1$ et $b = 9n + 4$.

7 Montrer que pour tout entier n, $\text{PGCD}(n^2 + 2n; n + 3)$ est égal à 3 si $n \equiv 0$ [3] et à 1 sinon.

8 À l'aide de l'algorithme d'Euclide, déterminer le PGCD des couples $(279; 11222)$, $(6157; 1645)$ et $(747; 310)$.

9 Calculer, sans calculatrice, le PGCD de $2^{15} - 1$ et $2^{24} - 1$ à l'aide de l'algorithme d'Euclide.

10 Soit $s_n = \sum_{k=0}^{n} k$.
1. Donner une expression explicite de s_n.
2. Soit $d_n = \text{PGCD}(s_n; s_{n+1})$. Calculer d_n lorsque $n = 2k$ puis lorsque $n = 2k + 1$ (k entier naturel).
3. En déduire que pour $n \geq 2$, s_n et s_{n+1} ne sont jamais premiers entre eux, puis que s_n, s_{n+1} et s_{n+2} sont premiers entre eux dans leur ensemble.

11 Soit n un entier supérieur ou égal à 1
1. Déterminer le PGCD des nombres entiers $n(n + 1)$ et $(n - 1)(n + 2)$.
On pourra, pour cela, former leur différence.
Qu'en conclure pour les nombres
$$a = \frac{n(n+1)}{2} \text{ et } b = \frac{(n-1)(n+2)}{2} ?$$
2. Pour tout entier $n \geq 2$, on considère les nombres
$$b = \frac{(n-1)(n+2)}{2} \text{ et } c = \frac{(n-2)(n+3)}{2}.$$
Déterminer le PGCD de b et c, suivant les valeurs du reste de la division de n par 4.

Théorème de Bezout

12 Montrer que pour tout entier n, $n^2 + 2n$ et $n + 1$ sont premiers entre eux.

13 Dire si les nombres suivants sont premiers entre eux.
1. $a = 2142$ et $b = 3351$
2. $a = 38$ et $b = 45$

14 Soit m et n deux entiers naturels non nuls tels que
$$\text{PGCD}(m; n) = 7 \text{ et } mn = 588.$$
1. Justifier l'existence de deux entiers m' et n' premiers entre eux tels que $m'n' = 12$.
2. Quelles sont les valeurs possibles de m' et n' ?
En déduire les valeurs possibles de m et n.

15 Déterminer les couples d'entiers naturels $(a; b)$ tels que
$$a + b = 296 \text{ et } \text{PGCD}(a; b) = 37.$$

16 Appliquer l'algorithme d'Euclide aux entiers suivants puis trouver une relation de Bezout.
1. $a = 38$ et $b = 17$;
2. $a = 48$ et $a = 15$;
3. $a = 2706$ et $b = 402$.

17 Montrer que deux entiers a et b sont premiers entre eux si et seulement si a^2 et b^2 sont premiers entre eux.

Théorème de Gauss, équation $ax + by = c$

18 Soit n un entier. Montrer que si $7n$ est pair, alors n est pair.

19 Déterminer les entiers m et n tels que
a. $33m = 14n$ **b.** $63m = 91n$

20 Démontrer que pour tout entier naturel n, l'entier $n^2(n^2 - 1)$ est divisible par 3, par 4 et par 12.

21 Vrai ou faux ? « Si n est un entier pair et m un entier impair, alors $\text{PGCD}(n: m) = \text{PGCD}\left(\frac{n}{2}; m\right)$.

22 Trouver les entiers p et q dont le PGCD est 12 et le rapport $\frac{7}{9}$.

23 Voici un critère de divisibilité par 7 : « soustraire deux fois le dernier chiffre au nombre sans le dernier chiffre. Si ce nombre est divisible par 7, le nombre complet l'est également ».
Par exemple 861 est divisible par 7 car $86 - 2 \times 1 = 84$, puis $8 - 2 \times 4 = 0$, qui est bien divisible par 7.
Justifier ce critère en démontrant l'équivalence suivante, où d et u sont des entiers
$$7|10d + u \Leftrightarrow 7|d - 2u.$$
On pourra remarquer que $21u = 7 \times 3u$…

24 Déterminer une solution particulière de l'équation
$$24x - 13y = 1 \ (E_1).$$
Déduire une solution particulière des équations suivantes.
$24x + 13y = 1 \ (E_2)$ $24x + 13y = 4 \ (E_3)$
$-24x + 13y = 1 \ (E_4)$ $-24x - 13y = 2 \ (E_5)$

25 On cherche les solutions entières de l'équation

$$11x - 14y = 1.$$

1. Déterminer une solution $(x_0; y_0)$.
2. Montrer qu'une solution $(x; y)$ vérifie l'équation
$$11(x - x_0) = 14(y - y_0).$$
3. Résoudre cette équation.

26 Résoudre l'équation $5x + 17y = 4$ (x, y entiers).

27 Résoudre l'équation $9x \equiv 7\ [11]$, où x est un entier.

28 *(2011, métropole).* On se propose de déterminer l'ensemble S des entiers relatifs n vérifiant le système

$$\begin{cases} n \equiv 9\ [17] \\ n \equiv 3\ [5] \end{cases}.$$

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 s'il existe un entier relatif k tel que $n = 43 + 85k$.
3. 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 ?

29 Voici un problème trouvé dans un livre d'un mathématicien chinois du 3e siècle : « Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ? ».
Soit n le nombre de soldats de l'armée.

1. Justifier que n vérifie $\begin{cases} n \equiv 2\ [3] \\ n \equiv 3\ [5] \\ n \equiv 2\ [7] \end{cases}$.
2. Soit n une solution du système $\begin{cases} n \equiv 2\ [3] \\ n \equiv 3\ [5] \end{cases}$.
   a. Justifier qu'il existe deux entiers k et k' tels que $3k - 5k' = 1$ puis résoudre cette équation.
   b. En déduire que $\begin{cases} n \equiv 2\ [3] \\ n \equiv 3\ [5] \end{cases} \Leftrightarrow n \equiv 8\ [15]$.
3. Démontrer que $\begin{cases} n \equiv 2\ [3] \\ n \equiv 3\ [5] \\ n \equiv 2\ [7] \end{cases} \Leftrightarrow n \equiv 23\ [105]$.
4. Déterminer le nombre de soldat de cette armée, sachant qu'il est compris entre 7000 et 7100.

30 Montrer que pour tout entier naturel n, la fraction $\frac{n(2n+1)}{n+1}$ est irréductible.

Problèmes, sujets de baccalauréat

31 *(ISBN 10).* Le code ISBN (International Standard Book Number, Numéro international normalisé du livre) permet d'identifier chaque livre de manière unique dans le monde entier. Il sert notamment de numéro de référence dans les bases de données informatiques (bibliothèques, éditeurs). Il est composé de dix chiffres répartis en quatre groupes séparés par des tirets.

Exemples : ISBN 2-266-02612-7 ou ISBN 2-86623-490-1.
Le premier groupe correspond au pays de l'éditeur (2 pour la France), le deuxième groupe est le numéro de l'éditeur, le troisième celui du livre, enfin le dernier chiffre est une clé qui sert à vérifier qu'on n'a pas effectué d'erreurs de saisie en rentrant le code dans un ordinateur. Cette clé est calculée de la manière suivante.

À partir des neufs premiers chiffres a_1, a_2, …, a_8, a_9 (de gauche à droite sans tenir compte des tirets), on calcule la somme $e = a_1 + 2a_2 + \cdots + 8a_8 + 9a_9$. La clé est le reste de la division euclidienne de S par 11. Si ce reste est 10, on écrit alors le chiffre romain X.

Exemple : un livre américain est codé par les chiffres 0-19-857505-? La somme S vaut dans ce cas 208. Comme $208 = 18 \times 11 + 10$, la clé est X. On obtient alors le code 0-19-857505-X.

1. Supposons qu'une erreur de saisie (et une seule) ait eu lieu sur un chiffre, par exemple que le chiffre a_k ait été changé en a'_k (avec $1 \leq k \leq 9$).
   Soit e la somme correcte et e' la somme obtenue sur ce nouveau code mal saisi.
   Montrer que $e' = e + k(a'_k - a_k)$. En déduire que l'erreur ne sera pas détectée si et seulement si
   $$k(a'_k - a_k) \equiv 0\ [11].$$
   En remarquant que 11 est un nombre premier et que $-9 \leq a'_k - a_k \leq 9$, conclure.
2. Supposons que deux chiffres ait été interverti à la saisie, par exemple a_k et a_j.
   Montrer que $e' = e + (j - k)(a_k - a_j)$.
   L'erreur sera-t-elle détectée ?

32 On note N_p le rep-unit, c'est-à-dire l'entier s'écrivant avec p fois le chiffre 1 :

$$N_p = \underbrace{11\ldots1}_{p \text{ répétitions de 1}} = \sum_{k=0}^{k=p-1} 10^k.$$

On souhaite montrer qu'il existe un rep-unit divisible par 2017.

1. Montrer que $N_p = \frac{10^p - 1}{9}$.
2. On considère la division euclidienne par 2017 : expliquer pourquoi parmi les 2018 premiers rep-units, il en existe deux, au moins, ayant le même reste.
3. Soit N_p et N_q deux rep-units admettant le même reste ($p < q$). Quel est le reste de la division euclidienne de $N_q - N_p$ par 2017 ?
4. Démontrer l'égalité $N_q - N_p = N_{q-p}10^p$.
5. Conclure.

33 *(2005, Polynésie).* On considère la suite (u_n) d'entiers naturels définie par

$$u_0 = 14 \text{ et } u_{n+1} = 5u_n - 6 \text{ pour tout } n \in \mathbb{N}.$$

1. Calculer u_1, u_2, u_3 et u_4.
   Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?
2. Montrer que, pour tout $n \in \mathbb{N}$, $u_{n+2} \equiv u_n\ [4]$.
   En déduire que pour tout $k \in \mathbb{N}$, $u_{2k} \equiv 2\ [4]$ et que $u_{2k+1} \equiv 0\ [4]$.
3. **a.** Montrer par récurrence que, pour tout $n \in \mathbb{N}$,
   $$2u_n = 5^{n+2} + 3.$$

b. En déduire que, pour tout $n \in \mathbb{N}$, $2u_n \equiv 28\ [100]$.

4. Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.

5. Montrer que le PGCD de deux termes consécutifs de la suite (u_n) est constant. Préciser sa valeur.

34 *(2009, Liban).* Le but de l'exercice est de montrer qu'il existe un entier naturel n dont l'écriture décimale du cube se termine par 2009, c'est-à-dire tel que

$$n^3 \equiv 2009 \bmod 10000.$$

Partie A

1. Déterminer le reste de la division euclidienne de 2009^2 par 16.

2. En déduire que $2009^{8001} \equiv 2009 \bmod 16$.

Partie B

On considère la suite (u_n) définie sur les entiers naturels par $u_0 = 2009^2 - 1$ et, pour tout entier naturel n,

$$u_{n+1} = (u_n + 1)^5 - 1.$$

1. a. Démontrer que u_0 est divisible par 5.

b. Démontrer, en utilisant la formule du binôme de Newton, que pour tout entier naturel n,

$$u_{n+1} = u_n[u_n^4 + 5(u_n^3 + 2u_n^2 + 2u_n + 1)].$$

c. Démontrer par récurrence que ,pour tout entier naturel n, u_n est divisible par 5^{n+1}.

2. a. Vérifier que $u_3 = 2009^{250} - 1$ puis en déduire que $2009^{250} \equiv 1 \bmod 625$.

b. Démontrer alors que $2009^{8001} \equiv 2009 \bmod 625$.

Partie C

1. En utilisant le théorème de Gauss et les résultats établis dans les questions précédentes, montrer que

$$2009^{8001} - 2009$$

est divisible par 10000.

2. Conclure, c'est-à-dire déterminer un entier naturel dont l'écriture décimale du cube se termine par 2009.

35 *(2001, Nouvelle-Calédonie).*

Partie I – Soit x un nombre réel.

1. Montrer que $x^4 + 4 = (x^2 + 2)^2 - 4x^2$.

2. En déduire que $x^4 + 4$ peut s'écrire comme produit de deux trinômes à coefficients réels.

Partie II – Soit n un entier naturel supérieur ou égal à 2.

On considère les entiers

$$A = n^2 - 2n + 2 \text{ et } B = n^2 + 2n + 2$$

et d leur PGCD.

1. Montrer que $n^4 + 4$ n'est pas premier.

2. Montrer que, tout diviseur de A qui divise n, divise 2.

3. Montrer que, tout diviseur commun de A et B, divise $4n$.

4. Dans cette question on suppose que n est impair.

a. Montrer que A et B sont impairs. En déduire que d est impair.

b. Montrer que d divise n.

c. En déduire que d divise 2, puis que A et B sont premiers entre eux.

5. On suppose maintenant que n est pair.

a. Montrer que 4 ne divise pas $n^2 - 2n + 2$.

b. Montrer que d est de la forme $d = 2p$, où p est impair.

c. Montrer que p divise n. En déduire que $d = 2$. (On pourra s'inspirer de la démonstration utilisée à la question 4).

36 *(2011, Antilles-Guyane).*

1. On considère l'équation *(E)* : $11x - 7y = 5$, où x et y sont des entiers relatifs.

a. Justifier, qu'il existe un couple d'entiers relatifs $(u; v)$ tels que $11u - 7v = 1$. Trouver un tel couple.

b. En déduire une solution particulière de l'équation *(E)*.

c. Résoudre l'équation *(E)*.

d. Dans le plan rapporté à un repère orthonormé $(O; \vec{\imath}, \vec{\jmath})$, on considère la droite D d'équation cartésienne $11x - 7y - 5 = 0$. On note $\mathcal{C}$ l'ensemble des points $M(x; y)$ du plan tels que $0 \leq x \leq 50$ et $0 \leq y \leq 50$.

Déterminer le nombre de points de la droite D appartenant à l'ensemble $\mathcal{C}$ et dont les coordonnées sont des nombres entiers.

2. On considère l'équation *(F)* : $11x^2 - 7y^2 = 5$, où x et y sont des entiers relatifs.

a. Démontrer que si le couple $(x; y)$ est solution de (F), alors $x^2 \equiv 2y^2\ [5]$.

b. Soient x et y des entiers relatifs. Compléter les deux tableaux suivants :

Modulo 5, $x \equiv \ldots$	0	1	2	3	4
Modulo 5, $x^2 \equiv \ldots$					

Modulo 5, $y \equiv \ldots$					
Modulo 5, $y^2 \equiv \ldots$					

c. En déduire que si le couple $(x; y)$ est solution de *(F)*, alors x et y sont des multiples de 5.

3. Démontrer que si x et y sont des multiples de 5, alors le couple $(x; y)$ n'est pas solution de *(F)*. Que peut-on en déduire pour l'équation *(F)* ?

37 *(2016, centres étrangers).* Le but de cet exercice est d'étudier, sur un exemple, une méthode de chiffrement publiée en 1929 par le mathématicien et cryptologue Lester Hill. Ce chiffrement repose sur la donnée d'une matrice A, connue uniquement de l'émetteur et du destinataire.

Dans tout l'exercice, on note A la matrice définie par $A = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}$.

Partie A – Chiffrement de Hill

Voici les différentes étapes de chiffrement pour un mot comportant un nombre pair de lettres :

Étape 1. On divise le mot en blocs de deux lettres consécutives puis, pour chaque bloc, on effectue chacune des étapes suivantes.

Étape 2. On associe aux deux lettres du bloc les deux entiers x_1 et x_2 tous deux compris entre 0 et 25, qui correspondent aux deux lettres dans le même ordre, dans le tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Étape 3. On transforme la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ en en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ vérifiant $Y = AX$.

Étape 4. On transforme Y en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, où r_1 est le reste de la division euclidienne de y_1 par 26 et r_2 celui de la division euclidienne de y_2 par 26.
Étape 5. On associe aux entiers r_1 et r_2 les deux lettres correspondantes du tableau de l'étape 2.
Le bloc chiffré est le bloc obtenu en juxtaposant ces deux lettres.

Question : utiliser la méthode de chiffrement exposée pour chiffrer le mot « HILL ».

Partie B – Quelques outils mathématiques nécessaires au déchiffrement

1. Soit a un entier relatif premier avec 26.
Démontrer qu'il existe un entier relatif u tel que $u \times a \equiv 1\ [26]$.

2. On considère l'algorithme suivant :

Variables	a, u et r sont des nombres (a est naturel et premier avec 26)

Traitement	Lire a
	u prend la valeur 0
	r prend la valeur 0
	Tant que $r \neq 1$
	  u prend la valeur $u + 1$
	  r prend la valeur du reste de la division euclidienne de $u \times a$ par 26
	Fin du Tant que

Sortie	Afficher u

On entre la valeur $a = 21$ dans cet algorithme.

a. Reproduire sur la copie et compléter le tableau suivant, jusqu'à l'arrêt de l'algorithme.

u	0	1	2	…
r	0	21	…	…

b. En déduire que $5 \times 21 \equiv 1\ [26]$.

3. On note I la matrice $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

a. Calculer la matrice $12A - A^2$.
b. En déduire la matrice B telle que $BA = 21I$.
c. Démontrer que si $AX = Y$ alors $21X = BY$.

Partie C – Déchiffrement

On veut déchiffrer le mot VLUP.
On note $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ la matrice associée, selon le tableau de correspondance, à un bloc de deux lettres avant chiffrement, et $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ la matrice définie par l'égalité $Y = AX$.
Si r_1 et r_2 sont les restes respectifs de y_1 et y_2 dans la division euclidienne par 26, le bloc de deux lettres après chiffrement est associé à la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$.

1. Démontrer que $\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases}$

2. En utilisant la question B.2., établir que :
$$\begin{cases} x_1 \equiv 9r_1 + 16r_2\ [26] \\ x_2 \equiv 17r_1 + 25r_2\ [26] \end{cases}$$

3. Déchiffrer le mot VLUP, associé aux matrices $\begin{pmatrix} 21 \\ 11 \end{pmatrix}$ et $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

38 *(2016, métropole).* Le plan est muni d'un repère $(O; \vec{\imath}, \vec{\jmath})$

1. Exemple. Soit Δ_1 la droite d'équation $y = \frac{5}{4}x - \frac{2}{3}$.

a. Montrer que si $(x; y)$ est un couple d'entiers relatifs alors l'entier $15x - 12y$ est divisible par 3.
b. Existe-il au moins un point de la droite Δ_1 dont les coordonnées sont deux entiers relatifs ? Justifier.

Généralisation – On considère désormais une droite Δ d'équation $(E) : y = \frac{m}{n}x - \frac{p}{q}$ où m, n, p et q sont des entiers relatifs non nuls tels que
$$\text{pgcd}(m, n) = \text{pgcd}(p, q) = 1.$$
Ainsi, les coefficients de l'équation (E) sont des fractions irréductibles et on dit que Δ est une droite rationnelle.
Le but de l'exercice est de déterminer une condition nécessaire et suffisante sur m, n, p et q pour qu'une droite rationnelle Δ comporte au moins un point dont les coordonnées sont deux entiers relatifs.

2. On suppose ici que la droite Δ comporte un point de coordonnées $(x_0; y_0)$ où x_0 et y_0 sont des entiers relatifs.

a. En remarquant que le nombre $ny_0 - mx_0$ est un entier relatif, démontrer que q divise le produit np.
b. En déduire que q divise n.

3. Réciproquement, on suppose que q divise n.

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

4. Soit Δ la droite d'équation $y = \frac{3}{8}x - \frac{7}{4}$. Cette droite possède-t-elle un point dont les coordonnées sont des entiers relatifs ? Justifier.

5. On donne l'algorithme suivant.

Variables : M, N, P, Q : entiers relatifs non nuls, tels que $\text{pgcd}(M, N) = \text{pgcd}(P, Q) = 1$
X : entier naturel
Entrées : Saisir les valeurs de M, N, P, Q
Traitement : Si Q divise N alors
  X prend la valeur 0
  Tant que $\frac{M}{N}X - \frac{P}{Q}$ n'est pas un entier et $-\frac{M}{N} - \frac{P}{Q}$ n'est pas un entier faire
    X prend la valeur $X + 1$
  Fin tant que
  Si $\frac{M}{N}X - \frac{P}{Q}$ est entier alors
    Afficher X, $\frac{M}{N}X - \frac{P}{Q}$
  Sinon
    Afficher $-X$, $-\frac{M}{N}X - \frac{P}{Q}$
  Fin Si
Sinon
  Afficher « Pas de solutions »
Fin Si

a. Justifier que cet algorithme se termine pour toute entrée de M, N, P, Q, entiers relatifs non nuls tels que $\text{pgcd}(M, N) = \text{pgcd}(P, Q) = 1$.
b. Que permet-il d'obtenir ?

39 *(Les inversibles modulo n).*

Partie A – Inverse modulo n

Soit $n \geq 2$ un entier. On dit qu'un entier a **est inversible modulo n** s'il existe un entier b tel que $ab \equiv 1\ [n]$.

1. En utilisant le théorème de Bezout, montrer que a est inversible modulo n si et seulement si a et n sont premiers entre eux.

On note $U(n)$ l'ensemble des entiers compris entre 1 et n inversibles modulo n.

2. Déterminer $U(5)$ et $U(9)$.

3. Soit $a \in U(n)$ et b et c deux entiers tels que
$$ab \equiv 1\ [n] \text{ et } ac \equiv 1\ [n].$$
Montrer que $b - c$ est un multiple de n et en déduire que pour tout $a \in U(n)$, il existe un unique $b \in U(n)$ tel que $ab \equiv 1\ [n]$.
L'entier b est appelé **inverse de a modulo n** et sera noté a^{-1}.

Partie B – Théorème d'Euler

Soit $n \geq 2$ un entier. On note $\varphi(n)$ le nombre d'éléments de $U(n)$, autrement dit, le nombre d'entiers k premiers avec n vérifiant $1 \leq k \leq n$.

Nous allons montrer que pour tout $a \in U(n)$, on a
$$a^{\varphi(n)} \equiv 1\ [n].$$

1. Vérifier le théorème d'Euler pour $n = 5$ et $n = 9$.

Soit $a \in U(n)$ un entier fixé et $k \in \mathbb{N}^*$. On note r_k le reste dans la division euclidienne de ka par n et R_a l'ensemble de ces restes, c'est-à-dire
$$R_a = \{r_k ; k \in U(n)\}.$$

2. Pour $n = 9$, calculer R_2 et R_5. Que remarque-t-on ?

3. **a.** Montrer que $R_a \subset U(n)$.

b. Montrer que si k et ℓ sont deux entiers de U, alors
$$r_k = r_\ell \Rightarrow k = \ell.$$

c. En déduire que R_a possède autant d'élément que U, puis que $R_a = U(n)$.

4. Soit P le produit des éléments de $U(n) = R_a$, montrer que
$$a^{\varphi(n)} P \equiv P\ [n]$$
et en déduire le théorème grâce au théorème de Gauss.

Partie C – Ordre modulo n

1. Soit a un entier $k \in \mathbb{N}^*$ tel que $a^k \equiv 1\ [n]$. Montrer que $a \in U(n)$.

Soit $a \in U(n)$. D'après le théorème d'Euler l'ensemble
$$O(a) = \{k \in \mathbb{N}^* ; a^k \equiv 1\ [n]\}$$
n'est pas vide car $\varphi(n) \in O(a)$.

Le plus petit entier p de $O(a)$ s'appelle **ordre de a modulo n**. Nous allons montrer que $O(a)$ est l'ensemble des multiples de p. On en déduit en particulier que p divise $\varphi(n)$.

2. Soit k un multiple de p. Montrer que $k \in O(a)$.

3. Réciproquement, soit $k \in O(a)$. La division euclidienne de k par p s'écrit $k = pq + r$ avec $0 \leq r < p$. Montrer qu'alors $a^r \equiv 1\ [p]$ et conclure.

4. Donner l'ordre des éléments de $U(5)$ et $U(9)$.

40 *(Suite de Fibonacci).* Soit (F_n) la suite définie par
$$F_0 = 0,\ F_1 = 1 \text{ et } \forall n \in \mathbb{N},\ F_{n+2} = F_{n+1} + F_n.$$

1. Montrer que pour tout $n \in \mathbb{N}^*$, on a
$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$
En déduire que F_{n+1} et F_n sont premiers entre eux.

2. Montrer que pour tout $m \in \mathbb{N}^*$ et $n \in \mathbb{N}$, on a
$$F_{m+n} = F_m F_{n+1} + F_{m-1}F_n.$$
On pourra montrer par une récurrence sur $m \geq 1$:
« pour tout $n \in \mathbb{N}$, $F_{m+n} = F_m F_{n+1} + F_{m-1}F_n$ ».

3. Montrer que pour tout $n \in \mathbb{N}^*$ et $q \in \mathbb{N}$, F_n divise F_{nq}.

4. Soit m et n deux entiers non nuls vérifiant $m \geq n$. Montrer que $\text{PGCD}(F_m ; F_n) = \text{PGCD}(F_n ; F_r)$ où r est le reste de la division euclidienne de m par n.

5. Montrer pour tous entiers m et n,
$$\text{PGCD}(F_m ; F_n) = F_{\text{PGCD}(m;n)}.$$