

## TP2 : Equations Diophantiennes linéaires

N'oubliez pas d'exécuter (valider avec la touche Entrée) les commandes Maple (texte en rouge) avant de les utiliser.

Les exercices en petits caractères sont facultatifs.

### – Calcul des coefficients de Bézout

On utilisera la fonction **igcdex** de Maple :

```
[ > igcdex(456,123,'u','v');
```

qui rend le pgcd mais en plus

```
[ > u,v,u*456+v*123;
```

met des coefficients de Bézout dans les variables dont les noms sont donnés entre apostrophes.

Nous allons utiliser ces calculs pour résoudre différentes équations.

### – Equation $ax+by=c$

Exercice 1 : écrire une fonction qui prenne en entrée trois entiers a, b et c et rende les entiers x et y tels que  $ax+by=c$ .

```
[ > sol1(456,123,21);
```

```
                                {x=119+41k,y=-441-152k}
```

Comparez avec les solutions données par `isolve` (?isolve). La façon dont les résultats sont rendus permet de les utiliser dans la fonction `subs` (?subs).

Exercice 2 : écrire une fonction qui prenne en entrée trois entiers a, b et m et rende les x tels que  $ax \equiv b \pmod{m}$ .

```
[ > sol2(123,21,456);
```

```
                                {15,167,319}
```

Comparez avec les solutions données par `msolve` (?msolve).

Exercice 3 : écrire une fonction qui prenne en entrée deux entiers a et m et rende l'inverse de a (mod m) s'il existe (pourquoi est-il alors unique ?) et FAIL sinon. Comparez avec les solutions données par `mod` (?mod, ?FAIL). Comprenez-vous l'intérêt de FAIL ?

Exercice 4 : dans les livres de casse-têtes mathématiques on peut trouver ce genre de problèmes : 5 marins se retrouvent sur une île déserte. Ils ramassent le maximum de noix de coco. La nuit venue le premier décide de dissimuler sa part : il divise le tas en 5 parts égales, il reste une noix de coco qu'il jette, il cache sa part. Ainsi fait le second un peu plus tard, puis le troisième, le quatrième et le cinquième. Le lendemain ils se partagent le tas restant en 5 parts égales. Combien y'avait-il de noix de coco au départ ?

### – Théorème des restes chinois

Exercice 5 : écrire une fonction qui prenne en entrée quatre entiers a, m, b et n et rende, si m et n sont premiers entre eux, l'unique x (mod mn) tel que  $x \equiv a \pmod{m}$  et  $x \equiv b \pmod{n}$ , FAIL sinon.

Exercice 6 : écrire une fonction qui prenne en entrée deux listes d'entiers  $[a_1 \dots a_n]$  et  $[m_1 \dots m_n]$  et rende, si les  $m_i$  sont premiers entre eux deux à deux, l'unique x modulo le produit des  $m_i$  tel que  $x \equiv a_i \pmod{m_i}$ , FAIL sinon.

