TP 02: Chinese Remainder, and Computing with Large Integers

Jean-Sébastien Coron

Université du Luxembourg
http://www.jscoron.fr

1 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 $24 \equiv 3 \mod 7$.

2 Addition

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

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

3 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} ?

4 Multiplication

Implement in C the multiplication algorithm on big integers.

5 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 $40!$?

6 Modular Exponentiation

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

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

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