

## Rappels

C'est une sous-branche de la sécurité.

Même si l'adverse connaît votre algorithme de cryptage, il doit être impossible pour l'adverse de décrypter votre message.

Pour cela, on étudie  $\mathbb{Z}/n\mathbb{Z}$ , permettant de travailler sur des blocs de taille finie.

$(\mathbb{Z}/n\mathbb{Z}, +) \Rightarrow$  groupe commutatif.

$(\mathbb{Z}/n\mathbb{Z}, +, *) \Rightarrow$  anneau commutatif unitaire

$(\mathbb{Z}/n\mathbb{Z}, +, *) \Rightarrow$  corps ssi  $n$  est premier

Dans  $\mathbb{Z}/n\mathbb{Z}$ :  $a \in \mathbb{Z}/n\mathbb{Z}$  inversible ssi  $a$  et  $n$  premier entre eux de plus, et dans ce dernier cas:

$$\exists s, t : as + nt = 1$$

$$s \equiv a^{-1} \pmod{n}$$

Existe-t-il  $n$  tel que  $a : 1 \leq a \leq n-1$  est premier avec  $n$  ?  $\Leftrightarrow n$  premier ?

$P1 \Rightarrow P2$ :  $n$  premier

$$d = \text{pgcd}(a, n)$$

$$n = dq, dq = 1 \text{ a un}$$

$$\text{si } d = n, a = qd' \neq 0, a > n !$$

$P2 \Rightarrow P1$

On suppose  $n$  non premier,  $n = dc$ ,  $c, d \neq 1$  et  $n$ .

$$2 \leq d \leq n-1, d \text{ est premier avec } n.$$

$$\text{pgcd}(d, n) = 1, d = 1 \text{ et } n \text{ est premier}$$

Bien entendu, les calculs vont plus loin que de l'addition ou de la multiplication.

Nous verrons des algorithmes et des propriétés basiques puis nous regarderons des structures de  $\mathbb{Z}/n\mathbb{Z}$ , enfin nous verrons le RSA, avec des tests de primalités.

## Exponentiation modulaire (général)

**Astuce :**

$$x^{2q} = (x^q)^2 \text{ 1 multiplication}$$

$$x^{2q+1} = x * (x^q)^2 \text{ 2 multiplication}$$

q a un chiffre de moins, en base 2, que 2q ou 2q + 1

**Exemple :**

$$5^{77} \pmod{9}$$

$$77 = 2 * 38 + 1$$

$$5^{77} = 5 * (5^{38})^2 \equiv 5 * 7^2 \equiv 5 * 49 \equiv 20 \equiv 2$$

$$5^{38} = (5^{19})^2 = 5^2 \equiv 25 \equiv 7$$

$$19 = 2 * 9 + 1$$

$$5^{19} = 5 * (5^9)^2 \equiv 5 * 8^2 = 5 * 64 \equiv 5$$

$$9 = 2^3 + 1$$

$$5^9 = 5 * (5^{2^3}) \equiv 5 * 7 = 35 \equiv 8$$

## Lemme Chinois

Soient  $n_1, n_2, \dots, n_k$  des nombres premiers entre eux deux à deux.

Soient  $a_1, a_2, \dots, a_k$  des entiers quelconques

Il existe un entier  $a \forall i a \equiv a_i \pmod{n_i}$

**Exemple :**

$$n_1 = 5, a_1 = 2, n_2 = 7, a_2 = 3$$

$$n_1 = 2 \quad n_2 = 3$$

$$0 \ 0 \ 0$$

$$1 \ 1 \ 1$$

$$0 \ 2 \ 2$$

$$1 \ 0 \ 3$$

$$0 \ 1 \ 4$$

$$1 \ 2 \ 5$$

$$0 \ 0 \ 6$$

$$1 \ 1 \ 7$$

On a  $a = 1$ .

### Démonstration avec $k = 2$ :

$n_1, n_2; (n_1, n_2) = 1$  et  $a_1, a_2$

### 1) Cas particulier

$a_1 = 0, a_2 = 0; a = n_1 * n_2$

$a_1 = 1, a_2 = 0 ?$

$? a = q * n_2$  et  $q * n_2 \equiv 1 \pmod{n_1}$

$(n_1, n_2) = 1, n_2$  inversible mod  $n_1$

{Euclide étendu}  $(\exists q) q * n_2 \equiv 1 \pmod{n_1}$

Il existe  $a_{10} \equiv 1 \pmod{n_1} \equiv 0 \pmod{n_2}$ .

$a_{10} = n_2^{-1} \pmod{n_1} * n_2$

$a_{01} \equiv 0 \pmod{n_1} \equiv 1 \pmod{n_2}$

$a_{01} = n^{-1} \pmod{n_2} * n_1$

Une solution :  $a = a_1 * a_{10} + a_2 * a_{01}$

Reprenons l'exemple d'en haut :

$7^{-1} \pmod{5} \equiv 3, a_{10} = 3 * 7 = 21$

$5^{-1} \pmod{7} \equiv 3, a_{01} = 3 * 5 = 15$

$a = 2 * 21 + 3 * 15 = 42 + 45 = 87 = 70 + 17$

## Fonction indicatrice d'Euler

Question: Combien d'éléments inversibles dans  $\mathbb{Z}/n\mathbb{Z}$  ?

$\# \{a \in \mathbb{N}, 1 \leq a \leq n-1; a \text{ et } n \text{ premiers entre eux}\} = \phi(n)$  "Euler totient function"

101 premier

$(\mathbb{Z}/101\mathbb{Z}, +, *)$  Corps

$((\mathbb{Z}/101\mathbb{Z}), *)$  groupe

Il y a  $\phi(101) = 100$  éléments

$\phi(100) = ?$

## **Bibliothèque C++**

gmp : calcul sur les grands nombres