

FEUILLE D'EXERCICES n° 10

Exercice 1 – [RACINES PRIMITIVES MOD p]

Soit $p > 2$ un nombre premier, on désire trouver une racine primitive modulo p , i.e. un $g \in \mathbb{F}_p^*$ d'ordre $p - 1$.

- 1) Supposons connue une racine primitive modulo p . Comment obtenir les autres ?
- 2) On tire g uniformément au hasard dans $[1, p - 1]$. Quelle est la probabilité que g convienne ?
- 3) On suppose dorénavant connue la factorisation $p - 1 = \prod_i \ell_i^{e_i}$, où les ℓ_i sont premiers et distincts. Montrer que $g \in \mathbb{F}_p^*$ est d'ordre $p - 1$ si et seulement si $g^{(p-1)/\ell_i} \neq 1$ pour tout i . On peut donc vérifier si un g explicite convient ou non. Quelle est la complexité binaire de cette vérification ?
- 4) Pour tout i , on désire maintenant trouver un g_i d'ordre $\ell_i^{e_i}$. On tire uniformément au hasard $h \in \mathbb{F}_p^*$ et on pose $g_i := h^{(p-1)/\ell_i^{e_i}}$.
 - a) Comment tester si g_i convient ?
 - b) Quelle est la complexité binaire du test ?
 - c) Quelle est la probabilité que g_i convienne ?
- 5) Montrer que dans un groupe abélien, si x et y ont des ordres m, n premiers entre eux, alors xy est d'ordre mn .
- 6) En déduire que $g := \prod_i g_i$ est bien d'ordre $p - 1$. Que dire de la complexité de cet algorithme ?

Exercice 2 – [AUTOUR DE POCKLINGTON-LEHMER]

Rappelons le théorème vu en cours.

Théorème. $n > 1$ est premier si et seulement si pour tout diviseur premier p de $n - 1$ il existe un entier a_p tel que

$$a_p^{n-1} \equiv 1 \pmod{n} \text{ et } \text{pgcd}(a_p^{(n-1)/p} - 1, n) = 1.$$

- 1) Supposons que $n - 1 = FU$ où $\text{pgcd}(F, U) = 1$, $F > \sqrt{n}$. Montrer que n est premier si et seulement si pour tout p premier divisant F il existe un entier a_p tel que

$$a_p^{n-1} \equiv 1 \pmod{n} \text{ et } \text{pgcd}(a_p^{(n-1)/p} - 1, n) = 1.$$

- 2) Supposons que $n - 1 = FU$ où $\text{pgcd}(F, U) = 1$. Supposons que tous les diviseurs premiers de U sont $> B$ avec $BF \geq \sqrt{n}$. Montrer que n est premier si et seulement si

- pour tout diviseur premier p de F il existe un entier a_p tel que

$$a_p^{n-1} \equiv 1 \pmod{n} \text{ et } \text{pgcd}(a_p^{(n-1)/p} - 1, n) = 1,$$

- et il existe un entier a tel que

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{et} \quad \text{pgcd}(a^F - 1, n) = 1.$$

Exercice 3 – [CANTOR-ZASSENHAUS EN CARACTÉRISTIQUE 2]

On rappelle l’algorithme de Cantor-Zassenhaus en caractéristique impaire.

Algorithme 1. Factorisation dans $\mathbb{F}_q[x]$.

Entrées: $q = p^k$, où p est un nombre premier impair, $Q \in \mathbb{F}_q[x]$ de degré n , produit de polynômes irréductibles deux à deux distincts de degré d .

Sorties: Un diviseur non trivial de Q , ou bien “échec”.

- 1) Tirer au hasard $A \in \mathbb{F}_q[x]$ de degré inférieur à n .
 - 2) Calculer $D = \text{pgcd}(A, Q)$. Si $D \neq 1$, sortir D .
 - 3) Calculer $B = A^{(q^d-1)/2} - 1 \pmod{Q}$
 - 4) Calculer $D = \text{pgcd}(B, Q)$. Si $D \neq 1$ et $D \neq Q$, sortir D . Sinon, sortir “échec”.
-

1) En appliquant cet algorithme, factoriser le polynôme $x^4 + x^3 + x - 1$ de $\mathbb{F}_3[x]$, en prenant $d = 2$ et $A = x - 1$.

2) Soit $m \geq 1$, et soit

$$T_m = x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^4 + x^2 + x \in \mathbb{F}_2[x].$$

- a) Montrer que $T_m(T_m + 1) = x^{2^m} + x$.
- b) En déduire que si $\alpha \in \mathbb{F}_{2^m}$, alors $T_m(\alpha) \in \mathbb{F}_2$.
- c) Montrer que l’application $\alpha \mapsto T_m(\alpha)$ de \mathbb{F}_{2^m} dans \mathbb{F}_2 est une application linéaire de \mathbb{F}_2 -espaces vectoriels. En déduire que les ensembles $\{\alpha \in \mathbb{F}_{2^m} : T_m(\alpha) = 0\}$ et $\{\alpha \in \mathbb{F}_{2^m} : T_m(\alpha) = 1\}$ ont même cardinal, soit 2^{m-1} .

Soient maintenant $q = 2^k$ et $Q \in \mathbb{F}_q[x]$ de degré n . On suppose que Q est produit de r polynômes irréductibles sur \mathbb{F}_q qu’on note P_1, \dots, P_r , deux à deux distincts et tous de même degré d . On note $R = \mathbb{F}_q[x]/(Q)$, $R_i = \mathbb{F}_q[x]/(P_i)$ et φ_i l’application canonique de R dans R_i définie par $\varphi_i(P \pmod{Q}) = P \pmod{P_i}$.

3) Soit $A \in R$. Montrer que $\varphi_i(T_{kd}(A)) = T_{kd}(\varphi_i(A))$. En déduire que $\varphi_i(T_{kd}(A)) \in \mathbb{F}_2$ et que si A est choisi au hasard dans R avec probabilité uniforme, $T_{kd}(A)$ appartient à \mathbb{F}_2 avec probabilité 2^{1-r} .

4) En déduire un algorithme pour factoriser Q et montrer que sa probabilité d’échec est inférieure à $1/2$.

Exercice 4 – [ALGORITHME DE BERLEKAMP : UN EXEMPLE SIMPLE]

Soit $f = x^4 + x^3 + x - 1 \in \mathbb{F}_3[x]$. On suppose qu’on a déjà calculé $\text{pgcd}(f, f') = 1$.

- 1) Le polynôme f a-t-il des racines dans \mathbb{F}_3 ? En déduire sans calculs $\text{pgcd}(f, x^3 - x)$.
- 2) Sachant cela, quelles sont les structures possibles de l’anneau $A = \mathbb{F}_3[x]/(f)$?
- 3) Soit F l’application de A dans lui-même qui à x associe x^3 . Écrire la matrice de $F - \text{Id}$ dans la base $1, x, x^2, x^3$ de A , et calculer son noyau N .

4) Prendre un élément a de ce noyau et calculer $\text{pgcd}(a, f)$, puis $\text{pgcd}(a - 1, f)$. Recommencer jusqu'à obtenir un facteur non trivial de f .

5) Vérifier que pour tout élément a de N et tout facteur irréductible g de f , il existe bien un entier k tel que

$$a \equiv k \pmod{g}.$$

Exercice 5 – [ALGORITHME DE BERLEKAMP : UN AUTRE EXEMPLE SIMPLE]

Soit $f = x^6 + 2x^5 + x^4 + 2x^3 + x - 1 \in \mathbb{F}_5[x]$. On suppose qu'on a déjà calculé que $\text{pgcd}(f, f') = 1$.

1) Le polynôme f a-t-il des racines dans \mathbb{F}_5 ? En déduire sans calculs $\text{pgcd}(f, x^5 - x)$.

2) Sachant cela, quelles sont les structures possibles de l'anneau $A = \mathbb{F}_5[x]/(f)$?

3) Soit F l'application de A dans lui-même qui à x associe x^5 . Écrire la matrice de $F - \text{Id}$ dans la base $1, x, \dots, x^5$ de A , et calculer son noyau N . On pourra utiliser sans démonstration les résultats suivants.

$$x^{10} \equiv -2x^5 + 2x^4 - x^3 - x^2 + x - 2 \pmod{f}$$

$$x^{15} \equiv -x^5 + 2x^4 - 2x^3 + 2x + 2 \pmod{f}$$

$$x^{20} \equiv -2x^5 + 2x^4 + x^3 + 1 \pmod{f}$$

$$x^{25} \equiv x \pmod{f}.$$

4) Combien f possède-t-il de facteurs irréductibles? Quel est leur degré?

5) Prendre un élément a de N et calculer $\text{pgcd}(a, f)$ et $\text{pgcd}(a^2 - 1, f)$. Recommencer jusqu'à obtenir un facteur non trivial de f .