1 Commandes Xcas pour la spécialité maths Terminale S.

Ces commandes se trouvent dans le menu `Cmds`.

Arithmétique	
`iquo(a,b), irem(a,b)`	quotient et reste de la division euclidienne de a par b
`isprime(p)`	Test de primalité
`gcd(a,b), lcm(a,b)`	PGCD, PPCM de 2 entiers
`iabcuv(a,b,c)`	Renvoie u et v tels que $au + bv = c$
`powmod(a,n,m)`	Renvoie $a^n \pmod m$
`L:=convert(a,base,b)`	conversion de a en base b
`a:=convert(L,base,b)`	conversion inverse
`n:=a % b; A:=n % 0`	$n \in \mathbb{Z}/b\mathbb{Z}$ congru à a ; $A \in \mathbb{Z},\ A = a \pmod b$
Matrices et vecteurs	
`M:=matrix(3,4,(j,k)->j+k)`	matrice définie par une formule
`M:=[[1,2,3],[4,5,6]]`	matrice définie par des coefficients (ou bien créer un tableur Xcas en lui donnant un nom de variable)
`v:=[0,1,0]`	vecteur défini par ses coordonnées
`M[0,1] ou M(1,2)`	élément de `M` ligne 1 colonne 2 les indices commencent à 0 ou à 1 selon la notation
`M[j,k]:=a`	modifie l'élément d'indice j,k (copie M)
`M[j,k] =< a ou M(j,k) =< a`	modifie en place l'élément d'indice j,k
`+,-,*`	addition, soustraction, multiplication de matrices/vecteurs
`inv(M)`	inverse d'une matrice carrée `M`
`M^4`	puissance entière d'une matrice
`matpow(M,n)`	puissance (symbolique) d'une matrice faire `supposons(n>0)` si `M` n'est pas inversible
`P,D:=jordan(M)`	diagonalisation de la matrice `M` (hors programme)
Autres	
`asc("chaine")`	renvoie la liste des codes ASCII d'une chaine
`char(L)`	renvoie la chaine de caractères à partir d'une liste
`rsolve()`	résolution de suites récurrentes
`L:=readrgb("fichier")`	lecture du fichier image (jpg, png) dans `L`
`writergb("fichier.png",L)`	stocke et affiche l'image contenue dans `L`
`rectangle(dx,0,dy/dx,` `gl_texture="fichier")`	affiche l'image de taille `dx,dy` contenue dans fichier

Attention : la notation `M(j,k):=a` est interprétée comme une définition de fonction si `j,k` est symbolique (non entier) et non comme une affectation de l'indice j,k de M. On peut utiliser la notation `M(j,k)=<a` qui modifie toutes les matrices partageant la représentation de M, est donc beaucoup plus rapide pour de grosses matrices, mais peut avoir des effets surprenants.
N.B. : il peut être nécessaire d'utiliser la version 0.9.6 ou ultérieure de Xcas.

2 Exemples d'illustrations

- **Cryptographie**
  `s:="un message a coder"; L:=asc(s)`, la liste `L` contient une suite d'entiers compris entre 0 et 255. Pour le système RSA, on peut générer une paire de premiers et n

`p:=nextprime(10^30); q:=nextprime(10^15); n:=p*q;`
(on peut aussi utiliser de l'aléatoire) puis une paire de clefs,
`n1:=euler(n); c:=rand(); d:=inv(c % n1) % 0`
puis coder et décoder avec `N:=powmod(L,c,n); char(powmod(N,d,n));` Pour éviter des attaques évidentes, on peut créer des regroupements de 8 par deux conversion en base
`l:=convert(L,base,256); M:=convert(l,base,256^8)`
Pour le système de Hill, on crée par exemple une matrice aléatoire 2,2
`n:=nextprime(512); M:=ranm(2,2) % n; Minv:=inv(M);`
(on recommence si `M` n'est pas inversible), puis on calcule les produits par paire d'éléments de `L` (ajouter un espace dans `s` en fin de si le nombre d'éléments est impair)
`N:=seq(M*[L[2*j],L[2*j+1]],j,0,size(L)/2-1)`
Le décodage en utilisant `Minv`
`O:=seq(Minv*N[j],j,0,size(N)-1)`
puis il faut aplatir `O` avant d'appeler `char`
`P:=[]; pour j de 0 jusque size(O)-1 faire P:=concat(P,O[j]); fpour; P`

– **Systèmes dynamiques, graphes probabilistes**
Ouvrir un tableur (menu Tableur), indiquez par exemple 4 lignes et 4 colonnes et choisissez un nom de matrice, par exemple `M` puis remplissez-le par exemple avec

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \end{pmatrix}$$

Si vous n'avez pas le bon nombre de lignes ou de colonnes ou oublié le nom de variable, cliquez sur la ligne `Sheet config...` du tableur. Vous pouvez ensuite faire une étude formelle
`supposons(n>0); Mn:=matpow(M,n); limit(Mn,n=inf)`
ou numérique avec `v:=seq(1./nrows(M),j,1,nrows(M));`
`pour j de 1 jusque 100 faire v:=M*v; fpour;`
Notez que pour un graphe probabiliste, les sommes des colonnes doivent être égales à 1 pour la convention du programme de TS (produit matrice, par vecteur).
Un exemple de modèle proie-prédateur se trouve sur le site pédagogique de Xcas
`www-fourier.ujf-grenoble.fr/~parisse/irem.html`

– **Images**
Voir la session `image.xws` sur le site de Xcas (cf. ci-dessus).

– **Autres**
Cherchez le mot-clef fougere (F12 dans Xcas), ou fraction continue (en lien avec l'identité de Bézout, les réduites successives sont les coefficients de Bézout de $au_n - bv_n = (-1)^n r_n$), ...