Exercices classe PGCD , Bézout ,Gauss

Exercice 1

Les nombres de la forme $2^n - 1$ où n est un entier naturel non nul sont appelés ***nombres de Mersenne****.*

1. *On désigne par a, b et c trois entiers naturels non nuls tels que*

   $PGCD(b\ ;\ c) = 1$.

   Prouver, à l'aide du théorème de Gauss, que :

   si b divise a et c divise a alors le produit bc divise a.

2. *On considère le nombre de Mersenne $2^{33} - 1$.*

   Un élève utilise sa calculatrice et obtient les résultats ci-dessous.

$(2^{33} - 1) \div 3$	*2863311530*
$(2^{33} - 1) \div 4$	*2147483648*
$(2^{33} - 1) \div 12$	*715827882,6*

   Il affirme que 3 divise $(2^{33} - 1)$ et 4 divise $(2^{33} - 1)$ et 12 ne divise pas $(2^{33} - 1)$.

   (a) *En quoi cette affirmation contredit-elle le résultat démontré à la question* ***1.*** *?*

   (b) *Justifier que, en réalité, 4 ne divise pas $(2^{33} - 1)$.*

   (c) *En remarquant que $2 \equiv -1 \quad [3]$, montrer que, en réalité, 3 ne divise pas $2^{33} - 1$.*

   (d) *Calculer la somme $S = 1 + 2^3 + (2^3)^2 + (2^3)^3 + \cdots + (2^3)^{10}$.*

   (e) *En déduire que 7 divise $2^{33} - 1$.*

3. *On considère le nombre de Mersenne $2^7 - 1$. Est-il premier ? Justifier.*

4. *On donne l'algorithme suivant où $MOD(N,\ k)$ représente le reste de la division euclidienne de N par k.*

Variables :	*n entier naturel supérieur ou égal à 3*
	k entier naturel supérieur ou égal à 2
Initialisation :	*Demander à l'utilisateur la valeur de n.*
	Affecter à k la valeur 2.
Traitement :	*Tant que $MOD(2^n - 1,\ k) \neq 0$ et $k \leqslant \sqrt{2^n - 1}$*
	Affecter à k la valeur $k + 1$
	Fin de Tant que.
Sortie :	***Afficher*** *k.*
	Si $k > \sqrt{2^n - 1}$
	Afficher *CAS 1*
	Sinon
	Afficher *CAS 2*
	Fin de Si

(a) *Qu'affiche cet algorithme si on saisit $n = 33$? Et si on saisit $n = 7$?*

(b) *Que représente le CAS 2 pour le nombre de Mersenne étudié ? Que représente alors le nombre k affiché pour le nombre de Mersenne étudié ?*

(c) *Que représente le CAS 1 pour le nombre de Mersenne étudié ?*

Exercice 2

Partie A

Pour deux entiers naturels non nuls a et b, on note $r(a,\ b)$ le reste dans la division euclidienne de a par b.

On considère l'algorithme suivant :

Variables :	*c est un entier naturel*
	a et b sont des entiers naturels non nuls
Entrées :	*Demander a*
	Demander b
Traitement:	*Affecter à c le nombre $r(a,\ b)$*
	Tant que $c \neq 0$
	Affecter à a le nombre b
	Affecter à b la valeur de c
	Affecter à c le nombre $r(a,\ b)$
	Fin Tant que
Sortie :	*Afficher b*

1. *Faire fonctionner cet algorithme avec $a = 26$ et $b = 9$ en indiquant les valeurs de a, b et c à chaque étape.*

2. *Cet algorithme donne en sortie le PGCD des entiers naturels non nuls a et b.*

   Le modifier pour qu'il indique si deux entiers naturels non nuls a et b sont premiers entre eux ou non.

Partie B

À chaque lettre de l'alphabet on associe grâce au tableau ci-dessous un nombre entier compris entre 0 et 25.

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*

On définit un procédé de codage de la façon suivante :

Étape 1 : *on choisit deux entiers naturels p et q compris entre 0 et 25.*

Étape 2 : *à la lettre que l'on veut coder, on associe l'entier x correspondant dans le tableau ci-dessus.*

Étape 3 : *on calcule l'entier x' défini par les relations*

$$x' \equiv px + q \quad [26] \quad et \quad 0 \leqslant x' \leqslant 25.$$

Étape 4 : *à l'entier x', on associe la lettre correspondante dans le tableau.*

1. *Dans cette question, on choisit $p = 9$ et $q = 2$.*
   (a) *Démontrer que la lettre V est codée par la lettre J.*
   (b) *Citer le théorème qui permet d'affirmer l'existence de deux entiers relatifs u et v tels que $9u + 26v = 1$. Donner sans justifier un couple $(u,\ v)$ qui convient.*
   (c) *Démontrer que $x' \equiv 9x + 2 \quad [26]$ équivaut à $x \equiv 3x' + 20 \quad [26]$.*
   (d) *Décoder la lettre R.*
2. *Dans cette question, on choisit $q = 2$ et p est inconnu. On sait que J est codé par D.*
   Déterminer la valeur de p (on admettra que p est unique).
3. *Dans cette question, on choisit $p = 13$ et $q = 2$. Coder les lettres B et D. Que peut-on dire de ce codage ?*

Exercice 3

On considère l'algorithme suivant, où A et B sont des entiers naturels tels que $A < B$:

Entrées :	*A et B entiers naturels tels que $A < B$*
Variables :	*D est un entier* *Les variables d'entrées A et B*
Traitement :	
	Affecter à D la valeur de $B - A$
	Tant que $D > 0$ *B prend la valeur de A* *A prend la valeur de D* *Si $B > A$ Alors* *D prend la valeur de $B - A$* *Sinon* *D prend la valeur de $A - B$* *Fin Si* *Fin Tant que*
Sortie :	*Afficher A*

1. *On entre $A = 12$ et $B = 14$.*
   Déterminer la valeur affichée par l'algorithme.
2. *Cet algorithme calcule la valeur du PGCD des nombres A et B.*
   En entrant $A = 221$ et $B = 331$, l'algorithme affiche la valeur 1.
   (a) *Justifier qu'il existe des couples $(x\ ;\ y)$ d'entiers relatifs solutions de l'équation*

$$(E) \qquad 221x - 331y = 1.$$

(b) *Vérifier que le couple* $(3\ ;\ 2)$ *est une solution de l'équation (E).*
En déduire l'ensemble des couples $(x\ ;\ y)$ *d'entiers relatifs solutions de l'équation (E).*

3. *On considère les suites d'entiers naturels* (u_n) *et* (v_n) *définies pour tout entier naturel* n *par*

$$u_n = 2 + 221n \quad et \quad \begin{cases} v_0 &= 3 \\ v_{n+1} &= v_n + 331 \end{cases}$$

(a) *Exprimer* v_n *en fonction de l'entier naturel* n.

(b) *Déterminer tous les couples d'entiers naturels* $(p\ ;\ q)$ *tels que* $u_p = v_q, \quad 0 \leqslant p \leqslant 500 \quad et \quad 0 \leqslant q \leqslant 500.$

Exercice 4

Partie A Inverse de 23 modulo 26

On considère l'équation

$$(E)\ :\quad 23x - 26y = 1,$$

où x *et* y *désignent deux entiers relatifs.*

1. *Vérifier que le couple* $(-9\ ;\ -8)$ *est solution de l'équation* (E).

2. *Résoudre alors l'équation* (E).

3. *En déduire un entier* a *tel que* $0 \leqslant a \leqslant 25$ *et* $23a \equiv 1 \pmod{26}$.

Partie B Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

Étape 1 *Chaque lettre du mot est remplacée par un entier en utilisant 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 obtient un couple d'entiers $(x_1\ ;\ x_2)$ *où* x_1 *correspond à la première lettre du mot et* x_2 *correspond à la deuxième lettre du mot.*

Étape 2 $(x_1\ ;\ x_2)$ *est transformé en* $(y_1\ ;\ y_2)$ *tel que :*

$$(S_1)\ \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \quad avec\ 0 \leqslant y_1 \leqslant 25\ et\ 0 \leqslant y_2 \leqslant 25.$$

Étape 3 $(y_1\ ;\ y_2)$ *est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.*

Exemple : $\underbrace{TE}_{\text{mot en clair}} \overset{\text{étape1}}{\Longrightarrow} (19, 4) \overset{\text{étape 2}}{\Longrightarrow} (13, 19) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{NT}_{\text{mot codé}}$

1. *Coder le mot ST.*

2. *On veut maintenant déterminer la procédure de décodage:*

(a) *Montrer que tout couple* $(x_1\ ;\ x_2)$ *vérifiant les équations du système* (S_1)*, vérifie les équations du système :*

$$(S_2)\ \begin{cases} 23x_1 & \equiv & 4y_1 + 23y_2 & (\text{mod } 26) \\ 23x_2 & \equiv & 19y_1 + 11y_2 & (\text{mod } 26) \end{cases}$$

(b) *À l'aide de la partie B, montrer que tout couple* $(x_1\ ;\ x_2)$ *vérifiant les équations du système* (S_2)*, vérifie les équations du système*

$$(S_3)\ \begin{cases} x_1 & \equiv & 16y_1 + y_2 & (\text{mod } 26) \\ x_2 & \equiv & 11y_1 + 5y_2 & (\text{mod } 26) \end{cases}$$

(c) *Montrer que tout couple* $(x_1\ ;\ x_2)$ *vérifiant les équations du système* (S_3)*, vérifie les équations du système* (S_1)

(d) *Décoder le mot* ***YJ****.*

Exercice 5

Partie A

On considère l'équation (E) : $25x - 108y = 1$ *où* x *et* y *sont des entiers relatifs.*

1. *Vérifier que le couple* $(13\ ;\ 3)$ *est solution de cette équation.*

2. *Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).*

Partie B

Dans cette partie, a désigne un entier naturel et les nombres c et g sont des entiers naturels vérifiant la relation $25g - 108c = 1$.

On rappelle le petit théorème de Fermat :

Si p est un nombre premier et a un entier non divisible par p, alors a^{p-1} *est congru à 1 modulo p que l'on note* $a^{p-1} \equiv 1\ [p]$.

1. *Soit* x *un entier naturel. Démontrer que si* $x \equiv a\ [7]$ *et* $x \equiv a\ [19]$*, alors* $x \equiv a\ [133]$.

2. (a) *On suppose que a n'est pas un multiple de 7.*
   Démontrer que $a^6 \equiv 1\ [7]$ *puis que* $a^{108} \equiv 1\ [7]$*. En déduire que* $(a^{25})^g \equiv a\ [7]$.

   (b) *On suppose que a est un multiple de 7. Démontrer que* $(a^{25})^g \equiv a\ [7]$.

   (c) *On admet que pour tout entier naturel a,* $(a^{25})^g \equiv a\ [19]$.
   Démontrer que $(a^{25})^g \equiv a\ [133]$.

Partie C

On note A l'ensemble des entiers naturels a tels que : $1 \leqslant a \leqslant 26$.

Un message, constitué d'entiers appartenant à A, est codé puis décodé. La phase de codage consiste à associer, à chaque entier a de A, l'entier r tel que $a^{25} \equiv r\ [133]$ *avec* $0 \leqslant r < 133$.

La phase de décodage consiste à associer à r , l'entier r_1 *tel que* $r^{13} \equiv r_1\ [133]$ *avec* $0 \leqslant r_1 < 133$.

1. *Justifier que* $r_1 \equiv a$ [133].
2. *Un message codé conduit à la suite des deux entiers suivants :* 128 59.
   Décoder ce message.

Exercice 6

On se propose de déterminer l'ensemble $\mathcal{S}$ *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* $\mathcal{S}$.
   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* $\mathcal{S}$.
   (c) *Donner un exemple d'entier* n_0 *appartenant à* $\mathcal{S}$.
2. *Caractérisation des éléments de* $\mathcal{S}$.
   (a) *Soit* n *un entier relatif appartenant à* $\mathcal{S}$. *Démontrer que* $n - n_0 \equiv 0 \quad [85]$.
   (b) *En déduire qu'un entier relatif* n *appartient à* $\mathcal{S}$ *si et seulement si il 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 7

1. *On considère l'équation (E) :* $11x - 7y = 5$, *où* x *et* y *sont des entiers relatifs.*
   (a) *Justifier, en énonçant un théorème, 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* $(O; \vec{i}; \vec{j})$ *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* $0 \leqslant x \leqslant 50$ *et* $0 \leqslant y \leqslant 50$.
   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* $x^2 \equiv 2y^2$ *(mod 5).*
   (b) *Soient* x *et* y *des entiers relatifs. Recopier et compléter les deux tableaux suivants:*

Modulo 5, x est congru à	*0*	*1*	*2*	*3*	*4*
Modulo 5, x^2 est congru à					

Modulo 5, y est congru à	*0*	*1*	*2*	*3*	*4*
Modulo 5, $2y^2$ est congru à					

Quelles sont les valeurs possibles du reste de la division euclidienne de x^2 et de $2y^2$ par 5 ?

(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) ?*

Exercice 8

On rappelle la propriété connue sous le nom de petit théorème de Fermat :

Si p est un nombre premier et q un entier naturel premier avec p, alors $q^{p-1} \equiv 1 \pmod{p}$.

On considère la suite (u_n) définie pour tout entier naturel n non nul par :

$$u_n = 2^n + 3^n + 6^n - 1.$$

1. *Calculer les six premiers termes de la suite.*
2. *Montrer que, pour tout entier naturel n non nul, u_n est pair.*
3. *Montrer que, pour tout entier naturel n pair non nul, u_n est divisible par 4.*

   On note (E) l'ensemble des nombres premiers qui divisent au moins un terme de la suite (u_n).
4. *Les entiers 2, 3, 5 et 7 appartiennent-ils à l'ensemble (E) ?*
5. *Soit p un nombre premier strictement supérieur à 3.*

   (a) *Montrer que : $6 \times 2^{p-2} \equiv 3 \pmod{p}$ et $6 \times 3^{p-2} \equiv 2 \pmod{p}$.*

   (b) *En déduire que $6u_{p-2} \equiv 0 \pmod{p}$.*

   (c) *Le nombre p appartient-il à l'ensemble (E) ?*

Exercice 9

Pour tout entier naturel n supérieur ou égal à 2, on pose $A(n) = n^4 + 1$. L'objet de l'exercice est l'étude des diviseurs premiers de $A(n)$.

1. *Quelques résultats*

   (a) *Étudier la parité de l'entier $A(n)$.*

   (b) *Montrer que, quel que soit l'entier n, $A(n)$ n'est pas un multiple de 3.*

(c) *Montrer que tout entier d diviseur de $A(n)$ est premier avec n.*

(d) *Montrer que, pour tout entier d diviseur de $A(n)$: $n^8 \equiv 1 \mod d$.*

2. *Recherche de critères*

Soit d un diviseur de $A(n)$. On note s le plus petit des entiers naturels non nuls k tels que $n^k \equiv 1 \mod d$.

(a) *Soit k un tel entier. En utilisant la division euclidienne de k par s, montrer que s divise k.*

(b) *En déduire que s est un diviseur de 8.*

(c) *Montrer que si, de plus, d est premier, alors s est un diviseur de $d-1$. On pourra utiliser le petit théorème de Fermat.*

3. *Recherche des diviseurs premiers de $A(n)$ dans le cas où n est un entier pair.*

Soit p un diviseur premier de $A(n)$. En examinant successivement les cas $s = 1$, $s = 2$ puis $s = 4$, conclure que p est congru à 1 modulo 8.

4. Dans cette question toute trace de recherche, même incomplète, sera prise en compte dans l'évaluation.

Appliquer ce qui précède à la recherche des diviseurs premiers de $A(12)$.

Indication : *la liste des nombres premiers congrus à 1 modulo 8 débute par 17, 41, 73, 89, 97, 113, 137, ...*

Exercice 10

1. *Montrer que, pour tout entier naturel non nul k et pour tout entier naturel x :*

$$(x-1)\left(1+x+x^2+\cdots+x^{k-1}\right) = x^k - 1.$$

Dans toute la suite de l'exercice, on considère un nombre entier a supérieur ou égal à 2.

2. (a) *Soit n un entier naturel non nul et d un diviseur positif de n : $n = dk$.*
Montrer que $a^d - 1$ est un diviseur de $a^n - 1$.

(b) *Déduire de la question précédente que $2^{2004} - 1$ est divisible par 7, par 63 puis par 9.*

3. *Soient m et n deux entiers naturels non nuls et d leur pgcd.*

(a) *On définit m' et n' par $m = dm'$ et $n = dn'$. En appliquant le théorème de Bezout à m' et n', montrer qu'il existe des entiers relatifs u et v tels que : $mu - nv = d$.*

(b) *On suppose u et v strictement positifs.*
Montrer que : $(a^{mu} - 1) - (a^{nv} - 1)\, a^d = a^d - 1$.
Montrer ensuite que $a^d - 1$ est le pgcd de $a^{mu} - 1$ et de $a^{nv} - 1$.

(c) *Calculer, en utilisant le résultat précédent, le pgcd de $2^{63} - 1$ et de $2^{60} - 1$.*

Exercice 11

Dans cet exercice, a et b désignent des entiers strictement positifs.

1. (a) *Démontrer que s'il existe deux entiers relatifs u et v tels que $au + bv = 1$ alors les nombres a et b sont premiers entre eux.*
   (b) *En déduire que si $(a^2 + ab - b^2)^2 = 1$, alors a et b sont premiers entre eux.*
2. *On se propose de déterminer les couples d'entiers strictement positifs $(a\ ;\ b)$ tels que $(a^2 + ab - b^2)^2 = 1$. Un tel couple sera appelé solution.*
   (a) *Déterminer a lorsque $a = b$.*
   (b) *Vérifier que (1 ; 1), (2 ; 3) et (5 ; 8) sont trois solutions particulières.*
   (c) *Montrer que si $a < b$, alors $a^2 - b^2 < 0$.*
3. (a) *Montrer que si $(x\ ;\ y)$ est une solution différente de (1 ; 1) alors $(y - x\ ;\ x)$ et $(y\ ;\ y + x)$ sont aussi des solutions.*
   (b) *Déduire de **2. b.** trois nouvelles solutions.*
4. *On considère la suite de nombres entiers strictement positifs $(a_n)_n$ définie par $a_0 = a_1 = 1$ et pour tout entier $n, n \geqslant 0,\ a_{n+2} = a_{n+1} + a_n$.*

   Démontrer que pour tout entier $n \geqslant 0,\ (a_n\ ;\ a_{n+1})$ est solution.

   En déduire que les nombres a_n et a_{n+1} sont premiers entre eux.

Exercice 12

Dans cet exercice, on pourra utiliser le résultat suivant : Étant donnés deux entiers naturels a et b non nuls, si $PGCD(a\ ;\ b) = 1$ alors $PGCD(a^2\ ;\ b^2) = 1$

Une suite (S_n) est définie pour $n > 0$ par $S_n = \sum_{p=1}^{n} p^3$. On se propose de calculer, pour tout entier naturel non nul n, le plus grand commun diviseur de S_n et S_{n+1}.

1. *Démontrer que, pour tout $n > 0$, on a : $S_n = \left(\dfrac{n(n+1)}{2}\right)^2$.*
2. *Étude du cas où n est pair. Soit k l'entier naturel non nul tel que $n = 2k$.*
   (a) *Démontrer que $PGCD(S_{2k}\ ;\ S_{2k+1}) = (2k+1)^2 PGCD(k^2\ ;\ (k+1)^2)$.*
   (b) *Calculer $PGCD\ (k\ ;\ k+1)$.*
   (c) *Calculer $PGCD(S_{2k}\ ;\ S_{2k+1})$.*
3. *Étude du cas où n est impair. Soit k l'entier naturel non nul tel que $n = 2k + 1$.*
   (a) *Démontrer que les entiers $2k + 1$ et $2k + 3$ sont premiers entre eux.*
   (b) *Calculer $PGCD(S_{2k+1}\ ;\ S_{2k+2})$.*

4. *Déduire des questions précédentes qu'il existe une unique valeur de n, que l'on déterminera, pour laquelle S_n et S_{n+1} sont premiers entre eux.*

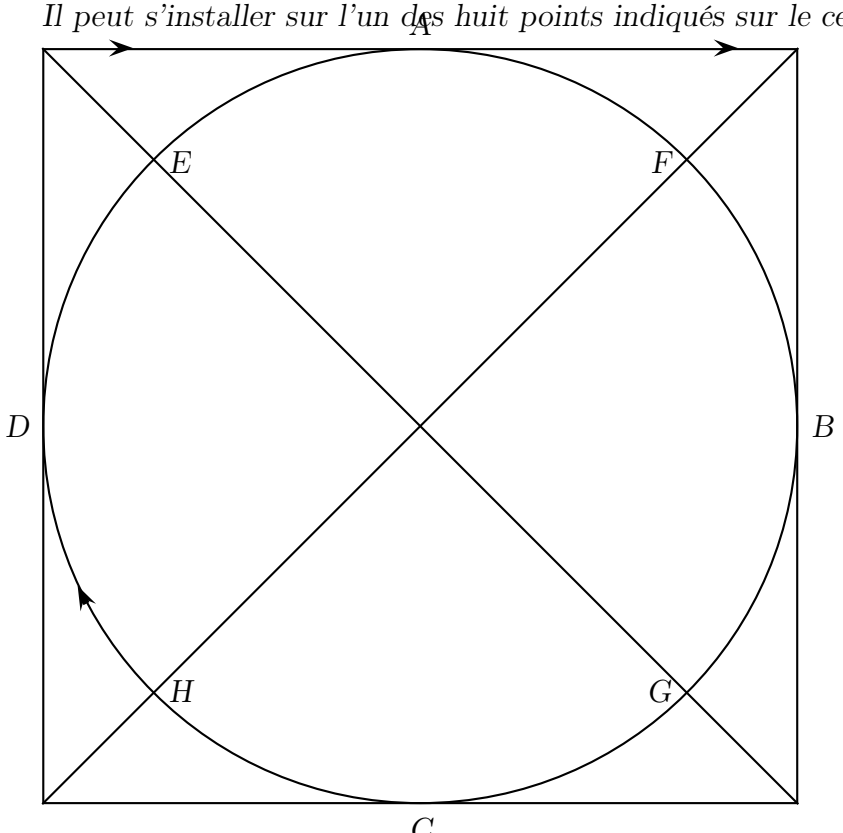
Exercice 13

1. *On considère l'équation* $(\mathcal{E})$: $17x - 24y = 9$, *où* $(x,\ y)$ *est un couple d'entiers relatifs.*

   (a) *Vérifier que le couple* $(9\ ;\ 6)$ *est solution de l'équation* $(\mathcal{E})$.

   (b) *Résoudre l'équation* $(\mathcal{E})$.

2. *Dans une fête foraine, Jean s'installe dans un un manège circulaire représenté ci-dessous. Il peut s'installer sur l'un des huit points indiqués sur le cercle.*



Le manège comporte un jeu qui consiste à attraper un pompon qui, se déplace sur un câble formant un carré dans lequel est inscrit le cercle. Le manège tourne dans le sens des aiguilles d'une montre, à vitesse constante. Il fait un tour à vitesse constante. Il fait un tour en 24 secondes. Le pompon se déplace dans le même sens à vitesse constante. Il fait un tour en 17 secondes.

Pour gagner, Jean doit attraper le pompon, et il ne peut le faire qu'aux points de contact qui sont notés A, B, C et D sur le dessin.

À l'instant $t = 0$, Jean part du point H en même temps que le pompon part du point A.

(a) *On suppose qu'à un certain instant t Jean attrape le pompon en A. Jean a déjà pu passer un certain nombre de fois en A sans y trouver le pompon. À l'instant*

t, on note y le nombre de tours effectués depuis son premier passage en A et x le nombre de tours effectués par le pompon. Montrer que $(x,\ y)$ est solution de l'équation $(\mathcal{E})$ de la question 1.

(b) *Jean a payé pour 2 minutes ; aura-t-il le temps d'attraper le pompon ?*

(c) *Montrer, qu'en fait, il n'est possible d'attraper le pompon qu'au point A.*

(d) *Jean part maintenant du point E. Aura-t-il le temps d'attraper le pompon en A avant les deux minutes ?*

Exercice 14

Les trois questions de cet exercice sont indépendantes.

1. (a) *Déterminer l'ensemble des couples $(x,\ y)$ de nombres entiers relatifs, solution de l'équation (E) :* $8x - 5y = 3$.

   (b) *Soit m un nombre entier relatif tel qu'il existe un couple $(p,\ q)$ de nombres entiers vérifiant $m = 8p + 1$ et $m = 5q + 4$.*

   Montrer que le couple $(p,\ q)$ est solution de l'équation (E) et en déduire que $m \equiv 9 \pmod{40}$.

   (c) *Déterminer le plus petit de ces nombres entiers m supérieurs à 2000.*

2. (a) *Démontrer que pour tout nombre entier naturel k on a : $2^{3k} \equiv 1 (\text{modulo } 7)$.*

   (b) *Quel est le reste dans la division euclidienne de 2^{2009} par 7 ?*

3. Dans cette question, toute trace de recherche, même incomplète, ou d'initiative, même non fructueuse, sera prise en compte dans l'évaluation.

   Soient a et b deux nombres entiers naturels inférieurs ou égaux à 9 avec $a \neq 0$.

   On considère le nombre $N = a \times 10^3 + b$. On rappelle qu'en base 10 ce nombre s'écrit sous la forme $N = \overline{a00b}$.

   On se propose de déterminer parmi ces nombres entiers naturels N ceux qui sont divisibles par 7.

   (a) *Vérifier que $10^3 \equiv -1 (\text{modulo } 7)$.*

   (b) *En déduire tous les nombres entiers N cherchés.*

Exercice 15

1. *On se propose, dans cette question, de déterminer tous les entiers relatifs N tels que*

$$\begin{cases} N & \equiv & 5 & (13) \\ N & \equiv & 1 & (17) \end{cases}$$

   (a) *Vérifier que 239 est solution de ce système.*

   (b) *Soit N un entier relatif solution de ce système.*

   Démontrer que N peut s'écrire sous la forme $N = 1 + 17x = 5 + 13y$ où x et y sont deux entiers relatifs vérifiant la relation $17x - 13y = 4$.

(c) *Résoudre l'équation* $17x - 13y = 4$ *où* x *et* y *sont des entiers relatifs.*

(d) *En déduire qu'il existe un entier relatif* k *tel que* $N = 18 + 221k$.

(e) *Démontrer l'équivalence entre* $N \equiv 18 \quad (221)$ *et* $\begin{cases} N & \equiv & 5 & (13) \\ N & \equiv & 1 & (17) \end{cases}$.

2. Dans cette question, toute trace de recherche, même incomplète, ou d'initiative, même infructueuse, sera prise en compte dans l'évaluation.

(a) *Existe-t-il un entier naturel* k *tel que* $10^k \equiv 1 \quad (17)$ *?*

(b) *Existe-t-il un entier naturel* l *tel que* $10^l \equiv 18 \quad (221)$ *?*

Exercice 16

Soit A l'ensemble des entiers naturels de l'intervalle $[1\ ;\ 46]$.

1. *On considère l'équation* (E) : $\quad 23x + 47y = 1$*où* x *et* y *sont des entiers relatifs.*

(a) *Donner une solution particulière* $(x_0,\ y_0)$ *de* (E).

(b) *Déterminer l'ensemble des couples* $(x,\ y)$ *solutions de* (E).

(c) *En déduire qu'il existe un unique entier* x *appartenant à* A *tel que* $23x \equiv 1 \quad (47)$.

2. *Soient* a *et* b *deux entiers relatifs.*

(a) *Montrer que si* $ab \equiv 0 \quad (47)$ *alors* $a \equiv 0 \quad (47)$ *ou* $b \equiv 0 \quad (47)$.

(b) *En déduire que si* $a^2 \equiv 1 \quad (47)$ *alors* $a \equiv 1 \quad (47)$ *ou a* $a \equiv -1 \quad (47)$.

3. (a) *Montrer que pour tout entier* p *de* A*, il existe un entier relatif* q *tel que* $p \times q \equiv 1 \quad (47)$.
Pour la suite, on admet que pour tout entier p *de* A*, il existe un unique entier, noté* $\text{inv}(p)$*, appartenant à* A *tel que* $p \times inv(p) \equiv 1 \quad (47)$.
Par exemple :
$\text{inv}(1) = 1$ *car* $1 \times 1 \equiv 1 \quad (47)$, $\text{inv}(2) = 24$ *car* $2 \times 24 \equiv 1 \quad (47)$,
$\text{inv}(3) = 16$ *car* $3 \times 16 \equiv 1 \quad (47)$.

(b) *Quels sont les entiers* p *de* A *qui vérifient* $p = \text{inv}(p)$ *?*

(c) *Montrer que* $46! \equiv -1 \quad (47)$.

Exercice 17

1. (a) *Déterminer le reste dans la division euclidienne de 2009 par 11.*

(b) *Déterminer le reste dans la division euclidienne de* 2^{10} *par 11.*

(c) *Déterminer le reste dans la division euclidienne de* $2^{2009} + 2009$ *par 11.*

2. *On désigne par* p *un nombre entier naturel. On considère pour tout entier naturel non nul* n *le nombre* $A_n = 2^n + p$*. On note* d_n *le PGCD de* A_n *et* A_{n+1}.

(a) *Montrer que d_n divise 2^n.*

(b) *Déterminer la parité de A_n en fonction de celle de p. Justifier.*

(c) *Dans cette question, toute trace de recherche, même incomplète, ou d'initiative même non fructueuse, sera prise en compte dans l'évaluation. Déterminer la parité de d_n en fonction de celle de p. En déduire le PGCD de $2^{2009}+2009$ et $2^{2010}+2009$.*

Exercice 18

Les questions 1 et 2 sont indépendantes. Soit n un entier naturel non nul.

1. *On considère l'équation notée (E) : $3x+7y=10^{2n}$ où x et y sont des entiers relatifs.*

   (a) *Déterminer un couple $(u\ ;\ v)$ d'entiers relatifs tels que $3u+7v=1$.*
   En déduire une solution particulière $(x_0\ ;\ y_0)$ de l'équation (E).

   (b) *Déterminer l'ensemble des couples d'entiers relatifs $(x\ ;\ y)$ solutions de (E).*

2. *On considère l'équation notée (G) : $3x^2+7y^2=10^{2n}$ où x et y sont des entiers relatifs.*

   (a) *Montrer que $100\equiv 2$ (modulo 7). Démontrer que si $(x\ ;\ y)$ est solution de (G) alors $3x^2\equiv 2^n$ (modulo 7).*

   (b) *Reproduire et compléter le tableau suivant :*

Reste de la division euclidienne de x par 7	*0*	*1*	*2*	*3*	*4*	*5*	*6*
Reste de la division euclidienne de $3x^2$ par 7.							

   (c) *Démontrer que 2^n est congru à 1, 2 ou 4 modulo 7. En déduire que l'équation (G) n'admet pas de solution.*

Exercice 19

On se propose d'étudier des couples $(a,\ b)$ d'entiers strictement positifs, tels que : $a^2=b^3$

Soit $(a,\ b)$ un tel couple et $d=PGCD(a,\ b)$. On note u et v les entiers tels que $a=du$ et $b=dv$.

1. *Montrer que $u^2=dv^3$.*

2. *En déduire que v divise u, puis que $v=1$.*

3. *Soit $(a,\ b)$ un couple d'entiers strictement positifs.*

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

4. Dans cette question, toute trace de recherche, même incomplète, ou d'initiative même non fructueuse. sera prise en compte dans l'évaluation.

   Montrer que si n est le carré d'un nombre entier naturel et le cube d'un autre entier, alors $n \equiv 0 \quad [7]$ ou $n \equiv 1 \quad [7]$.

Exercice 20

Les deux parties sont indépendantes

Un bit est un symbole informatique élémentaire valant soit 0, soit 1.

Partie A : ligne de transmission

Une ligne de transmission transporte des bits de données selon le modèle suivant :

- *elle transmet le bit de façon correcte avec une probabilité p ;*
- *elle transmet le bit de façon erronée (en changeant le 1 en 0 ou le 0 en 1) avec une probabilité $1 - p$.*

On assemble bout à bout plusieurs lignes de ce type, et on suppose qu'elles introduisent des erreurs de façon indépendante les unes des autres.

On étudie la transmission d'un seul bit, ayant pour valeur 1 au début de la transmission. Après avoir traversé n lignes de transmission, on note :

- *p_n la probabilité que le bit reçu ait pour valeur 1 ;*
- *q_n la probabilité que le bit reçu ait pour valeur 0.*

On a donc $p_0 = 1$ et $q_0 = 0$.

On définit les matrices suivantes :

$$A = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix} \quad X_n = \begin{pmatrix} p_n \\ q_n \end{pmatrix} \quad P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

On admet que, pour tout entier n, on a : $X_{n+1} = AX_n$ et donc, $X_n = A^n X_0$.

1. (a) *Montrer que P est inversible et déterminer P^{-1}.*

   (b) *On pose : $D = \begin{pmatrix} 1 & 0 \\ 0 & 2p-1 \end{pmatrix}$. Vérifier que : $A = PDP^{-1}$.*

   (c) *Montrer que, pour tout entier $n \geqslant 1$,*

   $$A^n = PD^nP^{-1}.$$

   (d) *En vous appuyant sur la copie d'écran d'un logiciel de calcul formel donnée ci-contre, déterminer l'expression de q_n en fonction de n.*

2. *On suppose dans cette question que p vaut $0,98$. On rappelle que le bit avant transmission a pour valeur 1. On souhaite que la probabilité que le bit reçu ait pour valeur 0 soit inférieure ou égale à $0,25$. Combien peut-on, au maximum, aligner de telles lignes de transmission ?*

1	$X0 := [[1], [0]]$	
	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	M
2	$P := [[1,\ 1],\ [1,\ -1]\ ]$	
	$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	M
3	$D := [[1,\ 0],[0, 2*p-1]]$	
	$\begin{bmatrix} 1 & 0 \\ 0 & 2*p-1 \end{bmatrix}$	M
4	$P*(D\hat{}n)*P\hat{}(-1)*X0$	
	$\begin{bmatrix} \frac{(2*p-1)^n+1}{2} \\ \frac{-(2*p-1)^n+1}{2} \end{bmatrix}$	M

Partie B : étude d'un code correcteur, le code de Hamming (7, 4)

On rappelle qu'un **bit** *est un symbole informatique élémentaire valant soit* 0*, soit* 1*.*
On considère un mot formé de 4 bits que l'on note b_1*,* b_2*,* b_3 *et* b_4*.*
Par exemple, pour le mot 1101 , on a $b_1 = 1$*,* $b_2 = 1$*,* $b_3 = 0$ *et* $b_4 = 1$*.*
On ajoute à cette liste une clé de contrôle $c_1c_2c_3$ *formée de trois bits :*

- c_1 *est le reste de la division euclidienne de* $b_2 + b_3 + b_4$ *par 2 ;*
- c_2 *est le reste de la division euclidienne de* $b_1 + b_3 + b_4$ *par 2 ;*
- c_3 *est le reste de la di vision euclidienne de* $b_1 + b_2 + b_4$ *par 2.*

On appelle alors message la suite de 7 bits formée des 4 bits du mot et des 3 bits de contrôle.

1. *Préliminaires*

   (a) *Justifier que* c_1*,* c_2 *et* c_3 *ne peuvent prendre comme valeurs que 0 ou 1.*

   (b) *Calculer la clé de contrôle associée au mot 1001.*

2. *Soit* $b_1b_2b_3b_4$ *un mot de 4 bits et* $c_1c_2c_3$ *la clé associée.*

   Démontrer que si on change la valeur de b_1 *et que l'on recalcule la clé, alors :*

   - *la valeur de* c_1 *est inchangée ;*
   - *la valeur de* c_2 *est modifiée ;*
   - *la valeur de* c_3 *est modifiée.*

3. *On suppose que, durant la transmission du message, au plus un des 7 bits a été transmis de façon erronée. À partir des quatre premiers bits du message reçu, on recalcule les 3 bits de contrôle, et on les compare avec les bits de contrôle reçus.*

   Sans justification, recopier et compléter le tableau ci-dessous. La lettre F *signifie que le bit de contrôle reçu ne correspond pas au bit de contrôle calculé, et* J *que ces deux bits sont égaux.*

Bit erroné / *Bit de contrôle calculé*	b_1	b_2	b_3	b_4	c_1	c_2	c_3	*Aucun*
c_1	J							
c_2	F							
c_3	F							

4. *Justifier rapidement, en vous appuyant sur le tableau, que si un seul bit reçu est erroné, on peut dans tous les cas déterminer lequel, et corriger l'erreur.*

5. *Voici deux messages de 7 bits :*

$$A = 0100010 \quad et \quad B = 1101001.$$

On admet que chacun d'eux comporte au plus une erreur de transmission.

Dire s'ils comportent une erreur, et la corriger le cas échéant.