TP 4: Basic Programming Exercises

Jean-Sébastien Coron

Université du Luxembourg

1 Euclid's Algorithm

Write a program `gcd` taking as input 2 integers and outputting their gcd, using Euclid's algorithm.

```
$ gcd 12 15
3
```

2 Decomposition

Write a program `factor` taking as input an integer n and outputting its factorization, using the naive algorithm. For example, for $150 = 2^1 \cdot 3^1 \cdot 5^2$:

```
$ factor 150
(2,1) (3,1) (5,2)
```

3 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
```