Algorithme d'Euclide

$a_0 = a \quad \rightarrow \quad a_{i+1} = b_i$

$b_0 = b \quad\quad\quad b_{i+1} \equiv a_i \, mod(b_i)$

On s'arrête dès que $b_i = 0$ et le pgcd(a,b) sera égale à a_i ou b_{i-1} ($pgcd(a,b) = a \wedge b = a_i = b_{i-1}$)

Algorithme d'Euclide étendu

→ Permet de calculer les coefficient de Bézout : $\exists u, v \in \mathbb{Z}$ tel que $a \wedge b = u * a + v * b$

$u_0 = 1, u_1 = 0$
$v_0 = 0, v_1 = 1$
$r_0 = a, r_1 = b$

$i \geq 2 \quad r_i = u_i * a + v_i * b \quad tel\, que$
$u_i = u_{i-2} - q_{i-1} * u_{i-1}$
$v_i = v_{i-2} - q_{i-1} * v_{i-1}$
q_i est le $quotient$ de r_{i-1} par r_i
O, s'arrête dès que $r_i = 0$ et $u = u_{i-1}, v = v_{i-1}$ et $pgcd(a,b) = r_{i-1}$

Exemple $a = 243 \quad et \quad b = 198$

$u_0 = 1, v_0 = 0, r_0 = 243$
$u_1 = 0, v_1 = 1, r_1 = 198$ $\quad q_1 = 1 \quad (r_0 | r_1)$

itération $i = 2$ →
$$u_2 = u_0 - q_1 * u_1 = 1 - 1 * 0 = 1$$
$$v_2 = v_0 - q_1 * v_1 = 0 - 1 * 1 = -1 \qquad \text{et} \quad q_2 = 4 \quad (r_1 | r_2)$$
$$r_2 = u_2 * a + v_2 * b = 1 * 243 + (-1) * 198 = 45$$

itération $i = 3$
$$u_3 = u_1 - q_2 * u_2 = 0 - 4 * 1 = -4$$
$$v_3 = v_1 - q_2 * v_2 = 1 - 4 * (-1) = 5 \qquad \text{et} \quad q_3 = 2 \quad (r_2 | r_3)$$
$$r_3 = u_3 * a + v_3 * b = (-4) * 243 + 5 * 198 = 18$$

itération $i = 4$
$$u_4 = u_2 - q_3 * u_3 = 1 - 2 * (-4) = 9$$
$$v_4 = v_2 - q_3 * v_3 = (-1) - 2 * (5) = -11 \qquad \text{et} \quad q_4 = 2 \quad (r_3 | r_4)$$
$$r_4 = u_4 * a + v_4 * b = (9) * 243 + (-11) * 198 = 9$$

itération $i = 5$
$$u_5 = u_3 - q_3 * u_4 = (-4) - 2 * (9) = -22$$
$$v_5 = v_3 - q_3 * v_4 = (5) - 2 * (-11) = 27$$
$$r_5 = u_5 * a + v_5 * b = (-22) * 243 + (27) * 198 = 0$$

$r_5 = 0 \Rightarrow u = u_4 = 9 \quad , \quad v = v_4 = -11 \quad et \quad pgcd(243,198) = r_4 = 9$

Calcul efficace de $x^k mod(n)$

calculer d'abord $t = m^e$ et ensuite $t \, mod(n)$. → méthode est coûteuse en temps et en calcul

→ Mais on peut être beaucoup plus efficace. On remarque que toute puissance x^k peut en fait s'écrire comme un produit de puissances de la forme x^{2^l} : en effet, k peut s'écrire comme une somme d'entiers de la forme 2^l .

Exemple : $x^{13}=x^1\times x^4\times x^8$ et Il suffit alors de calculer successivement les x^{2^l} par des élévations au carré puis de multiplier ces puissances entre elles. Dans notre cas on utilise :

- 3 multiplications pour calculer successivement x^2 , x^4 et x^8
- 2 multiplications pour effectuer le produit de x^1 , x^4 et x^8

On effectue en tout 5 multiplications au lieu de 12.

→ **Décomposition d'un entier dans la base {0,1}:**

L'écriture d'un entier $k\in\mathbb{N}^*$ sera de la forme : $k=\sum_{l=0}^{p} k_l 2^l$ où les k_l sont des entiers compris entre 0 et 1

La méthode la plus efficace pour calculer l'exponentiation modulaire consiste alors à :

- Convertir l'exposant k en notation binaire.
- Puis on déduit la décomposition de k en somme de puissances de 2.
- On procède ensuite à des élévations au carré successives de x pour obtenir x^k

Exponentiation Rapide modulaire

1) On écrit le développement de l'exposant (k) en base 2 : $k=\sum_{l=0}^{p} k_l * 2^l$ avec $k_i\in\{0,1\}$
2) On calcule successivement le $x^{2^l} mod(n)$
3) On rassemble : $x^k=x^{\sum_{l=0}^{p} k_l*2^l}=\prod_{l=0}^{p}\left(x^{2^l}\right)^{k_l}$ car $x^{a+b}=x^a*x^b$ et $x^{a.b}=\left(x^a\right)^b$

Exemple : Calculer $5^{11} mod(14)$

11=8+2+1 donc $11=(1,1,0,1)$

$$5^{2^0} mod(14)\equiv 5 mod(14)$$
$$5^{2^1} mod(14)\equiv 25 mod(14)\equiv 11 mod(14)$$
$$5^{2^2} mod(14)\equiv 5^2*5^2 mod(14)\equiv 11*11 mod(14)\equiv 121 mod(14)\equiv 9 mod(14)$$
$$5^{2^3} mod(14)\equiv 5^8 mod(14)\equiv 5^4*5^4 mod(14)\equiv 9*9 mod(14)\equiv 81 mod(14)\equiv 11 mod(14)$$

$$5^{11}\equiv\left(5^{2^3}\right)^{(1)}+\left(5^{2^2}\right)^{(0)}+\left(5^{2^1}\right)^{(1)}+\left(5^{2^0}\right)^{(1)}\equiv 5*1*11*11 mod(14)\equiv 55*11 mod(14)$$

→ $5^{11}\equiv 13*11 mod(14)\equiv 143 mod(14)\equiv 3 mod(14)$

Exercice 1 : $p=17, q=11$

1. Trouver le plus grand e tel que $pgcd(e,\varphi(n))=1$
2. Calculer la clé privée RSA en utilisant l'algorithme de Euclide étendu
3. Chiffrer le message «fst» (Utiliser la table Ascii)

Solution : n=187 e=77 d=133

fst → 102 115 116 Donc le message M à chiffrer est 102 115 116 (m1,m2,m3)

$c_1=m_1^e mod(n)=102^{77} mod(187)=119$ $c_2=m_2^e mod(n)=115^{77} mod(187)=47$

$c_3=m_3^e mod(n)=116^{77} mod(187)=107$

Le chiffrement de M sera le message C = 119 047 107

Déchiffrement :

$m_1=c_1^d mod(n)=119^{133} mod(187)=102$

$m_2=c_2^d mod(n)=47^{133} mod(187)=115$ $m_3=c_3^d mod(n)=107^{133} mod(187)=116$ OK