**Notes**

- ElGamal est un système de sécurité qui ne dispose pas de brevet (contrairement au RSA par exemple).

- Le Théorème de Shoup permet d’affirmer que le logarithme discret nécessite opérations au moins. <http://perso.univ-rennes1.fr/christophe.ritzenthaler/cours/DLP.pdf>

-L’algorithme étendu d’Euclide est en O(log2(max(a,b))).

- Proposition 5.5. Soit n ≥ 2 et m ∈ Z. Les affirmations suivantes sont ´equivalentes :

(1) Les entiers m et n sont premiers entre eux ;

(2) L’´el´ement m engendre le groupe (Z/nZ, +) ;

(3) L’´el´ement m est inversible dans (Z/nZ, .).

(Source : <http://math.univ-lyon1.fr/capes/IMG/pdf/new.congruence.pdf> )

- Construction d’un élément générateur : Dans un premier temps, il faudrait pouvoir tester si un élément est générateur (c’est-à-dire d’ordre p −1). Pour cela on ne connaît pas actuellement d’autre moyen que de faire intervenir la factorisation de p − 1 en nombres premiers :

Théorème 2.5 : L’élément α est générateur si et seulement si pour tout 1 ≤ i ≤ k on a : .