Utilisation de Xcas en arithmétique

Il faudra structurer votre console, pour que le fichier sauvegardé soit lisible.
Pour différencier chaque exercice dans votre console Xcas, vous pouvez créer des groupements pour chaque exercice : menu `Edit --> Nouveau groupe`, avec possibilité de nommer le groupe obtenu.
Vous pouvez ensuite entrer des lignes de commentaires, qui ne seront pas exécutés et s'afficheront en vert : menu `Outils --> Nouveau commentaire`.
Vous pouvez réagencer également vos lignes de calculs, et en supprimer, en les sélectionnant au niveau de leur numéro, et en les déplaçant avec la souris, et en allant dans le menu `Edit --> Supprimer niveaux sélectionnés`.

Exercice 1. *Calculs dans $\mathbb{Z}/n\mathbb{Z}$*
Pour entrer un entier a modulo n, il suffit d'écrire `a % n` ou `a mod n`. Attention : Xcas affiche par défaut le reste entier symétrique comme représentant de la classe de a modulo n, et non le reste de la division euclidienne (par exemple `2 % 3` affiche `-1 % 3`).
On peut ensuite effectuer les calculs usuels dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, avec les symboles d'opération usuels : `+, -, *, /, ^`. Tester différents calculs.
Puissances d'un entier modulo n : comparer les deux procédures suivantes sur des exemples : `(a^m) % n` et `(a % n)^m` ; que se passe-t-il ?
Applications :
a. Vérifier le théorème d'Euler ($a^{\varphi(n)} \equiv 1 \mod n$), pour différentes valeurs de a et n telles a et n soient premiers entre eux. On pourra utiliser la fonction `euler(n)`, et aussi `gcd(a,n)` (cf exercice 3) pour tester si les deux entiers a et n sont premiers entre eux.
b. Résoudre les équations suivantes (on pourra utiliser la fonction `solve(expr,var)`) :
$100x \equiv 2 \mod 541$, $319x \equiv 185 \mod 209$, $551x \equiv 703 \mod 361$, $403x \equiv 52 \mod 299$.
c. Calculer dans $\mathbb{Z}/11\mathbb{Z}$, $\prod_{a=0}^{10}(x-a)$. On pourra utiliser la fonction `product(expr,var,min,max)`.

Exercice 2. *Calculs dans $\mathbb{Z}$: division euclidienne*
Division euclidienne de a par b : `iquo(a,b)` donne le quotient et `irem(a,b)` donne le reste. On peut obtenir directement le quotient et le reste dans une liste par la fonction `iquorem(a,b)`.
Pour obtenir le reste entier symétrique ($a = bq + s$ avec $-b/2 < s < b/2$), on utilise `smod(a,b)`.
On peut retrouver le reste de a^m modulo n, par la fonction `powmod(a,m,n)`.
Applications :
a. Donner les trois derniers chiffres du nombre 2011^{399}. Donner les deux derniers chiffres du nombre 19969^{19969}.
b. Quel est le chiffre des unités de $2013^{2012^{2011}}$?

Exercice 3. *Calculs dans $\mathbb{Z}$: pgcd, égalité de Bezout*
Pour calculer le pgcd de deux entiers relatifs a et b on utilise : `gcd(a,b)`. La commande `iegcd(a,b)` renvoie une liste de 3 entiers u, v, d tels que $au + bv = d = pgcd(a,b)$ (égalité de Bezout).
La commande `iabcuv(a,b,c)` renvoie elle une solution de l'équation $ax + by = c$. Quel est le lien entre les deux fonctions `iegcd(a,b)` et `iabcuv(a,b,c)` ?
Applications :
a. Vérifier pour différentes valeurs du couple d'entiers naturels (m,n) tel que $0 < n < m$, que :
$pgcd(p^m - 1, p^n - 1) = p^{pgcd(m,n)} - 1$. Est-ce que p doit nécessairement être un nombre premier ?
b. Résoudre l'équation $235x - 341y = 112$.
c. Trouver l'inverse de 23699 modulo 253921, et de 22646 modulo 70616 en utilisant une fonction décrite ci-dessus. Vérifier avec un calcul dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 4. *Calculs dans $\mathbb{N}$: diviseurs, primalité*

1. Pour obtenir la décomposition en facteurs premiers d'un entier n on utilise `ifactor(n)`. Si de plus, on souhaite pouvoir récupérer précisément les facteurs premiers de n, ainsi que leur exposant, on utilisera la commande `ifactors(n)` qui fournit le résultat sous forme de liste.

   La commande `idivis(n)` fournit la liste de tous les diviseurs de l'entier n.

   Applications :

   a. Quel est l'exposant de 17 dans la décomposition en facteurs premiers de 500! ? Par combien de 0 se termine 500! ?

   b. Tester la factorisation des six premiers nombres de Fermat $F_n = 2^{2^n} + 1$. Quel est le premier nombre de Fermat qui n'est pas premier ?

   c. Etudier la factorisation des entiers $\dfrac{10^k - 1}{9}$ pour k variant de 1 à 40, puis de 1 à 60. Que constate-t-on ?

   d. Parmi les entiers de 1 à 2013 quel est celui qui a le plus grand nombre de diviseurs ?

   Pour les questions b. à d., on pourra utiliser des commandes de création et de manipulation de listes : `seq(expr,var,min,max)` pour la création d'une liste, `size(L)` pour la taille d'une liste, et `sort(L)` pour le tri d'une liste (et éventuellement, `SortD(L)` ou encore `sort(M,(x,y)->x[0]>y[0])` pour le tri décroissant d'une liste ou d'une matrice).

2. La fonction `isprime(n)` teste la primalité de l'entier n et renvoie `vrai` si l'entier est premier et `faux` sinon. La commande `is_pseudoprime(n)` teste la pseudo-primalité et renvoie 0 si l'entier n'est pas premier, 1 s'il l'est probablement, et 2 s'il l'est de façon certaine.

   Pour "trouver" des nombres premiers on pourra utiliser les deux fonctions `nextprime(n)` ou `prevprime(n)` qui donnent respectivement le prochain et le précédent nombre pseudo-premier à partir de l'entier n.

   Applications :

   a. Etudier la primalité des entiers $\dfrac{10^k - 1}{9}$ pour k variant de 1 à 40, puis de 1 à 100. Comparer avec l'exercice 4.1.c. Qu'en pensez-vous ?

   b. Trouver un nombre premier (ou probablement premier) s'écrivant avec 300 chiffres. Trouver le plus petit et le plus grand nombre premier s'écrivant avec 300 chiffres.

   c. Nombres de Mersenne : un nombre de Mersenne est un entier s'écrivant sous la forme $2^p - 1$ avec p premier. Trouver les 12 premiers nombres de Mersenne. Quels sont ceux qui sont premiers ? Seriez-vous capable de trouver un nombre premier de Mersenne s'écrivant avec au moins 20 chiffres ?