Algorithmes arithmétiques

Clément Ménier

Table des matières

1 L'algorithme d'Euclide

1.1 Description

Le but est de rechercher le pgcd entre 2 nombres a et b et des coefficients de Bezout associés. On recherche donc s, t tels que $d = sa + tb$. Voici l'algorithme pour le faire:

$(a_0, a_1) \leftarrow (a, b)$
$(s_0, s_1) \leftarrow (1, 0)$
$(t_0, t_1) \leftarrow (0, 1)$
tant que $a_1 \neq 0$ faire
  $q \leftarrow a_0$ div a_1
  $(a_0, a_1) \leftarrow (a_1, a_O - qa_1)$
  $(t_0, t_1) \leftarrow (t_1, t_0 - qt_1)$
  $(s_0, s_1) \leftarrow (s_1, s_0 - qs_1)$

1.2 Complexité

Supposons $a, b \leq N$. On cherche à borner le nombre d'itérations.

$$\begin{array}{rclrcl} c_{n+1} & = & 0 & a_{n+1} & = & 0 \\ c_n & = & 1 & a_n & = & d \\ c_{n-1} & = & c_n + c_{n+1} & a_{n-1} & = & qd \\ \vdots & & & a_i & = & a_{i+2} + q_i a_{i+1} \\ c_0 & = & c_1 + c_2 & a_0 & = & a_2 + q_0 a_1 \end{array}$$

On a par récurrence $c_i \leq a_i$ car $d \geq 1$ et $q_i \geq 1$. Or $c_n \sim \left(\frac{1+\sqrt{5}}{2}\right)^n$. Donc $N \geq \left(\frac{1+\sqrt{5}}{2}\right)^n$. Et l'algorithme est donc en $\mathcal{O}(logN)$.

PROPOSITION 1 *Dans Euclide, tous les coefficients intermédaires s_i, t_i sont $< |a|$.*

LEMME 1 $s_{i+1}t_i - s_i t_{i+1} = (-1)^i$
  PREUVE : Ceci se démontre par récurrence sur i. ■

LEMME 2 *(s_i) (resp (t_i)) est de signe alterné et croissante en valeur absolue pour $i \geq 1$ (resp $i \geq 2$).*
  PREUVE : Pour (t_i) :
  On montre que $t_i = (-1)^{i+1} t'_i$ avec $t'_i > 0$ et croissant par récurence sur i.
    $t_2 = -q_1 < 0$
    $|t_2| = q_1 \geq 1 = |t_1|$
    $t_{i+1} = t_{i-1} - q_i t_i = (-1)^{i+2}(t'_{i-1} + q_i t'_i)$
    $t'_{i-1} + q_i t'_i \geq t'i > 0$ car $q_i \geq 1$ et $t'_{i-1} > 0$.
  ■

2 Les restes chinois

2.1 Le problème

Soit $m_0, \ldots, m_{n-1}$ n entiers premiers entre-eux, ie : $\forall i \neq j, m_i \wedge m_j = 1$. Soit $M = \prod_{i=0}^{n-1} m_i$. Le but est étant donné $r_O, \ldots, r_{n-1}$ de trouver r tel que :

$$\begin{cases} x & \equiv & r_0 \ [m_0] \\ & \vdots & \\ x & \equiv & r_{n-1} \ [m_{n-1}] \end{cases} \iff x \equiv r \ [M]$$

L'existence d'un tel r est assuré par le fait que :

$$\begin{array}{ccc} \frac{\mathbb{Z}}{M\mathbb{Z}} & \simeq & \frac{\mathbb{Z}}{m_0\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{m_{n-1}\mathbb{Z}} \\ \overline{x}^M & \to & (\overline{x}^{m_0}, \ldots, \overline{x}^{m_{n-1}}) \end{array}$$

2.2 Lagrange

Soit $n_i = \frac{M}{m_i}$. Comme $n_i \wedge m_i = 1$ on a $n_i t_i + m_i s_i = 1$. On pose $e_i = n_i t_i$. On a alors $e_i \equiv 1 \ [m_i]$ et $e_i \equiv 0 \ [m_j] \ , i \neq j$.
On prend alors $r = \sum_{i=0}^{n-1} r_i e_i$

3 RSA de base

3.1 Algorithme

Voici l'algorithme du RSA :

- trouver 2 grands entiers premiers p et q, $n = pq$;
- d premier avec $\varphi(n) = (p-1)(q-1)$;
- calculer $e \equiv d^{-1} \ [\varphi(n)]$;
- publier (e, n);
- coder les messages par blocs d'entiers $M < n$;
- envoyer le message $C \equiv M^e \ [n]$;
- décoder $D \equiv C^d \ [n]$.

On sait que $M^{ed} \equiv M \ [n]$.

REMARQUE 1 Le calul de e se fait par la recherche des coefficients de Bezout entre d et $\varphi(n)$. On a alors $ed = 1 - v\varphi(n)$.

3.2 Sécurité

Pour craquer le système :

- factoriser n : connaissances de p et q et donc de d ;
- calculer $\varphi(n)$ sans factoriser n ? Impossible car $pq = n$ et $p + q = n + 1 - \varphi(n)$;
- pour authentifier: signature + message, ex : $(\text{Yves Robert})^d[n]$;

4 Pile ou face téléphonique

- A : p, q premiers et donne $n = pq$ à B;
- B : choisit x $[n]$ et envoie $r = x^2$ $[n]$ à A
- A calcule $r1 = r$ $[p]$ et ses racines dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ et $r2 = r$ $[q]$ et ses racines dans $\frac{\mathbb{Z}}{q\mathbb{Z}}$ et reconstruit $\pm w$ ou $\pm y$.

A envoie son résultat à B :

- si c'est x B a perdu;
- si c'est y B a gagné et A demande une preuve : B est connaissant x et y désormais est en mesure de trouver p et q (car $x^2 - y^2 \equiv 0$ $[n]$).

REMARQUE 2 Comment résoudre $x^2 \equiv a$ $[p]$ avec p premier. Un tel x existe ssi $a^{\frac{p-1}{2}} \equiv 1$ $[p]$.

Si $p \equiv 3$ $[4]$, $x = a^{\frac{p+1}{4}}$ marche.
Si $p \equiv 5$ $[8]$, $x = 2a(4a)^{\frac{p-5}{8}}$ marche.