Les coefficients de Bézout

Soit a et b deux entiers naturels non nuls tels que $d = PGCD(a;b)$.
Il **existe toujours** deux entiers relatifs u et v tels que $a \times u + b \times v = d$.

Les deux nombres u et v sont appelés les **coefficients de Bézout**. Ce couple de nombre **n'est pas unique**. C'est en réécrivant les différentes étapes de l'algorithme d'Euclide que l'on peut déterminer ce couple de nombres.

Application directe

On considère $a = 145$ et $b = 55$. Ecrire l'algorithme d'Euclide pour déterminer $d = PGCD(a;b)$. En partant de la dernière égalité où le reste est non nul et en exprimant celui-ci successivement en fonction des restes précédents, déterminer un couple d'entiers relatifs $(u;v)$ tels que $a \times u + b \times v = d$.

On considère $a = 257$ et $b = 45$. Ecrire l'algorithme d'Euclide pour déterminer $d = PGCD(a;b)$. En partant de la dernière égalité où le reste est non nul et en exprimant celui-ci successivement en fonction des restes précédents, déterminer un couple d'entiers relatifs $(u;v)$ tels que $a \times u + b \times v = d$.

On considère $a = 1050$ et $b = 735$. Ecrire l'algorithme d'Euclide pour déterminer $d = PGCD(a;b)$. En partant de la dernière égalité où le reste est non nul et en exprimant celui-ci successivement en fonction des restes précédents, déterminer un couple d'entiers relatifs $(u;v)$ tels que $a \times u + b \times v = d$.

Théorème de Bézout

Soit a et b deux entiers naturels non nuls. a et b sont **premiers entre eux** si et seulement si il existe **deux entiers relatifs** u et v tels que $\boxed{a \times u + b \times v = 1}$.

Théorème de Gauss

Soit a, b et c trois entiers naturels non nuls.
Si a divise le produit $b \times c$ et si a est premier avec b alors a divise c.

Equation diophantienne

Une équation diophantienne est une équation dont tous les **coefficients** sont **entiers** et dont les **solutions** recherchées sont **entières** elles aussi.

Par exemple, les équations du type $ax + by = c$ avec a, b, c, x et y entiers. Les Théorèmes de Bézout et de Gauss sont **à la base** du procédé de résolution des **équations diophantiennes**.

Problème d'Euler

Un jour, dans une auberge, s'arrêtent plusieurs diligences. Des hommes, mais aussi des femmes, en moindre nombre, mais tout autant affamées s'attablent. Il est convenu à l'issue du repas que les hommes paieront chacun 19 sous et les femmes 13 sous chacune. L'aubergiste récolte ainsi exactement 1000 sous. Combien d'hommes et de femmes sont descendus ce soir-là à l'auberge ?

Réservation

En montagne, un randonneur a effectué des réservations dans deux types d'hébergements : l'hébergement A et l'hébergement B. Une nuit en hébergement A coute 24 euros tandis qu'une nuit en hébergement B coute 45 euros. Il se rappelle que le cout total de sa réservation a été de 438 euros et qu'il n'a pas passé plus de 13 nuits dans l'hébergement A. Sauriez-vous l'aider à retrouver le nombre exact de nuits passées dans l'hébergement A et le nombre exact de nuits passées dans l'hébergement B ?

Sauriez-vous compléter l'algorithme proposé ci-dessous pour déterminer les mêmes résultats ?

Entrée : x et y sont des nombres
Traitement : Pour x variant de 0 … (1)
Pour y variant de 0 … (2)
Si … (3)
Afficher x et y
Fin Si
Fin Pour
Fin Pour
Fin traitement

Application directe

Déterminer tous les couples d'entiers relatifs $(x;y)$ solutions de l'équation $\boxed{7x-11y=5}$

Déterminer tous les couples d'entiers relatifs $(x;y)$ solutions de l'équation $\boxed{8x-5y=7}$

Déterminer tous les couples d'entiers relatifs $(x;y)$ solutions de l'équation $\boxed{37x+27y=1000}$.

Déterminer tous les couples d'entiers relatifs $(x;y)$ solutions de l'équation $\boxed{4x+18y=30}$.

Arithmétique et astronomie

Un astronome a observé le jour J_0 le corps céleste A qui apparaît périodiquement tous les 105 jours. Six jours plus tard, J_0+6, il observe le corps B, dont la période d'apparition est de 81 jours. On appelle J_1 le jour de la prochaine apparition simultanée des deux objets aux yeux de l'astronome.

1. On appelle u et v le nombre de périodes effectuées respectivement par A et par B entre J_0 et J_1. Montrer que le couple $(u;v)$ est solution de l'équation $(E) \Leftrightarrow 35x-27y=2$.

2. Déterminer un couple d'entiers relatifs solution particulière de l'équation $(F) \Leftrightarrow 35x-27y=1$. En déduire un couple d'entiers relatifs solution particulière de l'équation (E) puis déterminer toutes les solutions de (E).

3. Déterminer la solution $(u;v)$ permettant de déterminer J_1. Combien de jours s'écouleront entre J_0 et J_1 ?

A la fête foraine

Partie A

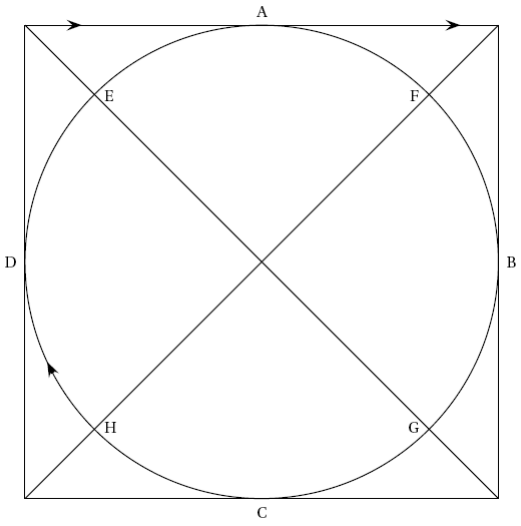
On considère l'équation $(E) 17x-24y=9$ où $(x;y)$ est un couple d'entiers relatifs.

1. Déterminer un couple d'entier relatifs $(x_0;y_0)$ solution de l'équation (E).

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

Partie B

Jean s'installe dans un manège circulaire représenté par le schéma proposé 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 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.



A l'instant $t=0$, Jean part du point H en même temps que le pompon part du point 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. On note y le nombre de tours effectués par Jean depuis son premier passage en A et x le nombre de tours effectués par le pompon.

1. Montrer que le couple $(x;y)$ est une solution de l'équation (E) de la partie A

2. Jean a payé pour deux minutes : aura-t-il le temps d'attraper le pompon ?

3. Si Jean part du point E aura-t-il le temps d'attraper le pompon en A avant deux minutes ?

Codage & décodage d'une lettre

On considère l'équation $(E)11x-26y=1$ où x et y désignent deux nombres entiers relatifs. Déterminer un couple d'entier relatifs $(x_0;y_0)$ solution de l'équation (E). Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E). Déterminer le couple d'entiers relatifs $(x_1;y_1)$ solution de (E) tel que $0\leq x_1\leq 25$.

On assimile chaque lettre de l'alphabet à un nombre entier comme l'indique 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

On code tout nombre entier x de la façon suivante : on calcule $11x+8$, puis on calcule le reste de la division euclidienne de $11x+8$ par 26 que l'on appelle y. Ainsi $y\equiv 11x+8 \pmod{26}$. A l'aide de ce procédé coder « GIONO ».

Démontrer que pour tous nombres entiers relatifs x et y on a $y\equiv 11x+8 \pmod{26}$ si et seulement si $x\equiv 19(y-8) \pmod{26}$. A l'aide de ce procédé, décoder « JUNSV ».
Proposer l'écriture en langage libre de deux algorithmes : le premier permettant de coder une lettre, le deuxième permettant de décoder une lettre à partir de son rang dans l'alphabet.

Codage et décodage d'une lettre

a et b étant deux entiers naturels donnés, on associe à tout entier n de Ω le reste de la division euclidienne de $(an+b)$ par 26. Ce reste est alors associé à la lettre correspondante. Dans toute la suite de l'exercice on prend $a=5$ et $b=2$. Coder la lettre « M ».

On se propose désormais de déterminer un procédé de décodage. Résoudre l'équation $(E)5x-26y=1$. Déterminer le couple de solution $(x;y)$ de l'équation (E) tel que $0\leq x\leq 25$. Montrer que $5x+2\equiv y \pmod{26}$ si et seulement si $x\equiv 21(y-2) \pmod{26}$. Décoder la phrase « V'CQKW FWO KCTLO ! ».

Le théorème de Bézout au service d'un problème de codage décodage

Pour coder un message, on procède de la manière suivante : à chacune des 26 lettres de l'alphabet on commence par associer un entier n de l'ensemble $\Omega = \{0;1;2;...;25\}$ selon 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

On définit un procédé de codage de la façon suivante. On choisit deux entiers naturels p et q. A la lettre que l'on veut coder, on associe l'entier x correspondant dans le tableau proposé ci-dessus. On calcule l'entier y défini par les relations $y \equiv px+q[26]$ et $0 \leq y \leq 25$. A l'entier y ainsi obtenu on associe la lettre correspondante dans le tableau.

Partie A

Dans cette partie, on choisit $p=9$ et $q=5$.

1. Coder le mot « GIONO ».
2. Quel est 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 vérifie cette égalité.
3. Démontrer que $y \equiv 9x+5[26]$ équivaut à $x \equiv 3y+11[26]$.
4. Décoder à l'aide de cette équivalence le mot « UDCZS ».

Partie B

Dans cette partie, on choisit $p=13$ et $q=2$.

5. Coder les lettres B et D.
6. Que peut-on dire de ce nouveau procédé de codage ? Est-il possible, dans ce cas-là, de définir un procédé de décodage ? La réponse à cette question sera descriptive, courte et synthétique. Elle ne se basera sur aucun calcul.

Codage, décodage et analyse fréquentielle

Une personne a mis au point le procédé de cryptage suivant : à chaque lettre de l'alphabet, on associe un entier n comme indiqué dans le tableau ci-dessous, on choisit ensuite deux entiers a et b compris entre 0 et 25, tout nombre entier n compris entre 0 et 25 est codé par le reste de la division euclidienne de $an+b$ par 26.

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

Le tableau proposé ci-dessous donne les fréquences exprimées en pourcentage des lettres utilisées dans un texte écrit en français. Elles sont issues de ce que l'on appelle une analyse fréquentielle.

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Fréquence	9,42	1,02	2,64	3,38	15,87	0,94	1,04	0,77	8,41	0,89	0,00	5,33	3,23
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Fréquence	7,14	5,13	2,86	1,06	6,46	7,90	7,26	6,24	2,15	0,00	0,30	0,24	0,32

Partie A

Un texte écrit en français et suffisamment long a été codé selon ce procédé. L'analyse fréquentielle du texte codé a montré qu'il contient 15,9 % de O et 9,4 % de E. On souhaite déterminer les nombres a et b qui ont permis le codage.

1. Quelles lettres ont été codées par les lettres O et E ?
2. Montrer que les entiers a et b sont solutions du système $\begin{cases} 4a+b \equiv 14[26] \\ b \equiv 4[26] \end{cases}$
3. Déterminer tous les couples d'entiers (a,b) ayant pu permettre le codage de ce texte.

Partie B

4. On choisit $a=22$ et $b=4$. Coder les lettres K et X. Ce codage est-il envisageable ?
5. On choisit $a=9$ et $b=4$. Déterminer un inverse de 9 modulo 26. Décoder le mot NBELA. Trouver les lettres « invariantes » par ce codage, c'est-à-dire les lettres codées par elles-mêmes.

Un autre exercice pour s'entrainer

On a reçu le message suivant : « JWPNWMRCFWMY ». On sait que le chiffrement est affine et une analyse fréquentielle nous indique que la lettre E est codée par la lettre E et que la lettre J est codée par la lettre N. Soit la fonction affine f définie par $f(x)=ax+b$ où a et b sont des entiers naturels compris entre 0 et 25.

1. Démontrer que a et b vérifient le système suivant $\begin{cases} 4a+b \equiv 4[26] \\ 9a+b \equiv 13[26] \end{cases}$.
2. Démontrer que $5a \equiv 9[26]$ puis que $a \equiv 7[26]$. En déduire que $b \equiv 2[26]$.

On considère désormais la fonction affine f définie par $f(x)=7x+2$.

3. Montrer que $7x+2 \equiv y(26)$ équivaut à $x \equiv 15y+22[26]$ puis décoder le message.
4. Ce codage admet-il une (ou des) lettre(s) invariantes. Si oui, la ou lesquelles(s) ?

Codage & décodage d'un couple de lettres

Partie A

Que permet d'obtenir cet algorithme ? Soyez précis dans votre réponse. Faire fonctionner l'algorithme pour $n=255$, $n=202$, $n=205$, $n=104$, $n=286$, $n=101$, $n=68$, $n=323$, $n=187$, $n=209$, $n=156$.

Variable :	n est une variable entière positive
Entrée :	Lire n
Traitement :	Tant que $n \geq 26$ n prend la valeur $n-26$
Sortie :	Afficher n

Partie B 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 C 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 :

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

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 : $\underbrace{\text{TE}}_{\text{mot en clair}} \overset{\text{étape 1}}{\Longrightarrow} (19,4) \overset{\text{étape 2}}{\Longrightarrow} (13,19) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{\text{NT}}_{\text{mot codé}}$

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 :

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

   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

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

   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**.

Un tour de magie

Dans cette situation, on appelle numéro du jour de naissance le rang de ce jour dans le mois et numéro du mois de naissance, le rang du mois dans l'année. Par exemple, pour une personne née le 14 mai, le numéro du jour de naissance est le 14 et le numéro du mois de naissance est le 5.

Lors d'une représentation un magicien demande aux spectateurs d'effectuer le programme de calcul suivant :

« Prenez le numéro de votre jour de naissance et multipliez-le par 12. Prenez le numéro de votre mois de naissance et multipliez-le par 37. Ajoutez les deux nombres obtenus. Je pourrai alors vous donner la date de votre anniversaire ».

1. Un spectateur annonce « 308 » : sauriez-vous déterminer sa date anniversaire ?
2. Un autre annonce « 503 » : sauriez-vous déterminer sa date anniversaire ?
3. Modifier et compléter l'algorithme ci-dessous pour qu'il affiche les réponses attendues :

```
Variables :    j et m sont des entiers naturels
Traitement :   Pour m allant de 1 à 12 faire :
                   Pour j allant de 1 à 31 faire :
                       z prend la valeur 12j + 31m
                       Afficher z
                   Fin Pour
               Fin Pour
```

Petit théorème de Fermat

Théorème

Si p est un **nombre premier** et si a est un entier supérieur ou égal à deux **non divisible** par p, Alors $a^{p-1}-1$ est **divisible** par p, c'est-à-dire $\boxed{a^{p-1}\equiv 1[p]}$.

Démonstration

Considérons les $p-1$ premiers multiples de a qui sont a, $2a$, $3a$, … et $(p-1)a$.
Considérons les restes de la division de ces multiples de a par p notés r_1, r_2, r_3 … r_{p-1}.

Ces restes sont deux à deux distincts, en effet supposons que deux restes soient identiques et menons un raisonnement par l'absurde. $r_i=r_j \Rightarrow ia\equiv ja[p]\Rightarrow (i-j)a\equiv 0[p]\Rightarrow p\,|\,(i-j)$ ce qui est impossible puisque $-p<i-j<p$.

Ainsi les restes r_1, r_2, r_3 … r_{p-1} sont tous différents et égaux à tous les restes non nuls possibles dans la division euclidienne par p, à savoir, tous les entiers compris entre 1 et $(p-1)$. Ainsi :

$$a\times 2a\times 3a\times\ldots\times(p-1)a\equiv r_1\times r_2\times r_3\times\ldots\times r_{p-1}[p]$$
$$\Leftrightarrow (p-1)!a^{p-1}\equiv 1\times 2\times 3\times\ldots\times(p-1)[p]$$
$$\Leftrightarrow (p-1)!a^{p-1}\equiv (p-1)![p]$$
$$\Leftrightarrow (p-1)!\left(a^{p-1}-1\right)\equiv 0[p]$$

Et donc comme p est premier avec tous les facteurs de $(p-1)!$ strictement inférieurs à p, le théorème de Gauss permet de dire que

$$p\,|\,a^{p-1}-1 \text{ et donc } a^{p-1}-1\equiv 0[p]$$

Conséquence

Si p est un **nombre premier** et si a est un entier naturel supérieur ou égal à deux,
Alors a^p-a est **divisible** par p, c'est-à-dire $\boxed{a^p\equiv a[p]}$.

Démonstration

Par disjonction de cas, si p ne divise pas a, l'égalité est directement issue du petit théorème de Fermat en multipliant les membres de gauche et de droite par a. Dans le cas contraire, c'est-à-dire si p divise a, les deux membres sont congrus à 0 modulo p et l'égalité reste vraie.

Exercices d'application directe

- Montrer que pour tout n, les nombres $3^{6n}-1$ sont divisibles par 7.
- Montrer que pour tout n, les nombres n^5-n sont divisibles par 5.
- Quels sont les restes dans la division par 41 des nombres 4^{20}, 25^{20}, 49^{20}, 50^{41} ?
- Montrer que pour tout n, les nombres $n^{13}-n$ sont divisibles par 7 et par 13.
- Soit p un nombre premier supérieur à 2, montrer que p divise $1+2+2^2+\ldots+2^{p-2}$.
- Vérifier que 761 est un nombre premier. On considère le nombre n constitué de 760 chiffres tous égaux à 9. Après avoir calculé $n+1$, montrer que n est divisible par 761.