TP 02: Euclid's extended algorithm and Chinese Remainder

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 Chinese Remainder

Write a program `restechinois` taking as input a_1, n_1, a_2, n_2 with $\gcd(n_1, n_2) = 1$, and printing z such that $z \equiv a_1 \mod n_1$ and $z \equiv a_2 \mod n_2$.

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

because $24 \equiv 4 \mod 5$ and $24 \equiv 3 \mod 7$.