TP 4: computing in $\mathbb{Z}_n$

Jean-Sébastien Coron

Université du Luxembourg

1 Substraction

Implement the substraction algorithm for big integers given in the course, and test it with random values with the previously implemented addition algorithm for big integers.

2 Division with remainder

Implement the division with remainder algorithm for big integers given in the course.

3 Computing in $\mathbb{Z}_n$

Implement the addition and multiplication algorithm for integers in $\mathbb{Z}n$

4 Euler function

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

```
$ euler 10
4
```

5 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.