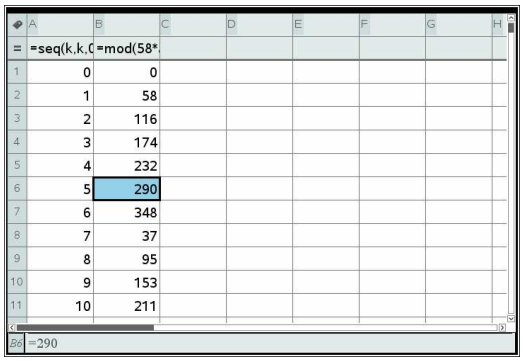
# CAPES 2015. EPREUVE 2, PB 1

*Ce problème aborde deux méthodes de codage, dont le codage affine. En cherchant un peu dans la page « épreuve sur dossier », le lecteur trouvera des sujets d'ESD (arithmétique) dans lesquels le thème du codage affine est abordé. Il est conseillé de s'y référer pour information. Je passe sur les deux premières questions qui amènent à démontrer le théorème de Bézout puis celui de Gauss.*

## Partie A. Un chiffrement monographique.

### III. Chiffrement lettre à lettre

**1.** Coder le mot GAUSS revient à coder la séquence $(6, 0, 20, 18, 18)$. On obtient $(348, 0, 53, 306, 306)$.




$a \mapsto \text{mod}(58 * a, 369)$ définit une application injective de l'ensemble $[0\,;25]$ vers l'ensemble $[0\,;369]$ que l'on est amené à tabuler.

Dans un premier temps, le décodage de $(290, 232, 248, 327, 0, 364)$ se fait en repérant les correspondances dans le tableur. On obtient $(5, 4, 17, 12, 0, 19)$, ce qui correspond au mot FERMAT.

« L'activité de classe » que l'on peut proposer se borne à tabuler l'application $a \mapsto \text{mod}(58 * a, 369)$. Elle a pour objectif de susciter la curiosité (?) et de « poser le vrai problème » :

- On peut faire quelques constatations sur ce codage : l'injectivité de l'application ainsi construite, le fait que les lettres sont codées par « paquets de 6 ou 7 lettres » .
- Le décodage du mot FERMAT se fait en repérant dans la colonne B où sont les nombres 290, 232, etc.… et en notant quels sont leurs antécédents
- Ce procédé est peu performant et fastidieux. Comment faire pour décoder plus rapidement … ? Il faudrait sinon inverser l'application $a \mapsto \text{mod}(58 * a, 369)$ au moins trouver un moyen de passer facilement des images aux antécédents.

**2.** Les entiers *n* et *e* étant premiers entre eux, il existe deux entiers relatifs *u* et *v* tels que : $nu + ev = 1$
Par conséquent : $ev \equiv 1\,(n)$. Plus généralement, quel que soit l'entier relatif $k$ : $e(v + kn) \equiv 1\,(n)$.
Il suffit de choisir $k$ de telle sorte que $kn > -v$ pour que l'entier $v + kn$ soit strictement positif. En particulier, il existe un entier $k_0$ tel que : $0 < v + k_0 n < n$ (inégalités strictes des deux côtés : puisque $nu + ev = 1$, $n$ et $v$ sont premiers entre eux et $v$ n'est pas multiple de $n$). On peut choisir pour $f$ cet entier $v + k_0 n$.

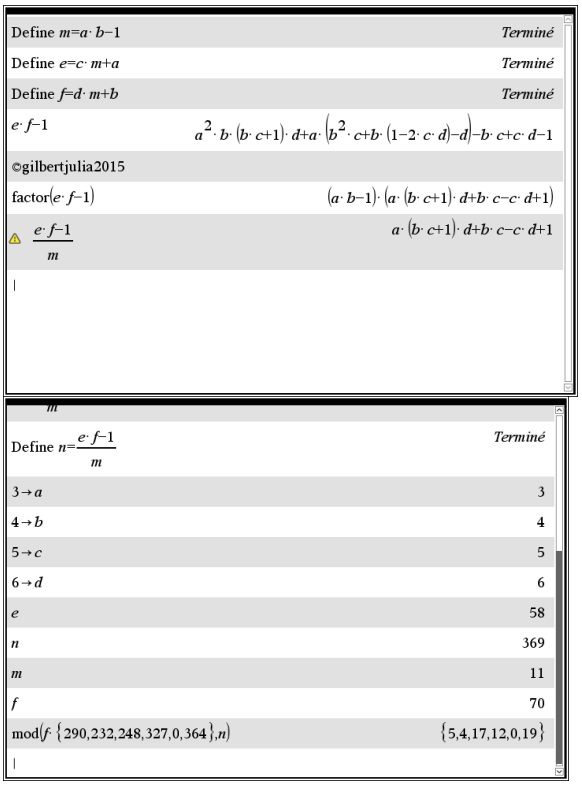
L'entier *y* est défini par : $\begin{cases} y \equiv ex\,(n) \\ 0 \le y < n \end{cases}$ *gjulia 2015*. Inversement *x* est défini par : $\begin{cases} fy \equiv x\,(n) \\ 0 \le x < n \end{cases}$ c'est-à-dire que *x* est le reste de la division euclidienne de $fy$ par *n*.
C'est en ce sens que la « connaissance de *f* permet de retrouver *y* ». Cela répond à l'interrogation émise lors de l'activité de classe « trouver un moyen de passer facilement des images aux antécédents ».

**3.** $e = c(a\,b-1)+a$ et $f = d(ab-1)+b$

L'entier $e\,f-1$ est divisible par $M$ et : $n = \dfrac{e\,f-1}{M} = a\,d(bc-1)+bc-c\,d+1$

- Puisque *a, b, c, d* sont supérieurs ou égaux à 3, $M \geq 8$, $e \geq 27$, $f \geq 27$.
- Puisque : $e\,f - M\,n = 1$, $e$ et $n$ sont premiers entre eux et de plus $e\,f \equiv 1\,(n)$

Ce procédé permet de construire une clé de codage avec une clef de décodage associée.




On retrouve la clef de codage proposée en début d'énoncé, avec comme clef de décodage : $f = 70$. Cette clef permet de décoder le mot proposé.

**4.1.** Par construction, le dernier reste non nul dans l'algorithme d'Euclide est le PGCD des deux nombres auxquels on applique l'algorithme ; puisque ici ces deux entiers sont premiers entre eux : $r_N = 1$

**4.2.** La construction des termes successifs des suites *u* et *v* s'effectue à l'aide d'une récurrence portant sur deux rangs.

Si $n = q_1 e + r_2$ est la division euclidienne de *n* par *e*, avec les notations $n = r_0$ ; $e = r_1$, on peut écrire d'une part : $r_0 = q_1 r_1 + r_2$ avec $0 \leq r_2 < r_1$ et d'autre part : $\begin{cases} r_0 = n\times 1 + e\times 0 \\ r_1 = n\times 0 + e\times 1 \\ r_2 = n\times 1 + e\times(-q_1) \end{cases}$ ce qui met en évidence les termes de rangs 0, 1 et 2 des suites *u* et *v*. L'important est que les deux premiers termes de chaque suite sont connus.

En supposant construits les termes de rangs *k* et $k-1$ de ces deux suites :

Pourvu que la division euclidienne de $r_{k-1}$ par $r_k$ ait du sens c'est-à-dire que $k \leq N$ : $r_{k+1} = r_{k-1} - r_k q_k = n(u_{k-1} - q_k u_k) + e(v_{k-1} - q_k v_k)$ et par conséquent : $u_{k+1} = u_{k-1} - q_k u_k$ ; $v_{k+1} = v_{k-1} - q_k v_k$.

En particulier : $r_N = 1 = n u_N + e v_N$. L'entier $v_N$ vérifie : $e v_N \equiv 1\,(n)$ et constitue une clef de décodage. Cependant, ce n'est pas nécessairement un entier naturel. Si on effectue la division euclidienne de $v_N$ par *n*, on obtient alors une clef de décodage entière naturelle.

Utiliser un tableur est une option pour construire les suites $u$ et $v$. Cela devrait donner les résultats ci-contre en « tirant vers le bas » comme l'indique l'énoncé. Lorsque le reste calculé est égal à zéro, le calcul du quotient devient indéfini. Le dernier reste non nul est $r_5$ et à ce rang $u_5 = -11\,;\, v_5 = 70$

| | A r | B q | C u | D v | E | F |
|---|---|---|---|---|---|---|
| = | | | | | | |
| 1 | 369 | | 1 | 0 | | |
| 2 | 58 | 6 | 0 | 1 | | |
| 3 | 21 | 2 | 1 | -6 | | |
| 4 | 16 | 1 | -2 | 13 | | |
| 5 | 5 | 3 | 3 | -19 | | |
| 6 | 1 | 5 | -11 | 70 | | |
| 7 | 0 | iPart(un... | 58 | -369 | | |

C4 =c2−b3·c3

On peut vérifier que : $369\times(-11)+58\times 70 = 1$

$369u+58v=1 \Leftrightarrow \exists k\in \mathbf{Z} \begin{cases} u=-11-58k \\ v=70+369k \end{cases}$. L'ensemble des clefs de décodage est l'ensemble des entiers $v$ ainsi déterminés qui sont des entiers naturels donc l'ensemble des entiers $v$ de la forme : $v=70+369k,\ k\in \mathbf{N}$.

## Partie B. Chiffrement de Hill.

**I.** La matrice $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si et seulement si il existe une matrice $B=\begin{pmatrix} x & z \\ y & t \end{pmatrix}$ telle que : $AB=BA=I_2$.

La recherche d'une matrice $B$ telle que $AB=I_2$ amène à la résolution de deux systèmes de 2 équations à 2 inconnues : $\begin{cases} ax+by=1 \\ cx+dy=0 \end{cases}$ ; $\begin{cases} az+bt=0 \\ cz+dt=1 \end{cases}$.

Si $ad-bc\neq 0$, chacun des deux systèmes a un unique couple de réels solution en l'occurrence : $\begin{cases} x=\dfrac{d}{ad-bc} \\ y=\dfrac{-c}{ad-bc} \end{cases}$ ; $\begin{cases} z=\dfrac{-b}{ad-bc} \\ t=\dfrac{a}{ad-bc} \end{cases}$, la matrice $\dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ étant l'inverse $A^{-1}$ de $A$.

On note que $A^{-1}=\dfrac{1}{ad-bc}\left((a+d)I_2-A\right)$, ce qui donne en multipliant par $(ad-bc)A$ :

$(ad-bc)I_2=(a+d)A-A^2$ (« équation caractéristique »)

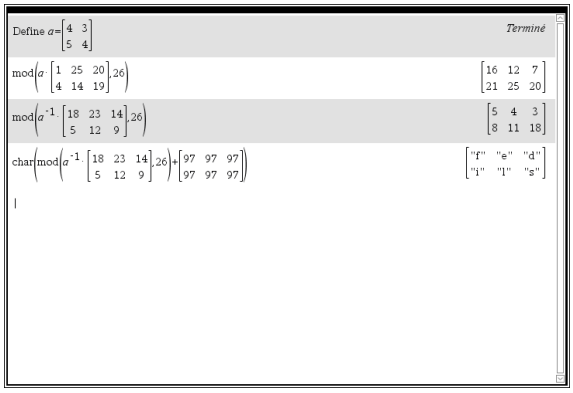
Si $ad-bc=0$, les deux systèmes ne peuvent avoir tous les deux en même temps des solutions, puisque les deux seconds membres $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ sont indépendants. Il n'existe aucune matrice $B$ telle que $AB=I_2$.

La condition $ad-bc\neq 0$ est nécessaire et suffisante pour assurer l'existence d'une matrice inverse.

**II.** Si la matrice $A$ est à coefficients dans **Z**, il est clair que la condition $|ad-bc|=1$ est suffisante pour que $A^{-1}$ ait elle aussi des coefficients dans **Z**. La notion de « déterminant d'une matrice » permet de justifier qu'elle est nécessaire car : $\det\left(A\times A^{-1}\right)=\det(A)\times\det\left(A^{-1}\right)=1$. Or, dans **Z**, l'équation $x\times y=1$ n'a pour solutions que $x=y=1$ et $x=y=-1$.

**III.** L'action de la matrice $A$ permet le codage, et l'action de $A^{-1}$ le décodage.

Pour information, selon le code ASCII, les lettres minuscules sont codées numériquement de 97 à 122. La fonction qui permet de passer d'un code numérique ASCII à la lettre correspondante est la fonction **char**. Ainsi la fonction $x\mapsto \textbf{char}(x+97)$ associe à un entier de $\{0;1;\ldots;25\}$ la lettre qui lui correspond conformément à l'énoncé.




**3.** $7u\equiv 1\,(26)$ si et seulement si il existe un entier relatif $v$ : $7u+26v=1$

Les entiers 7 et 26 sont premiers entre eux. En remarquant que $3\times 26-11\times 7=1$, on obtient que :

$7u+26v=1\Leftrightarrow 7(u+11)=26(3-v)$ puis que $7u+26v=1\Leftrightarrow(\exists k\in\textbf{Z})\begin{cases} u=26k-11 \\ v=-7k+3 \end{cases}$

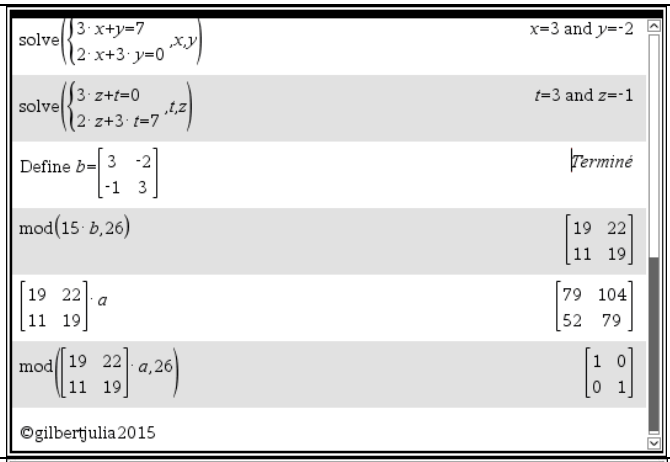
Parmi les entiers $u$ de la forme $u=26k-11$, un et un seul, en l'occurrence 15, est compris entre 0 et 25. Il vérifie $7\times 15\equiv 1\,(26)$

D'après la question de cours, $A^2 - 6A + 7I_2 = O_2$ et en conséquence : $(6I_2 - A)A = 7I_2$

La matrice $B = 6I_2 - A = \begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix}$ vérifie $BA = 7I_2$

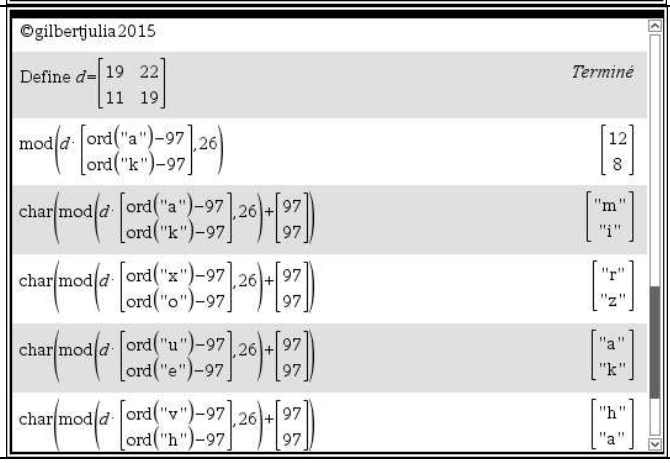
On peut retrouver le résultat en résolvant deux systèmes à deux inconnues ;

La matrice $15B \equiv \begin{pmatrix} 19 & 22 \\ 11 & 19 \end{pmatrix} (26)$ est telle que : $15BA \equiv I_2\ (26)$




Le décodage consiste à appliquer modulo 26 la matrice $D = 15B \equiv \begin{pmatrix} 19 & 22 \\ 11 & 19 \end{pmatrix}$ au vecteur colonne des numéros des deux lettres à décoder. On peut (chez soi mais pas devant sa copie de CAPES…) automatiser le décodage.

On reconnaît un hommage du jury du CAPES à la récente récipiendaire de la médaille Fields Maryam Mirzakhani .




**4.** Le codage d'un bloc de deux lettres $\begin{pmatrix} x \\ y \end{pmatrix}$ amène à définir : $\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} a\,x + b\,y \\ c\,x + d\,y \end{pmatrix} (26)$

Le décodage amène à savoir résoudre inversement tout système de congruences : $\begin{cases} ax + by \equiv x'\ (26) \\ cx + dy \equiv y'\ (26) \end{cases} [S1]$

En appliquant la matrice : $B = (a+d)I_2 - A = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ , le système [$S1$] implique : $\begin{cases} (ad - bc)x \equiv d\,x' - b\,y'\ (26) \\ (ad - bc)y \equiv -c\,x' + a\,y'\ (26) \end{cases} [S2]$.

Si $ad - bc$ est premier avec 26 (donc est un nombre impair non multiple de 13), alors il existe $u$ appartenant à $[1\,;\,25]$ tel que $u(ad - bc) \equiv 1\ (26)$ et $\begin{cases} x \equiv u(d\,x' - b\,y')\ (26) \\ y \equiv u(-c\,x' + a\,y')\ (26) \end{cases}$ : le décodage est possible.

Si $ad - bc$ n'est pas premier avec 26, alors il existe $u$ non congru à zéro modulo 26 tel que $(ad - bc)u \equiv 0\ (26)$ et dans ce cas : $A \times (uA - u(a+d)I_2) \equiv O_2\ (26)$. Il existe des vecteurs non nuls modulo

26 dont l'image par $A$ est pourtant le vecteur $\begin{bmatrix}0\\0\end{bmatrix}$. On peut citer $\begin{pmatrix}bu\\-au\end{pmatrix}$ ou $\begin{pmatrix}cu\\-du\end{pmatrix}$. Au cas où $au=bu=cu=du=0$, on citerait $\begin{pmatrix}u\\u\end{pmatrix}$.

La matrice $A$ ne construit pas une bijection de $[0\,;25]\times[0\,;25]$ sur lui-même, le déchiffrement est impossible (et le chiffrement n'est pas un bon chiffrement puisque plusieurs couples différents sont codés de la même façon …).

En conclusion, $ad-bc$ premier avec 26 est une condition nécessaire et suffisante pour que le décodage de tout bloc de deux lettres soit possible.