Contrôle du 7 octobre 2011
durée 1h30

Sans document.
Les réponses aux questions théoriques doivent être rédigées rigoureusement.
Les réponses aux questions utilisant Maple doivent comporter les commandes tapées, leurs résultats et vos commentaires.

Exercice 1 (1 point) Rédaction

La qualité de la rédaction vaut 1 point.

Exercice 2 (4 points) Equations diophantiennes linéaires

Résoudre dans **Z** les équations :

- $241662\, x + 372160\, y = 669308$
- $105411\, x + 392506\, y = 160517$

On demande toutes les solutions et la suite de calculs pour les obtenir.
Explicitez le lien entre vos solutions et celles de la commande **isolve** de Maple.

Exercice 3 (5 points) Equations modulaires

Résoudre dans **Z/nZ** les équations :

- $257784\, x = 232773 \bmod 879615$
- $98031\, x = 111872 \bmod 365026$

On demande toutes les solutions et la suite de calculs pour les obtenir.
Vérifiez avec la commande **msolve** de Maple.

Exercice 4 (10 points) Test de primalité

- Montrer que si n est un nombre premier impair alors l'équation $x^2 = 1 \bmod n$ a pour seules solutions $x = 1 \bmod n$ ou $x = (-1) \bmod n$.
- Soit n un nombre premier impair et a un entier entre 1 et $n-1$, montrer que $a^{\left(\frac{n-1}{2}\right)}$ est égal à 1 ou -1 modulo n .
- Ecrire une procédure `TestPremier(n,a)` qui effectue le test ci-dessus et rend **true** *si* n est peut-être premier, **false** sinon.
- Donner tous les n <u>non premiers</u> entre 1000 et 2000 pour lesquels ce test répond **true** avec $a = 6$.