TP3 - Corps finis et factorisation de polynômes

13 Novembre 2020

Les TPs comportent une partie à faire sur feuille (explicitement indiquée), ainsi qu'une partie implémentation.

L'objectif de ce TP est de manipuler les corps finis et de parler de l'agorithme de Berlekamp pour la factorisation de polynômes sur corps fini.

> Sur `sage`, vous pouvez obtenir la documentation d'une fonction/méthode en ajoutant un '?' à la fin, ou en tapant `help(cmd)`, où `cmd` est la commande en question.
> N'oubliez pas d'abuser de l'autocompletion pour prendre connaissance des méthodes disponibles sur un objet donné.

Notation. Soit $p \in \mathbb{Z}$ premier, soit $q = p^k$ pour un entier naturel k. On note :
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
- $\mathbb{F}_q \simeq \frac{\mathbb{F}_p[X]}{P}$ pour $P \in \mathbb{F}_p[X]$ irréductible de degré k.

Exercice 0 : Construction de corps fini

Considérons le corps fini $\mathbb{F}_8 \simeq \frac{\mathbb{F}_2[X]}{P}$.

1. Quelles sont les valeurs possibles de P ?
2. Pour chaque valeur de P, en considérant α une racine primitive dans $\mathbb{F}_8$, listez les éléments de $\mathbb{F}_8$.
3. Justifiez que ces corps sont isomorphes, construisez l'isomorphisme correspondant.

Exercice 1 : Propriétés de corps finis

1. Soit K un corps fini à q élements. Montrez que pour $a \in K/\{0\}$, on a $a^q = a$.
2. L'application $\phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $\phi(a) = a^p$ est appelé *application de Frobenius*. Montrez que cette application est un morphisme de corps.
3. Montrez que l'ensemble des points fixes de $\phi_2 : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$, $\phi(a) = a^q$ est un sous-corps de $\mathbb{F}_{q^n}$ à q éléments, autrement dit :
$$\{x \in \mathbb{F}_{q^n}, x^q = x\} \simeq \mathbb{F}_q$$

Exercice 2 : Partie sans carré

Soit F un corps. Un polynôme $P \in F[X]$ est dit *sans carré* si il n'est divisible par le carré d'aucun polynôme non constant sur F, ou de manière équivalente, s'il ne possède que des racines simples dans tous les corps contenant F. En particulier, ce résultat est valable pour $F = \mathbb{F}_p$.
Par exemple, si on note $P(X) = (X+1)(X+2)(X+3)^2(X+4)^2(X+5)^3$, alors :
- La *partie sans carré* de P est $(X+1)(X+2)(X+3)(X+4)(X+5)$
- La *décomposition sans carré* de P est $\{[(X+1)(X+2), 1], [(X+3)(X+4), 2], [(X+5), 3]\}$.

1. Soit $P \in \mathbb{F}_p[X]$, montrez que la dérivée $P' = 0 \Leftrightarrow P = Q^p$.
2. Montrez que $P \in \mathbb{F}_p[X]$ est sans carré $\Leftrightarrow \text{pgcd}(P, P') = 1$.

Exercice 3 : Algorithme de Berlekamp

Soit $P = P_1 \cdot P_2 \cdots P_r \in \mathbb{F}_p[X]$ un polynôme de degré n, sans carré. On peut factoriser P en éléments distincts et irréductibles P_i à l'aide d'un algorithme déterministe en $\mathcal{O}(n^w + nM(n)\log(n)p)$ opérations, avec M un fonction de multiplication, et w l'exposant de l'algèbre linéaire sur $\mathbb{F}_p$.

1. Notons $\Phi : \mathbb{F}_p[X]/P \longrightarrow \mathbb{F}_p[X]/P$, $\Phi(a) = a^p - a$ l'application de Berlekamp. Montrez que cette application est $\mathbb{F}_p$-linéaire.
2. Soit $a \in \mathbb{F}_p[X]$ tel que $deg(a) \in [1, deg(P) - 1]$ et $a \in \ker \Phi$. Montrez qu'on a les deux propriétés suivantes :
   — pour $i \in [1, r]$, $a_i = (a \bmod P_i) \in \mathbb{F}_p$
   — ces constantes ne sont pas toutes égales.
   (a) Construisez un isomorphisme $f : \mathbb{F}_p[X]/P \longrightarrow \mathbb{F}_p[X]/P_1 \times \cdots \times \mathbb{F}_p[X]/P_r$ et décrivez
   $$\Phi : \mathbb{F}_p[X]/P_1 \times \cdots \mathbb{F}_p[X]/P_r \longrightarrow \mathbb{F}_p[X]/P_1 \times \cdots \mathbb{F}_p[X]/P_r$$
   (b) En rappelant que sur un corps K, $X^p - X = \prod_{a \in K}(X - a)$, montrez que les a_i sont constants.
   (c) Montrez la seconde propriété.
3. Montrez que $\exists b \in \mathbb{F}_p$ tel que $d = pgcd(P, a - b)$ est un diviseur non trivial de P.
4. Implémentez l'algorithme de Berlekamp décrit ci-dessous.
   (a) Factorisez $P = X^7 + X^5 + X^3 + X^2 + 1$ sur $\mathbb{F}_2$.
   (b) Factorisez $P = X^{10} + 86 * X^9 + 19 * X^8 + 35 * X^7 + 67 * X^6 + 67 * X^5 + 61 * X^4 + 39 * X^3 + 14 * X^2 + 51 * X + 7$ sur $\mathbb{F}_{101}$.
   Vous pouvez vérifier vos résultats avec la méthode `factor` de sage.

Algorithme 1 : `BerlekampFactor`(P)

```
1  if degP < 1 then
2  |  return P;
3  end
4  else if P' == 0 then
5  |  Calucler Q tel que P = Q^p;
6  |  return BerlakempFactor(Q);
7  end
8  else
9  |  U = gcd(P, P');
10 |  if U ≠ 1 then
11 |  |  return BerlakempFactor(P/U);
12 |  end
13 |  else
14 |  |  Calculer la matrice M = Mat(Φ) = Mat(φ) − Id ∈ M_d dans la base (1, X, ··· , X^{d−1}) ;
15 |  |  Calculer un base B de ker M ;
16 |  |  if dim(B) == 1 then
17 |  |  |  return P;
18 |  |  end
19 |  |  else
20 |  |  |  Choisir un élément non constant Q ∈ B ;
21 |  |  |  return ⋃_{α∈F_p} BerlekampFactor(pgcd(P, Q − α)) ;
22 |  |  end
23 |  end
24 end
```