1 TD

Exercice 1 Calculez le pgcd de $x^{202} + x^{101} + 1$ et sa dérivée modulo 3 et modulo 5. Conclusion ?

Exercice 2 Soit $P = 51x^3 - 35x^2 + 39x - 115$ et $Q = 17x^4 - 23x^3 + 34x^2 + 39x - 115$ dans $\mathbb{Q}[X]$. Calculez le pgcd de P et Q modulo 5, 7 et 11. En déduire le pgcd de P et Q par le théorème des restes chinois. Que se passe-t-il modulo 17 ?

Exercice 3 Déterminer le PGCD de $x^4 + x + 1$ et $x^3 + 7x^2 + 7x + 1$ dans $\mathbb{Q}[X]$.

Exercice 4 Soit P le polynôme $x^4 + 13x + 1$. P est-il squarefree modulo p pour $p = 7$? $p = 11$? P est-il squarefree dans $\mathbb{Q}[X]$?

Exercice 5 Déterminer la factorisation square-free de $x^7 + x^6 + x + 1$ modulo 2.

Exercice 6 Factoriser $x^5 - x^4 + x^3 - x^2 - 1$ modulo 3 et modulo 5 en utilisant uniquement le PGCD. En déduire la factorisation sur $\mathbb{Q}[X]$.

2 TP

Exercice 1 Écrire un programme qui détermine le degré probable du pgcd de 2 polynômes en une variable en utilisant le pgcd modulaire (on considère le degré probable déterminé lorsqu'on trouve deux nombres premiers réalisant le minimum des degrés trouvés)

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 $\mathrm{GF}(p, n)$

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 En utilisant uniquement l'instruction de calcul de PGCD déterminer la multiplicité maximale d'un facteur irréductible de $x^{14} - x^{13} - 14x^{12} + 12x^{11} + 78x^{10} - 54x^9 - 224x^8 + 116x^7 + 361x^6 - 129x^5 - 330x^4 + 72x^3 + 160x^2 - 16x - 32 \in \mathbb{Q}[x]$ Réaliser ensuite une factorisation partielle de ce polynôme.

Exercice 7 Implémenter l'algorithme de Hörner pour évaluer un polynome en un point. Écrire une fonction qui renvoie les facteurs de degré 1 d'un polynôme P dans $\mathbb{Z}/p$ pour p premier (pas trop grand) en testant.
Amélioration : on pourra calculer $x^p \pmod{p, P}$ puis le pgcd de $x^p - x$ et P modulo p pour diminuer le degré du polynôme à tester.