

Université de BORDEAUX	ANNEE UNIVERSITAIRE 2014/2015 Examen première session	Collège Sciences et technologies
	Master 1 Code UE : MSIN820, MSMA820 Epreuve : Algèbre et calcul formel Date : 22/04/2015 Heure : 8h00 Durée : 3h Documents autorisés : Feuilles d'exercices (énoncés). Epreuve de M. Jehanne	

Exercice 1

1. Soit m un entier naturel supérieur ou égal à 2. Déterminer le polynôme Q de $\mathbb{Z}[x]$ tel que

$$x^m - 1 = (x - 1)Q(x).$$

2. Montrer que si $2^n - 1$ est premier, alors n est premier.

On appelle *nombre de Mersenne* tout nombre de la forme $M_n = 2^n - 1$ où n est un nombre premier. On appelle *nombre premier de Mersenne* un nombre de Mersenne qui est premier.

3. Soit n un entier impair. On pose $L_1 = 4$ et on définit par récurrence la suite $(L_i)_{i \geq 1}$ en posant $L_{i+1} = L_i^2 - 2$ pour tout $i \geq 1$. On suppose que $L_{n-1} \equiv 0 \pmod{M_n}$. Il s'agit dans les questions qui suivent de montrer que M_n est premier.

- a) Soit p le plus petit diviseur premier de M_n . Soit $P = x^2 - 4x + 1$ dans $\mathbb{F}_p[x]$. On note α et β les racines de P dans \mathbb{F}_{p^2} . Que valent $\alpha + \beta$ et $\alpha\beta$?

- b) Montrer par récurrence sur i que l'image de L_{i+1} dans \mathbb{F}_p est égale à $\alpha^{2^i} + \beta^{2^i}$ pour tout $i \geq 0$.

- c) Montrer que $\alpha^{2^{n-1}} = -1$. En déduire l'ordre de α .

- d) Montrer que M_n est premier.

4. [Application sur machine] On admet que la réciproque est vraie, c'est-à-dire que M_n est premier si et seulement si $L_{n-1} \equiv 0 \pmod{M_n}$.

- a) En utilisant ce résultat, écrire sur machine une fonction Mersenne qui étant donné un nombre premier impair n détermine si M_n est premier (pour $n = 19937$, la fonction doit donner le résultat en quelques secondes).

- b) Écrire une fonction Liste_Mersenne qui prend en entrée un entier naturel N et rend en sortie les N plus petits nombres premiers impairs n tels que M_n est premier (en utilisant la fonction Mersenne).

Exercice 2

Soit p un nombre premier.

1. a) Soit P un polynôme de $\mathbb{F}_p[x]$. Rappeler sans démonstration quel calcul de pgcd permet d'obtenir le produit des facteurs unitaires de degré 1 de P .

Nous avons vu comment on peut alors factoriser le polynôme obtenu, ce qui permet de calculer toutes les racines de P dans \mathbb{F}_p .

- b) Donner le résultat de ce pgcd dans le cas où $P = x^{10} - x + 1$ et $p = 11$ (on fera le calcul sur sage et on notera le résultat sur papier). En déduire que l'unique racine de ce polynôme P dans \mathbb{F}_{11} est 2.

Dans la suite de l'exercice, on considère un polynôme P de $\mathbb{Z}[x]$, et on s'intéresse aux racines de P dans $\mathbb{Z}/p^n\mathbb{Z}$, où n désigne un entier naturel non nul.

2. Soit donc $P \in \mathbb{Z}[x]$. Soit r un élément de \mathbb{Z} tel que $P(r) \equiv 0 \pmod{p^n}$. Que vaut $P(r) \pmod{p}$?

Réciproquement, soit r un entier tel que

$$P(r) \equiv 0 \pmod{p}.$$

Dans les questions suivantes, on suppose pour simplifier que

$$\text{pgcd}(P'(r), p) = 1$$

et on cherche à calculer un entier r_n tel que

$$r_n \equiv r \pmod{p} \quad \text{et} \quad P(r_n) \equiv 0 \pmod{p^n}.$$

3. Soient x, t, k et i des entiers tels que $k > 0$ et $i \geq 0$. Montrer que

$$(x + tp^k)^i \equiv x^i + itp^k x^{i-1} \pmod{p^{2k}}.$$

En déduire que

$$P(x + tp^k) \equiv P(x) + tp^k P'(x) \pmod{p^{2k}}.$$

4. On suppose avoir trouvé un entier r_k qui vérifie $r_k \equiv r \pmod{p}$ et $P(r_k) \equiv 0 \pmod{p^k}$ (donc p^k divise $P(r_k)$). Montrer qu'il existe un entier t_k tel que

$$\frac{P(r_k)}{p^k} + t_k P'(r_k) \equiv 0 \pmod{p^k},$$

et que cet entier est unique modulo p^k .

5. Soit alors $r_{2k} = r_k + t_k p^k$. Montrer que $r_{2k} \equiv r \pmod{p}$ et $P(r_{2k}) \equiv 0 \pmod{p^{2k}}$.

6. En utilisant l'algorithme que suggèrent les questions précédentes, calculer les racines de $x^3 + x + 1$ modulo 81 : on commencera par trouver à la main les racines modulo 3, puis on détaillera sur papier le calcul de chacun des t_k et r_k .

7. Écrire sur machine une fonction Relevement qui en entrée prend un nombre premier p , un entier naturel non nul n , un polynôme P de $\mathbb{Z}[x]$ et un entier r tel que $P(r) \equiv 0 \pmod{p}$ et $P'(r) \not\equiv 0 \pmod{p}$, et qui en sortie rend un entier s congru à r modulo p tel que $P(s) \equiv 0 \pmod{p^n}$.

8. En utilisant cette fonction, calculer l'unique racine de $x^{10} - x + 1$ modulo 11^7 .

Exercice 3

Soit K un corps et soient I et J deux idéaux de $K[X_1, \dots, X_n]$. On suppose que I et J sont tous deux donnés par une famille finie de générateurs, et l'on voudrait pouvoir calculer une famille de générateurs de l'idéal $I \cap J$. Pour cela, on va introduire une variable supplémentaire T , et l'on considérera $K[X_1, \dots, X_n]$ comme un sous anneau de $K[X_1, \dots, X_n, T]$.

1. Soit

$$\mathcal{R}(I, J) = \{Tg + (1 - T)h \in K[X_1, \dots, X_n, T] : g \in I, h \in J\}.$$

Montrer que $\mathcal{R}(I, J)$ est un idéal de $K[X_1, \dots, X_n, T]$.

2. Montrer que

$$I \cap J = \mathcal{R}(I, J) \cap K[X_1, \dots, X_n].$$

3. Soit $\{g_1, \dots, g_r\}$ (resp. $\{h_1, \dots, h_s\}$) une famille génératrice de I (resp. J). Montrer que $\mathcal{R}(I, J)$ est l'idéal de $K[X_1, \dots, X_n, T]$ engendré par

$$\{Tg_1, \dots, Tg_r\} \cup \{(1 - T)h_1, \dots, (1 - T)h_s\}.$$

4. Dédurre des questions précédentes une méthode pour calculer une base de Gröbner de $I \cap J$ et appliquer cette méthode au calcul de $I \cap J$ dans le cas où $I = \langle x^2 + y^3 - 1, x - xy + 3 \rangle$ et