TP 3: Computing with Large Integers, and Modular Exponentiation

Jean-Sébastien Coron

Université du Luxembourg

1 Addition

Implement in C language the big integer addition algorithm. You can use the structure:

```
typedef struct {
 int sign;
 int size;
 int *tab;
} bignum;
```

2 Fibonacci Sequence

We define the Fibonacci sequence $u_0 = 1$, $u_1 = 1$, $u_n = u_{n-1} + u_{n-2}$ for $n \geq 2$. Write a program that computes the n terms of the Fibonnaci sequence, for a given n, using the previous addition algorithm. You can use base $B = 10$.

Check that $u_{100} = 573147844013817084101$. What is the value of u_{101} ?

3 Multiplication

Implement in C the multiplication algorithm on big integers.

4 Factorial

We define $n! = n \cdot (n-1) \ldots 2 \cdot 1$. Write a program computing $n!$ for a given n, using the previous multiplication algorithm.

Check that $30! = 265252859812191058636308480000000$. What is the value of $40!$?

5 Modular Exponentiation

Write a program `expmod` that implements the modular exponentiation algorithm from the course, for small integers.

```
$ expmod 2342 6762 9343
7147
```

because $2342^{6762} \equiv 7147 \mod 9343$.