

	<p style="text-align: center;"><b>ANNÉE UNIVERSITAIRE 2024/2025</b></p> <p style="text-align: center;"><b>4TMA701U Calcul Formel</b></p> <p style="text-align: center;"><b>Examen terminal session 1</b></p> <p style="text-align: center;"><b>Date : 11/12/2024    Heure : 9h30    Durée : 3h</b></p> <p style="text-align: center;">Documents autorisés</p>	<p style="text-align: center;">Collège Sciences et Technologies</p>
--	---	---

Vous rendrez à la fin de l'examen une copie papier ainsi qu'un fichier sage contenant vos programmes (lisible, commenté et nettoyé si possible..) au format EX-Nom-Prenom.ipynb (feuille Jupyter) ou EX-Nom-Prenom.sage (fichier texte). Le fichier est à envoyer par e-mail à l'adresse christine.bachoc@u-bordeaux.fr

**Exercice 1** Soit  $p$  un nombre premier. Soit  $P(X) = \sum_{i=0}^k a_i X^i \in \mathbb{Z}[X]$ . On suppose dans tout ce qui suit qu'il existe un entier  $r$  tel que  $P(r) \equiv 0 \pmod{p}$  et  $P'(r) \not\equiv 0 \pmod{p}$  (ici  $P'(X)$  est le polynôme dérivé de  $P$ ).

Le but de l'exercice est de calculer pour tout  $n \geq 1$  un entier  $r_n$ , tel que  $r_n \equiv r \pmod{p}$  et  $P(r_n) \equiv 0 \pmod{p^n}$ . On dit que  $r_n$  est un *relèvement modulo  $p^n$  de la racine  $r$  de  $P$  modulo  $p$* .

1. Dans cette question, on calcule  $r_2$ .

- a) Justifiez l'existence d'un entier  $t$  tel que  $r_2 = r + tp$ , puis montrez que pour tout  $i \geq 1$ ,  $(r + tp)^i \equiv r^i + ir^{i-1}tp \pmod{p^2}$ .
- b) En déduire que  $P(r + tp) \equiv P(r) + P'(r)tp \pmod{p^2}$ .
- c) Soit  $b \in \mathbb{Z}$  tel que  $P(r) = bp$ . Soit  $c$  l'inverse de  $P'(r)$  modulo  $p$ . Justifiez l'existence de  $b$  et  $c$ , puis montrez que  $t \equiv -bc \pmod{p}$ .

2. Implémentation et application numérique

- a) Écrire dans Sage une fonction RELEVEMENT qui exécute le calcul de la question 1. Cette fonction prendra en entrées  $P(X)$ ,  $p$ ,  $r$ , tels que  $P(r) \equiv 0 \pmod{p}$  et  $P'(r) \not\equiv 0 \pmod{p}$  et sort un entier  $r_2$ ,  $0 \leq r_2 < p^2$  tel que  $r_2 \equiv r \pmod{p}$  et  $P(r_2) \equiv 0 \pmod{p^2}$ .
- b) Soit  $P(X) = X^{10} - X + 1 \in \mathbb{Z}[X]$  et  $p = 11$ . Calculer dans  $\mathbb{F}_{11}[X]$  le pgcd de  $P(X)$  et de  $X^{11} - X$  et en déduire que  $r = 2$  est l'unique racine modulo 11 de  $P(X)$  (justifiez votre réponse).
- c) Utilisez votre fonction RELEVEMENT pour calculer une racine de  $P$  modulo  $11^2$  qui relève  $r = 2$  et vérifiez le résultat.

3. Généralisation

- a) Inspirez-vous de la question 1 pour calculer  $r_{2^i}$  à partir de  $r_i$  pour tout  $i \geq 1$ .
- b) En déduire l'unique racine modulo  $11^7$  de  $X^{10} - X + 1$  (vous devriez pouvoir appliquer votre fonction RELEVEMENT itérativement sans modifications..)

**Exercice 2** Soit  $F = \mathbb{Z}/17\mathbb{Z}$  et soit  $P \in F[x]$  le polynôme de degré 23 dont les coefficients rangés par degré croissant sont :

$$[1, 0, 0, 15, 6, 8, 9, 3, 7, 14, 7, 1, 5, 14, 7, 2, 15, 4, 9, 11, 2, 4, 15, 1]$$

Le but de l'exercice est de factoriser  $P$ .

1. Calculez dans Sage les polynômes  $D_i = \text{pgcd}(P, x^{17^i} - x)$  pour  $i = 1, 2, 3, 6$ .
2. Expliquez pourquoi  $D_2$  divise  $D_6$ .
3. Soit  $Q = D_6/D_2$ . Expliquez pourquoi  $Q$  est le produit de trois polynômes irréductibles de degré 6 deux à deux distincts.
4. Calculez les diviseurs irréductibles de  $Q$  avec l'algorithme de Cantor-Zassenhaus, en expliquant ses étapes.
5. Donnez la factorisation complète de  $P$ .

**Exercice 3** Soit  $f = x^3 - xy - 4x + y^2 + 2y$  et  $g = x^2 + y^2 - 4$  deux polynômes de  $\mathbb{Q}[x, y]$ . Soit  $I$  l'idéal de  $\mathbb{Q}[x, y]$  engendré par  $f$  et  $g$ . On munit  $\mathbb{Q}[x, y]$  de l'ordre lexicographique tel que  $x > y$ .

1. Montrez à la main que  $(f, g)$  n'est pas une base de Groebner de  $I$ .
2. Soit  $B$  la base de Groebner réduite de  $I$ , calculez  $B$  avec Sage.
3. A l'aide de cette base, calculez les solutions dans  $\mathbb{R}^2$  du système suivant (vous expliquerez votre raisonnement).

$$\begin{cases} x^3 - xy - 4x + y^2 + 2y = 0 \\ x^2 + y^2 = 4 \end{cases}$$

4. Donnez une base du  $\mathbb{Q}$ -espace vectoriel  $\mathbb{Q}[x, y]/I$ . Quelle est la dimension de ce quotient ?