Mathématique et Cryptographie

Cours no. 1

Jean-Sébastien Coron

Université du Luxembourg

Programme

- Rappels en théorie des nombres
  - PGCD
  - Algorithme d'Euclide.
  - Congruence.
  - Algorithme d'Euclide étendu.

PGCD

- Diviseur commun.
  - Soient a, b deux entiers. Un diviseur commun à a et b est un entier m tel que $m|a$ et $m|b$.
- PGCD.
  - Le PGCD de deux entiers a et b est le plus grand diviseur commun de a et b.
  - Si $d = \text{PGCD}(a, b)$, alors pour tout m tel que $m|a$ et $m|b$, on a $m|d$.
- Exemple
  - $\text{PGCD}(9, 6) = 3$
  - $\text{PGCD}(7, 5) = 1$.

Algorithme d'Euclide

- Algorithme d'Euclide
  - Soient deux entiers positifs a, b.
  - Soient $r_0 = a$ et $r_1 = b$.
  - Pour $i \geq 0$, on définit les suites (r_i) et (q_i) telles que :

$$r_i = q_i \cdot r_{i+1} + r_{i+2}$$

    où q_i et r_{i+2} sont le quotient et le reste de la division Euclidienne de r_i par r_{i+1}.
  - Il existe $k > 0$ tel que $r_k = 0$.
  - Alors PGCD$(a, b) = r_{k-1}$.

Justification

- Soient $a > 0$ et $b \geq 0$.
  - Si $b = 0$, alors $\text{PGCD}(a, b) = \text{PGCD}(a, 0) = a$
  - Sinon, soit $a = b \cdot q + r$ avec $0 \leq r < b$.
  - Alors $\text{PGCD}(a, b) = \text{PGCD}(b, r)$.
  - (b, r) plus petit que (a, b).
- $\text{PGCD}(a, b) = \text{PGCD}(b, r)$
  - Si $d|a$ et $d|b$, alors $d|r$, et donc $d|\text{PGCD}(b, r)$. Donc $\text{PGCD}(a, b)|\text{PGCD}(b, r)$.
  - Si $d'|b$ et $d'|r$, alors $d'|a$, et donc $d'|\text{PGCD}(a, b)$. Donc $\text{PGCD}(b, r)|\text{PGCD}(a, b)$.
  - Donc $\text{PGCD}(a, b) = \text{PGCD}(b, r)$.

Congruence

- Définition
  - Soit un entier $n > 0$, et $a, b \in \mathbb{Z}$.
  - a est *congruent* à b si $n|(a - b)$.
  - $a \equiv b \pmod{n}$.
  - n est le *module* de la congruence.
  - Ne pas confondre avec le $\mod$ de la division Euclidienne.
- Théorème
  - Soit un entier $n > 0$. Pour tout entier a, il existe un entier b unique tel que $a \equiv b \pmod{n}$ et $0 \leq b < n$, avec $b := a \mod n$.

Exemples et propriétés

- Exemples :
  - $2 \equiv 8 \mod 3$ car $3|(8-2)$.
  - $12 \equiv 2 \mod 5$ car $5|(12-2)$.
- Propriétés :
  - $a \equiv b \mod n \Leftrightarrow \exists k \in \mathbb{Z}, a = b + k \cdot n$.
  - $a \equiv a \mod n$
  - $a \equiv b \mod n \Rightarrow b \equiv a \mod n$
  - $a \equiv b \mod n$ et $b \equiv c \mod n$ implique $a \equiv c \mod n$

Propriétés

- Compatibilité avec addition et multiplication
  - Si $a \equiv a' \mod n$ et $b \equiv b' \mod n$, alors
  - $a + b \equiv a' + b' \mod n$ et $a \cdot b \equiv a' \cdot b' \mod n$.
- Lors d'un calcul modulo n, on peut substituer à x une valeur x' congruente à x modulo n.
  - Calculer a avec $0 \leq a < 8$ tel que $a \equiv 83 \cdot 72 \mod 7$.
  - Première solution: $83 \cdot 72 = 5976$
    $a = 5976 \mod 7 = 5$.
  - Deuxième solution: $83 \equiv 6 \mod 7$, $72 \equiv 2 \mod 7$,
    $83 \cdot 72 \equiv 6 \cdot 2 \equiv 12 \equiv 5 \mod 7$.

Inverse multiplicatif

- Inverse multiplicatif :
  - Soient un entier $n > 0$ et $a \in \mathbb{Z}$. Un entier a' est dit *inverse multiplicatif* de a modulo n si $a \cdot a' \equiv 1 \mod n$.
- Théorème :
  - Soient $n, a \in \mathbb{Z}$ avec $n > 0$. Alors a possède un inverse multiplicatif modulo n si et seulement si $\text{PGCD}(a, n) = 1$.
  - Preuve ($\Rightarrow$)
    - Si a' inverse multiplicatif de a modulo n, alors $a \cdot a' = 1 \mod n$.
    - Soit $k \in \mathbb{Z}$ tel que $a \cdot a' = 1 + k \cdot n$.
    - Si $d|a$ et $d|n$, alors $d|1$. Donc $\text{PGCD}(a, n) = 1$.

Exemple

- Un inverse multiplicatif de 5 modulo 7 est 3 car

$$3 \cdot 5 \equiv 15 \equiv 1 \mod 7$$

- 2 ne possède pas d'inverse multiplicatif modulo 6 :
  - $2 \cdot 1 \equiv 2 \mod 6$
  - $2 \cdot 2 \equiv 4 \mod 6$
  - $2 \cdot 3 \equiv 0 \mod 6$
  - $2 \cdot 4 \equiv 2 \mod 6$
  - $2 \cdot 5 \equiv 4 \mod 6$

Algorithme d'Euclide étendu

- Algorithme d'Euclide étendu.
  - Soient $a, b \in \mathbb{Z}$ et $d = \text{PGCD}(a, b)$.
  - Permet de calculer $s, t \in \mathbb{Z}$ tels que $a \cdot s + b \cdot t = d$.
- Inverse multiplicatif.
  - Soit a, n avec $n > 0$ et $\text{PGCD}(a, n) = 1$.
  - Avec l'algorithme d'Euclide étendu, on calcule s, t tels que

$$a \cdot s + n \cdot t = 1$$

  - Alors $a \cdot s \equiv 1 \mod n$
  - s est un inverse multiplicatif de a modulo n.

Algorithme d'Euclide étendu

- Algorithme d'Euclide étendu, pour $a > 0$ et $b \geq 0$.
  - Similaire à l'algorithme d'Euclide normal, mais avec deux suites u_i et v_i supplémentaires.
  - $r_0 = a$ et $r_1 = b$.
  - Pour $i \geq 2$, soit $r_i = q_i \cdot r_{i+1} + r_{i+2}$
  - $u_0 := 1,\ v_0 := 0,\ u_1 := 0,\ v_1 := 1$ et pour $i \geq 2$, on définit $u_i = u_{i-2} - q_{i-2} \cdot u_{i-1}$ et $v_i = v_{i-2} - q_{i-2} \cdot v_{i-1}$.
- Il existe $k > 0$ tel que $r_k = 0$.
  - Alors $\mathrm{PGCD}(a, b) = r_{k-1} = u_{k-1} \cdot a + v_{k-1} \cdot b$.

Justification

- On a toujours $r_i = u_i \cdot a + v_i \cdot b$.
  - Vrai pour $r_0 = a = 1 \cdot a + 0 \cdot b$.
  - Vrai pour $r_1 = b = 0 \cdot a + 1 \cdot b$.
  - Si $r_{i-2} = u_{i-2} \cdot a + v_{i-2} \cdot b$ et $r_{i-1} = u_{i-1} \cdot a + v_{i-1} \cdot b$, alors :

$$\begin{aligned} u_i \cdot a + v_i \cdot b &= (u_{i-2} - q_{i-2} \cdot u_{i-1}) \cdot a + \\ &\quad (v_{i-2} - q_{i-2} \cdot v_{i-1}) \cdot b \\ &= r_{i-2} - q_{i-2} \cdot r_{i-1} \\ &= r_i \end{aligned}$$