TP 01: Basic 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
```

4 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 $24 \equiv 3 \mod 7$.

5 Euler function

Write a program `euler` that prints the Euler function of n:

```
$ euler 10
4
```

6 Carmichael numbers

A Carmichael number is an odd composite integer n such that Fermat's little theorem

$$a^{n-1} - 1 \equiv 0 \mod n$$

is satisfied for every choice of $1 < a < n$ such that $\gcd(a, n) = 1$.

For example, 561 is the smallest Carmichael number. Write a program that prints every Carmichael numbers less than 10000.