TP 02: Division modulaire et reste chinois

Jean-Sébastien Coron

Université du Luxembourg
www.jscoron.fr

1 Division modulaire

En utilisant l'algorithme d'Euclide étendu, écrire un programme `divisionmod` prenant en entrée a, b et n et affichant le quotient modulaire $c = a/b \mod n$ si b est inversible modulo n. On vérifiera à l'aide de $c \cdot b \equiv a \mod n$ que le résultat est correcte:

```
$ divisionmod 2 3 11
8
$ divisionmod 2 5 10
5 n'a pas d'inverse multiplicatif modulo 10
```

2 Reste chinois

Ecrire un programme `restechinois` prenant en entrée a_1, n_1, a_2, n_2 avec $\mathrm{PGCD}(n_1, n_2) = 1$, et affichant z tel que $z \equiv a_1 \mod n_1$ et $z \equiv a_2 \mod n_2$.

```
$ restechinois 4 5 3 7
24
```

car $24 \equiv 4 \mod 5$ et $24 \equiv 3 \mod 7$.