1 TD

Exercice 1 Déterminer les racines dans $\mathbb{Z}/p\mathbb{Z}$ de $P = x^4 + x + 1$ pour $p = 5$ et $p = 7$. Estimer le cout.

Exercice 2 Soit P le polynôme $x^4 + 13x + 1$. P est-il squarefree pour $p = 7$? $p = 11$?

Exercice 3 Soit P et Q deux polynômes à coefficients entiers. Montrer que pour tout nombre premier p ne divisant pas les coefficients dominants de P et Q, le degré du pgcd de P et Q dans $\mathbb{Q}[X]$ est inférieur ou égal au degré du pgcd de P et Q dans $\mathbb{Z}/p\mathbb{Z}[X]$. En déduire le PGCD de $x^4 + x + 1$ et $x^3 + 7x^2 + 7x + 1$.

Exercice 4 Soit $P = x^3 + x + 1$. Déterminer l'inverse de $3x^2 + x + 1$ dans $\mathbb{Z}/11\mathbb{Z}[x]/P$

Exercice 5 Soit P le polynôme $x^4 + x + 2$. P est-il irréductible modulo 3 ?

Exercice 6 Estimer le cout d'un test d'irréductibilité en fonction du degré du polynôme [et de la taille de p]. Déterminer le cout moyen de construction d'un polynôme irréductible de degré n modulo p.

Exercice 7

1. Déterminer un polynôme de degré 4 irréductible modulo 2. Utiliser ce polynôme pour générer la table d'addition d'un corps K=GF(2,4).
2. Déterminer un générateur g de votre corps*, et construire la table des puissances. En déduire une méthode rapide pour multiplier, inverser, calculer une racine carrée dans le corps K.
3. Résoudre dans K les équations $x^2 + x + 1 = 0$, $x^2 + gx + g^2 + g + 1 = 0$, $x^2 + gx + 1 = 0$..

Exercice 8 Pour multiplier deux polynômes $P = a_n X^n + ... + a_0$ et $Q = b_m X^m + ... + b_0$ à coefficients dans un corps $K = GF(p, d)$ extension de $\mathbb{Z}/p\mathbb{Z}$, on se ramène au produit de deux polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Soit $M \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme irréductible de degré d utilisé pour représenter les éléments du corps K. On pose :

$$p = a_n(X)X^{2nd} + ... + a_0(X), \quad q = b_m(X)X^{2md} + ... + b_0(X)$$

où les a_k, b_k sont des polynômes de $\mathbb{Z}/p\mathbb{Z}[X]$ de degré $\leq d-1$. On effectue le produit pq à l'aide d'un algorithme de multiplication efficace, à base de FFT. On décompose par paquets de degré de $2d$ en $2d$, $pq = c_{n+m}(X)X^{2(n+m)d} + ... + c_0(X)$ avec degré de c_k au plus $2d - 2$.
Comment obtient-on PQ en fonction des c_k ? Quelle est la complexité de cet algorithme ?

Exercice 9 Effectuer le produit de $x^2 + 2x - 1$ et $2x + 1$ par FFT dans $\mathbb{Z}/5\mathbb{Z}[x]$.

Exercice 10 Déterminer la factorisation square-free de $x^7 + x^6 + x + 1$ modulo 2.

Exercice 11 Factoriser $x^5 - x^4 + x^3 - x^2 - 1$ modulo 3.

Exercice 12 Déterminer une racine carrée de 5 modulo 101 en utilisant l'algorithme de Cantor-Zassenhauss. Quel est le cout de la recherche d'une racine carrée par cette méthode modulo un premier $p = 1 \pmod 4$?
Déterminer la factorisation de $x^2 + 3x + 7$ mod 101 sans chercher les racines de manière systématique.

Exercice 13 Soit $A = x^4 + 1$ modulo $p = 3$. Vérifier qu'il possède 2 facteurs de degré $d = 2$. Le factoriser en cherchant le PGCD de A avec $T^{(p^d-1)/2} - 1$ où T est un polynôme aléatoire de degré $2d - 1 = 3$.

2 TP

Exercice 0 Vérifier/faire les parties calculatoires des exercices de TD.

Exercice 1 Implémenter l'algorithme de Hörner pour évaluer un polynome en un point. Modifier l'algorithme pour calculer le quotient. Écrire une fonction qui renvoie les facteurs de degré 1 d'un polynôme dans $\mathbb{Z}/p$ pour p premier.

Exercice 2 Écrire une fonction renvoyant 1 si un polynôme est squarefree modulo p. Prolongement : renvoyer une factorisation partielle du polynôme (algorithme de Musser ou de Yun pour une factorisation squarefree).

Exercice 3 Écrire une fonction testant si un polynôme est irréductible modulo p. Utiliser cette fonction pour construire un polynôme irréductible de degré n modulo p puis une représentation du corps fini GF(p, n)

Exercice 4 Déterminer les degrés des facteurs de $x^7 + x^5 + 2x^4 + x^3 + x^2 + 2x + 1$ modulo 5 et 7 (sans utiliser la commande factor). Quelle est la factorisation sur $\mathbb{Q}$ de ce polynôme ?

Exercice 5 Écrire une fonction renvoyant la factorisation ddf (distinct degree factorization) d'un polynôme squarefree modulo p. Tester sur l'exemple de l'exercice précédent.

Exercice 6 Implémenter le corps à 256 éléments de manière efficace (en utilisant un entier 8 bits et une table).

Exercice 7 Trouver des nombres premiers $p < 2^{31}$ de la forme $1 + k2^{25}$. Déterminer une racine primitive 2^{25}-ième de l'unité pour p. A quelle condition peut-on calculer le produit de deux polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ par FFT ? Le faire sur un exemple en utilisant l'instruction `fft` avec 3 arguments.
Soit $n < 2^{31}$. Montrer qu'on peut effectuer un produit de polynômes dont la somme des degrés est $< 2^{25}$ sur $\mathbb{Z}/n\mathbb{Z}$ en utilisant au plus 3 nombres premiers p de ce type et 3 produits par FFT. En déduire une méthode de multiplication de polynômes à coefficients entiers par FFT.