Algorithme d'Euclide

Théorème : Soient a, b, q et c des entiers relatifs tels que : $a=bq+c$.
 On a : $\text{pgcd}(a,b) = \text{pgcd}(b,c)$.

Idée générale :

- On va mettre en place un tableau comprenant 3 colonnes notées a, b et c.
- Sur chaque ligne, le nombre c est égal au reste euclidien de a par b. On a donc : $\text{pgcd}(a,b)=\text{pgcd}(b,c)$.
- Pour engendrer une ligne à partir d'une autre, on copie en colonnes a et b, les valeurs respectives de b et de c de la ligne précédente et on réitère le processus.

<p>Activité : On se propose de mettre en place l'algorithme d'Euclide. On cherche à déterminer le pgcd de 4095 et de 98. Initialisez le tableau comme indiqué ci-contre.</p>		A	B	C
	1	a	b	c
	2	4095	98	
	3			
	4			
	5			
<p>Inscrire les formules adaptées pour produire le tableau ci-contre. On pourra utiliser les fonctions :</p> <ul style="list-style-type: none"> • MOD(x ;y) (reste euclidien de x par y) ou • ENT(x) (partie entière de x). <p>On calculera les cellules C2 puis A3 et B3. Les autres cellules s'obtiennent par recopie.</p>		A	B	C
	1	a	b	c
	2	4095	98	77
	3	98	77	21
	4	77	21	14
	5	21	14	7
<p>On recopiera les cellules de façon à obtenir la configuration ci-contre. Le pgcd est le dernier nombre non nul de la colonne C (ici, il s'agit de 7). La recopie peut provoquer des erreurs lorsque l'un des nombres est nul.</p> <p>Modifier les nombres initiaux pour déterminer d'autres pgcd.</p>		A	B	C
	1	a	b	c
	2	4095	98	77
	3	98	77	21
	4	77	21	14
	5	21	14	7
	6	14	7	0
	7	7	0	#DIV/0!
	8	0	#DIV/0!	#DIV/0!
9	#DIV/0!	#DIV/0!	#DIV/0!	

Détermination des coefficients de Bézout

Théorème : Soient a et b 2 entiers relatifs.

Il existe des entiers relatifs u et v tels que $au+bv = \text{pgcd}(a,b)$

Activité : On se propose de déterminer les coefficients de Bézout pour 2244 et 780.
Initialisez le tableau comme indiqué ci-contre.
Ce tableau signifie que :
 $1 \times 2244 + 0 \times 780 = 2244$ et
 $0 \times 2244 + 1 \times 780 = 780$.

	A	B	C
1	u	v	resultat
2	1	0	2244
3	0	1	780
4			
5			

On cherche à poursuivre l'algorithme d'Euclide, en conservant une égalité impliquant 2244 et 780.

Dans l'algorithme d'Euclide, le terme suivant est le reste euclidien de **2244** par **780**, soit **684**.
Nous effectuons ci-dessous une combinaison linéaire des 2 premières lignes pour obtenir une égalité liant 2244, 780 et 684. On réitérera ensuite le processus jusqu'à la fin de l'algorithme d'Euclide.

ligne 1	$1 \times 2244 + 0 \times 780 = 2244$	
ligne 2	$0 \times 2244 + 1 \times 780 = 780$	<u>division euclidienne de 2244 par 780</u>

reste = **684**
quotient = q (ici, q=2)

On détermine 1 fois la ligne 1 moins q fois la ligne 2.

$$(1 - q \times 0) \times 2244 + (0 - q \times 1) \times 780 = 2244 - q \times 780$$

donc : $684 = 2244 - q \times 780$

ligne 3	$1 \times 2244 - 2 \times 780 = 684$	
---------	--------------------------------------	--

division euclidienne de 780 par 684

reste = **96**
quotient = q' (ici, q'=1)

On détermine 1 fois la ligne 2 moins q' fois la ligne 3.

$$(0 - q' \times 1) \times 2244 + (1 - q' \times (-2)) \times 780 = 780 - q' \times 684$$

donc : $96 = 780 - q' \times 684$

ligne 4	$-1 \times 2244 + 3 \times 780 = 96$	
---------	--------------------------------------	--

division euclidienne de 780 par 684

etc...

etc...

La colonne C va être complétée en y reportant la suite des restes euclidiens obtenus dans l'algorithme d'Euclide.

Poursuivre le tableau en calculant en cellule C4 le reste euclidien de 2244 par 780.

On utilisera une formule exprimée à l'aide de la fonction **ENT**.

	A	B	C
1	u	v	resultat
2	1	0	2244
3	0	1	780
4			684
5			

La cellule C4 a été obtenue à l'aide d'une combinaison linéaire de C2 et C3.

Ecrire la formule pour que la cellule B4 s'obtienne à l'aide d'une combinaison linéaire de B2 et B3 utilisant les mêmes coefficients que dans la colonne C.

	A	B	C
1	u	v	resultat
2	1	0	2244
3	0	1	780
4	1	-2	684
5			

Faire de même avec la cellule A4.

Recopier les cellules vers le bas pour obtenir le tableau ci-contre.

La nullité de certains entiers peut provoquer des erreurs. La ligne intéressante est la 6, qui indique le pgcd de 2244 et de 780 (dernier entier non nul dans la colonne C).

Elle indique que :

$$8 \times 2244 - 23 \times 780 = 12$$

Modifier les nombres initiaux et prendre 2 nombres premiers a et b pour obtenir les entiers u et v tels que $au+bv=1$.

	A	B	C
1	u	v	resultat
2	1	0	2244
3	0	1	780
4	1	-2	684
5	-1	3	96
6	8	-23	12
7	-65	187	0
8	#DIV/0!	#DIV/0!	#DIV/0!
9	#DIV/0!	#DIV/0!	#DIV/0!

POUR ALLER PLUS LOIN.

Détermination d'un inverse modulo b donc dans Z/bZ

Théorème : Soient a et b 2 entiers relatifs premiers entre eux.

Il existe un entier u tel que $au \equiv 1$ (modulo b).

(en d'autres termes, a admet un inverse dans Z/bZ).

Remarques :

- Cela résulte de l'égalité de Bézout, puisque si a et b sont premiers entre eux, il existe u et v tels que $au+bv=1$ d'où $au \equiv 1$ (modulo b).
- Ce point est très souvent utilisé dans les codages.

Activité : Cette activité utilise le tableau précédent.

On se propose de trouver l'entier u tel que :
 $1613u \equiv 1$ (modulo 2244).

A l'aide du tableau précédent, vérifiez que 2244 et 1613 sont premiers entre eux. Le tableau produit est celui qui est mentionné ci-contre.

La dernière ligne permet de déduire que :
 $-409 \times 2244 + 569 \times 1613 = 1$.

	A	B	C
1	u	v	resultat
2	1	0	2244
3	0	1	1613
4	1	-1	631
5	-2	3	351
6	3	-4	280
7	-5	7	71
8	18	-25	67
9	-23	32	4
10	386	-537	3
11	-409	569	1

On déduit de ce qui précède que :

$$569 \times 1613 \equiv 1$$
 (modulo 2244).

Vérifiez cette égalité en complétant le tableau ci-contre (on utilisera la fonction MOD).

Recommencer avec d'autres valeurs et procéder à une vérification.

	E	F
1	b	2244
2		
3	a	1613
4	u	569
5	a*u	917797
6	a*u (mod b)	1

Chiffrement affine

Remarque générale :

Dans les problèmes de codages :

- l'EXPEDITEUR écrit un message qu'il va mettre sous une forme numérique x ;
- l'EXPEDITEUR code ce message qui devient un nombre émis y ;
- le RECEPTEUR décode y pour revenir à x , à partir duquel le message est retrouvé.

Il faut trouver des moyens efficaces :

- de passer de x (message initial chiffré) à y (message codé)
- de passer de y à x .

Ici, y est obtenu par transformation affine à partir de x , lui-même obtenu par une autre transformation affine à partir de y .

Théorème : Soient a et b 2 entiers compris entre 0 et 25. On suppose que a est premier avec 26.

Il existe 2 entiers c et d tels que, pour tous entiers x et y vérifiant :

$$ax+b \equiv y \pmod{26}$$

on ait :

$$x \equiv cy+d \pmod{26}.$$

Remarque: Le choix de 26 est lié au nombre de lettres à coder. Le théorème précédent se généralise avec un entier c quelconque, premier avec a .

Exemple :

- Supposons que l'on ait :

$$19x+3 \equiv y \pmod{26}.$$

Comme :

$$19 \times 11 \equiv 1 \pmod{26}$$

on en déduit que :

$$11 \times (19x+3) \equiv 11y \pmod{26} ; x+33 \equiv 11y \pmod{26} ; x \equiv 11y-33 \pmod{26}.$$

Remarque :

- La conclusion du théorème résulte de l'égalité de Bézout, puisque, si a et 26 sont premiers entre eux, il existe u et v tels que $au+26v=1$ d'où $au \equiv 1 \pmod{26}$.
- Puisque :

$$ax+b \equiv y \pmod{26}$$

on en déduit que :

$$u(ax+b) \equiv uy \pmod{26} ; uax \equiv uy-ub \pmod{26} ; x \equiv uy-ub \pmod{26}.$$

Activité :

On se propose de coder « bonjour » à l'aide du codage défini par $19x+3$ (modulo 26).

Reproduire le tableau ci-dessous, en suivant les indications :

- la cellule D2 indique le numéro de la lettre codée (0 pour a, 1 pour b, ...);
- le contenu de cette cellule est calculé à l'aide de CODE(D1)-97
 - en effet, dans un tableur, les lettres sont codées par des nombres successifs à partir de 97 obtenus par la fonction CODE ; ainsi, CODE(« a ») = 97, CODE(« b ») = 98, CODE(« c ») = 99...);
 - en retranchant 97, on peut ainsi coder les lettres par des entiers successifs compris entre 0 et 25.
- la cellule D3 est calculée à partir des valeurs affichées dans les cellules A2 et B2 ;
- les lettres de la ligne 6 sont obtenues à l'aide de la fonction CAR ;
- ainsi, la formule de la cellule D6 est CAR(D3+97).

	A	B	C	D	E	F	G	H	I	J	
1	a	b	MESSAGE INITIAL	b	o	n	j	o	u	r	
2	19	3		x	1	14	13	9	14	20	17
3			$y = ax+b \text{ mod } 26$	22	9	16	18	9	19	14	
4											
5											
6			MESSAGE CODE	w	j	q	s	j	t	o	

On se propose ici de décoder le message en créant une table de correspondance entre :

- le numéro de la lettre codée (notée x) et
- sa valeur après codage (notée y).

Les opérations à réaliser sont les suivantes :

- remplir la colonne L (remplir les cellules L2 et L3 et les recopier jusqu'à obtenir la valeur 25) ;
- remplir la colonne M ; y est $ax+b$ (modulo 26) ;

Nous allons créer la table dans les colonnes O et P, triées selon les « y », condition nécessaire pour que l'association puisse se faire.

Les opérations à réaliser sont les suivantes :

- sélectionner L1 :M27 ;
- positionner le curseur en O1 ;
- coller avec : *Edition* > *collage spécial* > *coller valeurs* ;
- sélectionner O2 : P27 ;
- trier avec *Données* > *trier* > *trier par* « y » *croissants*.

	L	M	N	O	P
1	x	y		x	y
2	0	3		19	0
3	1	22		4	1
4	2	15		15	2
5	3	8		0	3
6	4	1		11	4
7	5	20		22	5
8	6	13		7	6
.....					
19	17	14		24	17
20	18	7		9	18
21	19	0		20	19
22	20	19		5	20
23	21	12		16	21
24	22	5		1	22
25	23	24		12	23
26	24	17		23	24
27	25	10		8	25

Compléter la feuille avec les éléments indiqués ci-dessous, à l'aide des indications suivantes :

- la cellule D10 s'obtient à l'aide de la cellule D6 exactement comme la cellule D2 à partir de D1 ;
- pour trouver « x » (valeur de la lettre initiale) à partir du « y » (valeur après codage), on utilise la fonction RECHERCHE qui va utiliser le tableau d'index en colonnes O et P pour décoder ;
- ainsi, la formule de la cellule D11 est : RECHERCHE(D10;\$P\$2:\$P\$27;\$O\$2:\$O\$27) où :
 - D10 est la valeur à décoder ;
 - \$P\$2:\$P\$27 indique la zone où chercher cette valeur ;
 - \$O\$2:\$O\$27 indique la valeur décodée associée.

	A	B	C	D	E	F	G	H	I	J	
9			décodage par une table								
10				y	22	9	16	18	9	19	14
11				x	1	14	13	9	14	20	17
12			MESSAGE DECODE	b	o	n	j	o	u	r	

On se propose maintenant de décoder le message, non plus à l'aide d'une table de correspondance mais par le calcul.

On sait que (voir ci-dessus) si $19x+3 \equiv y \pmod{26}$, alors $x \equiv 11y-33 \pmod{26}$.

Compléter la feuille de calcul afin d'obtenir la configuration ci-dessous.

	A	B	C	D	E	F	G	H	I	J	
15	c	d	décodage par calcul								
16	11	-33		y	22	9	16	18	9	19	14
17			$x = cy+d \pmod{26}$	1	14	13	9	14	20	17	
18			MESSAGE DECODE	b	o	n	j	o	u	r	

Modifier :

- le message codé ; tout doit s'actualiser automatiquement ;
- les coefficients a et b ; il est alors nécessaire de :
 - refaire la table d'index ;
 - recalculer les coefficients c et d, en utilisant le dispositif mis en place plus haut.

Remarque : on peut copier dans cette feuille et à l'endroit choisi, le tableau de la détermination de l'inverse d'un entier dans $\mathbb{Z}/a\mathbb{Z}$ (car c est l'inverse de a dans $\mathbb{Z}/26\mathbb{Z}$).

	R	S	T
1	u	v	resultat
2	1	0	26
3	0	1	19
4	1	-1	7
5	-2	3	5
6	3	-4	2
7	-8	11	1

POUR ALLER ENCORE PLUS LOIN !!

Système RSA (Rivest, Shamir, Adleman)

Remarque générale :

Dans ce système, EXPEDITEUR et RECEPTEUR codent et décotent tous deux par élévation à la puissance modulo un entier.

Plus précisément, on utilise des entiers c, d, n choisis de telle sorte que, si l'EXPEDITEUR a un message sous une forme numérique x :

- l'EXPEDITEUR code le message x en calculant $y \equiv x^c \pmod{n}$;
- le RECEPTEUR décode le message y en calculant $y^d \equiv x \pmod{n}$.

Le théorème ci-dessous spécifie le contexte précis de ce système.

Théorème : on suppose que x, y, p, q, e et d sont des entiers tels que :

- p et q sont premiers et distincts ;
- p et q ne divisent pas x ;
- e est premier avec $(p-1)(q-1)$;
- d est tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$

Sous ces conditions :

$$\begin{aligned} \text{si } & x^e \equiv y \pmod{pq} \\ \text{alors } & y^d \equiv x \pmod{pq}. \end{aligned}$$

Preuve succincte :

En effet :

$$\begin{aligned} x^{(p-1)} &\equiv 1 \pmod{p} \quad (\text{théorème de Fermat}) && \text{donc :} \\ x^{(p-1)(q-1)} &\equiv 1 \pmod{p} \end{aligned}$$

De même :

$$\begin{aligned} x^{(q-1)} &\equiv 1 \pmod{q} \quad (\text{théorème de Fermat}) && \text{d'où :} \\ x^{(p-1)(q-1)} &\equiv 1 \pmod{q} \end{aligned}$$

Comme p et q sont distincts, pq divise $x^{(p-1)(q-1)} - 1$ et

$$x^{(p-1)(q-1)} \equiv 1 \pmod{pq} \quad (\text{congruence 1})$$

Or e et d sont tels que $ed \equiv 1 \pmod{(p-1)(q-1)}$ donc

il existe u tel que $ed = 1 + u(p-1)(q-1)$.

D'où :

$$\begin{aligned} y^d &\equiv (x^e)^d \pmod{pq}. \\ y^d &\equiv x^{ed} \pmod{pq}. \\ y^d &\equiv x^{1+u(p-1)(q-1)} \pmod{pq}. \\ y^d &\equiv x \pmod{pq} \quad \text{d'après (congruence 1)}. \end{aligned}$$

Remarque :

On se place sous les hypothèses du théorème. Notons n le produit pq .

- Dans le codage RSA, le RECEPTEUR choisit p, q et e . Il calcule d . Les entiers p, q et d constituent sa clé privée.
- L'EXPEDITEUR ne dispose que de n et de e , appelées clé publique.
- Si x est un code, il peut donc calculer $x^e \equiv y \pmod{n}$.
- Le RECEPTEUR va décoder en calculant $y^d \equiv x \pmod{n}$.
- La force de ce système de codage repose sur la quasi-impossibilité de résoudre la congruence $x^e \equiv y \pmod{n}$, où x est inconnu et de pouvoir décomposer n , ce qui est le cas pour l'instant si n possède plusieurs centaines de chiffres.

<p>Remarque préalable à la mise en œuvre : Pour mettre cet algorithme en œuvre dans un tableur, il est nécessaire de calculer $x^e \pmod n$, où e et n sont des grands nombres. Il faudrait donc écrire $\text{MOD}(x^e ; n)$.</p> <p>Malheureusement, la fonction MOD ne donne pas les résultats attendus dans le cas de grands nombres. Il est donc nécessaire de programmer la fonction PUISMOD en VisualBasic, présentée ci-contre et qui utilise un algorithme d'exponentiation rapide en prenant les restes modulo au fur et à mesure.</p>	<pre> DefCur X 'pour que X soit définie avec suffisamment de précision Function Puismod(N, p, n) e= 1: X = N: c = p Do While c > 0 If c Mod 2 <> 0 Then e = e * X - Int(e * X / n) * n End If X = X * X - Int(X * X / n) * n c = Int(c / 2) Loop Puismod = e End Function </pre>
<p>Pour enregistrer la fonction, il faut :</p> <ul style="list-style-type: none"> • choisir <i>Outils > Macro > Visual Basic Editor</i> ; • choisir dans la fenêtre qui s'ouvre : <i>Insertion > Module</i> ; • écrire la fonction dans la fenêtre présente et refermer le tout. 	

<p>Activité : Mettre en place la configuration ci-contre.</p> <p>Le RECEPTEUR choisit les nombres p, q et e (e est premier avec $(p-1)(q-1)$, ce qui est le cas avec 101, lui-même premier).</p> <p>L'EXPEDITEUR ne connaît que les nombres $n=pq$ et e.</p> <p>Le RECEPTEUR calcule le nombre d sans le communiquer.</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #d3d3d3;"> <th></th> <th>A</th> <th>B</th> <th>C</th> </tr> </thead> <tbody> <tr><td>1</td><td>EXPEDITEUR</td><td></td><td></td></tr> <tr><td>2</td><td></td><td>n</td><td>e</td></tr> <tr><td>3</td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td></tr> <tr><td>5</td><td></td><td></td><td></td></tr> <tr><td>6</td><td></td><td></td><td></td></tr> <tr><td>7</td><td></td><td></td><td></td></tr> <tr><td>8</td><td>RECEPTEUR</td><td></td><td></td></tr> <tr><td>9</td><td></td><td>p</td><td>q</td></tr> <tr><td>10</td><td></td><td>73</td><td>151</td></tr> </tbody> </table>		A	B	C	1	EXPEDITEUR			2		n	e	3				4				5				6				7				8	RECEPTEUR			9		p	q	10		73	151
	A	B	C																																										
1	EXPEDITEUR																																												
2		n	e																																										
3																																													
4																																													
5																																													
6																																													
7																																													
8	RECEPTEUR																																												
9		p	q																																										
10		73	151																																										
<p>Pour calculer le nombre d, on peut recopier, à partir de la cellule A13, le dispositif mis en place pour le calcul des coefficients de Bézout.</p> <p>La cellule C14 est $(p-1)(q-1)$, la cellule C15 est e. Le dispositif donne les coefficients de Bézout. Le nombre d est 3101.</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #d3d3d3;"> <th></th> <th>A</th> <th>B</th> <th>C</th> </tr> </thead> <tbody> <tr><td>13</td><td>u</td><td>v</td><td>resultat</td></tr> <tr><td>14</td><td>1</td><td>0</td><td>10800</td></tr> <tr><td>15</td><td>0</td><td>1</td><td>101</td></tr> <tr><td>16</td><td>1</td><td>-106</td><td>94</td></tr> <tr><td>17</td><td>-1</td><td>107</td><td>7</td></tr> <tr><td>18</td><td>14</td><td>-1497</td><td>3</td></tr> <tr><td>19</td><td>-29</td><td>3101</td><td>1</td></tr> <tr><td>20</td><td>101</td><td>-10800</td><td>0</td></tr> <tr><td>21</td><td>#DIV/0!</td><td>#DIV/0!</td><td>#DIV/0!</td></tr> <tr><td>22</td><td>#DIV/0!</td><td>#DIV/0!</td><td>#DIV/0!</td></tr> </tbody> </table>		A	B	C	13	u	v	resultat	14	1	0	10800	15	0	1	101	16	1	-106	94	17	-1	107	7	18	14	-1497	3	19	-29	3101	1	20	101	-10800	0	21	#DIV/0!	#DIV/0!	#DIV/0!	22	#DIV/0!	#DIV/0!	#DIV/0!
	A	B	C																																										
13	u	v	resultat																																										
14	1	0	10800																																										
15	0	1	101																																										
16	1	-106	94																																										
17	-1	107	7																																										
18	14	-1497	3																																										
19	-29	3101	1																																										
20	101	-10800	0																																										
21	#DIV/0!	#DIV/0!	#DIV/0!																																										
22	#DIV/0!	#DIV/0!	#DIV/0!																																										