TP 03: Euclid's extended algorithm

Jean-Sébastien Coron

Université du Luxembourg
http://www.jscoron.fr

1 Multiplicative inverse

Write a program `inverse` taking as input deux integers a and n, and outputting the multiplicative inverse of a modulo n if it exists, using Euclid's extended algorithm.

```
$ inverse 5 7
3
$ inverse 2 6
2 has no inverse modulo 6
```

2 Crible d'Erastothène

La méthode du crible d'Erastothène permet d'afficher efficacement tous les entiers premiers compris entre 1 et n, pour un entier n donné.

Un entier est dit *premier* si ses seuls diviseurs sont 1 et lui-même. Par exemple, 13 est premier, mais $15 = 3 \cdot 5$ n'est pas premier.

La méthode consiste à utiliser un tableau de n valeurs booléennes ("vrai" ou "faux"), la i-ème case du tableau correspondant à l'entier i. A la fin, si la i-ème case contient la valeur "vrai", alors l'entier i est déclaré premier. Sinon, l'entier i n'est pas premier.

On pourra utiliser un tableau d'entiers, la valeur "vrai" correspondant à 1, et la valeur "faux" correpondant à 0.

Initialement, toutes les cases du tableau sont déclarées à la valeur "vrai". Ensuite, pour chaque case i en partant de la case numéro 2, si cette case contient la valeur "vrai", alors on "raye" les cases multiples de i (c'est à dire que l'on met la valeur "faux" dans toutes les cases multiples de i jusqu'à n, sauf la case i elle-même). On continue ainsi jusqu'à la dernière case du tableau.

```
$ premier 15
1 2 3 5 7 11 13
```