# ALGORITHMIQUE DE BASE - TP N. 6

**Exercice 1 : Calcul d'un générateur de $\mathbb{F}_p$**
Soit $p \geq 3$ un nombre premier. Soit $p-1 = \prod_{i=1}^{n} l_i^{e_i}$ la décomposition en facteurs premiers de $(p-1)$.
Le but est d'écrire une fonction qui calcule un générateur de $\mathbb{F}_p^*$:

- Pour chaque $i$ on cherche $x_i$ (en le choisissant au hasard entre 1 et $p-1$) tel que $x_i^{(p-1)/l_i} \not\equiv 1 \mod p$ et on calcule $y_i = x_i^{(p-1)/(l_i^{e_i})}$.
- On aura que $x := \prod_{i=1}^{n} y_i \in \mathbb{F}_p$ est un générateur de $\mathbb{F}_p^*$.

**Exercice 2 : Racine carrée dans $\mathbb{F}_p$**
Soit $p$ un nombre premier, soit $F = \mathbb{F}_p$ le corps à $p$ éléments.
Soit $a \in F^*$. On cherche une racine carrée de $a$, si elle existe.

(1) Tout d'abord il faudra vérifier si $a$ est un carré ($\Leftrightarrow a^{(p-1)/2} \equiv 1 \mod p$).
(2) On pose $Q = T^{(p-1)/2} - 1$.
(3) Ensuite on choisit au hasard $x \in F^*$ et on calcule le polynôme $P = (T - x)^2 - a$
(4) On calcule $R = \gcd(P, Q) \in F[T]$ (pour le calculer rapidement, il faudra calculer $(Q \mod P) = (T^{(p-1)/2} - 1 \mod P)$ dans $F[T]$ par exponentiation rapide, puis calculer le pgcd avec $P$).
(5) Si $R$ est un polynôme de degré 1 on a fini, et on retourne $b + x$ où $b$ est le terme constant de $R$.
(6) Sinon on recommence au point (3).

**Exercice 3 : Racines d'un polynôme quelconque dans $\mathbb{F}_p$**
Soient $p, F$ comme dans l'exercice 2.
Soit $P(T) \in F[T]$ un polynôme quelconque. On cherche ses racines dans $F$.
On remarque tout d'abord que ses racines coïncident avec celles de $Q(T) = \gcd(P(T), T^p - T)$ et que le polynôme $Q(T)$ est scindé (remarque : si $Q = 1$ alors $P$ est irréductible dans $F$).
(Attention : pour calculer $Q(T)$ rapidement il faudra calculer $T^p \mod P(T)$ par exponentiation rapide, puis $T^p - T \mod P(T)$ puis le gcd.)
Par la suite, on va suivre la même stratégie que à l'Exercice 2 :

(1) On choisit au hasard $x \in F^*$.
(2) On calcule $V = Q(T - x)$.
(3) On pose $U = T^{(p-1)/2} - 1$.
(4) On calcule $R = \gcd(U, V)$ (même astuce que à l'Exercice 2).
(5) Si $R$ a degré $1 \leq d < (p-1)/2$ alors $R(T + x)$ est un facteur propre de $V$.
(6) Sinon, on repart au point (1).

On a vu comment trouver un facteur propre de $V$. Par récurrence, on pourra trouver un facteur linéaire, et donc une racine de $P(T)$.

---

*Date*: 2 décembre 2010.