Eléments à retenir sur les ensembles :

Langage ensembliste :

- Il est possible de définir un ensemble :
  - Par extension : On donne la liste de ses éléments
  - Par compréhension : On donne une règle pour retrouver les éléments
- Le nombre d'éléments dans un ensemble est appelé cardinal de l'ensemble : card(E)
- Un ensemble A est inclus dans un ensemble B ($A \subset B$) si chaque élément de A se trouve aussi dans B. A est donc un sous-ensemble de B
- Chaque ensemble est inclus dans lui-même ($A \subset A$)
- L'ensemble vide est inclus dans n'importe quel ensemble ($\{\} \subset A$).
- On appelle complémentaire à A dans E ($C_E A$) l'ensemble des éléments appartenant à E mais pas à A.
- L'intersection $A \cap B$ de deux ensembles contient les éléments qui appartiennent à la fois aux deux ensembles.
- La réunion A U B de deux ensembles contient les éléments qui appartiennent soit à l'un soit à l'autre ensemble.
- Le produit cartésien de deux ensembles contient l'ensemble des couples dont le premier élément appartient au premier ensemble et dont le second élément appartient au second ensemble.

Relations binaires :

- Une relation binaire est une notion qui lie un élément d'un ensemble de départ à un élément d'un ensemble d'arrivée : x R y.
- Cette relation peut être représentée par :
  - Un tableau simple
  - Un tableau à double entrées
  - Une matrice
  - Un diagramme sagittal
  - Une liste de couples
- Nous pouvons qualifier une relation binaire R :
  - Réflexive si pour tout x appartenant à E, x R x
  - Symétrique si pour tout couple (x,y) appartenant à E^2, x R y implique y R x

  - Antisymétrique si pour tout couple (x,y) appartenant à E^2, si on a x R y et y R x, alors forcément x = y
  - Transitive si pour tout triplet (x,y,z) appartenant à E^3, si on a x R y et y R z, alors forcément x R z
- Si la relation est réflexive, symétrique et transitive, il s'agit d'une relation d'équivalence
- Si la relation est réflexive, antisymétrique et transitive, il s'agit d'une relation d'ordre :
  - R est une relation d'ordre total si pour tout couple (x,y) appartenant à E^2 on a x R y ou y R x
  - Il s'agit d'une relation d'ordre partiel dans le cas contraire

Application d'un ensemble dans un ensemble :

- Une application d'un ensemble E vers un ensemble F est une relation binaire de E vers F qui à tout élément de E, associe un unique élément de F
- L'image directe d'un ensemble A ($A \subset E$) par une application f est l'ensemble des images de A : f(A)
- L'image réciproque d'un ensemble B ($B \subset F$) est un sous ensemble de E qui contient tous les éléments dont les images par f constituent B : $f^{-1}(B)$
- Une application peut être :
  - Surjective : Chaque élément de F possède au plus un antécédent
  - Injective : Chaque élément de F possède au moins un antécédent
  - Bijective : si elle est surjective et injective
- Une application composée de f par g est l'application de E dans G qui associe à chaque élément x de E, g(f(x)) : $g \circ f$:
  - La composée de deux injections est une injection
  - La composée de deux surjections est une surjection
  - La composée de deux bijections est une bijection
- Dans le cas d'une bijection (y = f(x)) il est possible de définir une bijection réciproque : $x = f^{-1}(y)$

Exercice type :

Trois amis, Kim, John et Bob, décident de mettre au point un système de cryptage de messages. Chacun des trois imagine la meilleure solution pour chiffrer un message et pour pouvoir naturellement le déchiffrer.

Langage ensembliste :

Dans un premier temps, les 3 amis se fixent une limite en termes de caractères à convertir. Ils veulent uniquement s'occuper des lettres majuscules, minuscules (sans accent, ni caractères spéciaux du genre 'ç') et des chiffres.

- Donner le cardinal de chacun des 3 ensembles :
  - A : l'ensemble des lettres majuscules
  - B : l'ensemble des lettres minuscules
  - C : l'ensemble des chiffres
- Donner le cardinal de l'ensemble E des caractères considérés par nos 3 amis.
- Utiliser les ensembles E, A, B et C et les opérations d'intersection ∩ et de réunion U pour exprimer :
  - L'ensemble E en fonction des 3 autres : E = ?
  - L'ensemble des lettres indépendamment de la casse : D = ?
  - Le complément à A dans E : $C_E A$ = ?

Relations binaires :

Avant de se lancer dans des notions de cryptage plus avancées, les 3 amis se concentrent sur un petit échantillon de caractères, plus précisément les chiffres {1, 2, 3}. Ils veulent utiliser les propriétés des relations binaires. Ils veulent associer une valeur de départ à une valeur d'arrivée à l'aide de cette relation. Pour cela ils proposent 3 types de relations : Ra, Rb, Rc :

- Ra : 2 Ra 1, 1 Ra 2, 2 Ra 3, 3 Ra 2
- Rb : 2 Rb 1, 1 Rb 2, 2 Rb 3, 3 Rb 2, 1 Rb 1, 2 Rb 2, 3 Rb 3
- Rc : 1 Rc 1, 2 Rc 2, 3 Rc 3

- Dites pour chaque Relation binaire si elle est :
    - Réflexive si pour tout x appartenant à E, x R x
    - Symétrique si pour tout couple (x,y) appartenant à E^2, x R y implique y R x
    - Antisymétrique si pour tout couple (x,y) appartenant à E^2, si on a x R y et y R x, alors forcément x = y
    - Transitive si pour tout triplet (x,y,z) appartenant à E^3, si on a x R y et y R z, alors forcément x R z
- Pourquoi aucune des solutions ne peut convenir pour crypter un message ?

Application d'un ensemble dans un ensemble :

Kim a entendu parler de l'algorithme de chiffrage affine pour crypter les messages. Elle en parle à John qui décide de l'utiliser pour crypter les chiffres de 0 à 9. Il utilise pour cela la fonction f(x) = (4*x + 7) modulo 10. Il obtient les conversions suivantes :

Départ	Arrivée
0	7
1	1
2	5
3	9
4	3
5	7
6	1
7	5
8	9
9	3

- Cette conversion est-elle injective, surjective ou bijective ?
- Peut-elle être utilisée dans le cas d'un chiffrage ?

Bob essaie de comprendre le problème et il lit sur un forum spécialisé que l'algorithme de chiffrage affine ne fonctionne que si le coefficient directeur et le nombre d'éléments sont premiers entre eux (PGCD(nbElem, a) = 1).

- Donner la liste des a possibles tels que PGCD(10, a) = 1

Bob propose d'utiliser la fonction affine f(x) = (3*x + 4) modulo 10.

- Est-ce un bon choix en termes de coefficient directeur ?

La répartition donnée par la conversion est :

Départ	Arrivée
0	4
1	7
2	0
3	3
4	6
5	9
6	2
7	5
8	8
9	1

- Cette conversion est-elle injective, surjective ou bijective ?

Composée d'applications :

Kim propose d'aller encore plus loin. Pour rendre le message encore plus difficile à décoder, nous pourrions utiliser le chiffrage affine de Bob et en plus effectuer un décalage César de 3 positions :

Départ	Affine	César
0	4	7
1	7	0
2	0	3
3	3	6
4	6	9
5	9	2
6	2	5
7	5	8
8	8	1
9	1	4

Il s'agit ici d'une composition d'application g ° f avec :

- f(x) = 3*x + 4 modulo 10
- g(x) = x + 3 modulo 10

- Vérifier que les deux fonctions sont bien des bijections
- Que peut-on en conclure sur la composition g ° f ?

Nous allons déchiffrer le message codé avec cette composition :

- Donner $g^{-1}(x)$, la fonction qui permet d'annuler l'action de g(x) tel que $g^{-1}(g(x)) = x$
- Sachant que $f^{-1}(x)$ est la fonction réciproque de f(x), donner la composition qui va permettre de déchiffrer le message
- On donne $f^{-1}(x) = 7*(x-4)$ modulo 10, vérifier que l'on peut décoder nos chiffres avec la composition proposée au-dessus.