université de BORDEAUX	**ANNEE UNIVERSITAIRE 2020/2021** **Examen première session** **Master 1 Code UE : 4TMA801U, 4TCY801S** **Epreuve : Algèbre et calcul formel** **Date : 5/05/2021 Heure : 9h00 Durée : 3h** Documents autorisés Epreuve de M. Jehanne	**Collège Sciences et technologies**

En fin d'énoncé, quelques commandes sage sont rappelées.

Comme toujours, il vous est demandé de justifier vos résultats avec précision.

Exercice 1

Soit q un nombre premier impair.

1. Soit f l'homomorphisme de groupes de $\mathbb{F}_q^*$ dans $\mathbb{F}_q^*$ qui à x associe $f(x) = x^2$. Soit $(\mathbb{F}_q^*)^2 = \mathrm{Im} f = \{x^2 \ : \ x \in \mathbb{F}_q^*\}$ l'ensemble des carrés de $\mathbb{F}_q^*$.

a) Montrer que $\ker f = \{-1, 1\}$. En déduire que card $(\mathbb{F}_q^*)^2 = \dfrac{q-1}{2}$.

b) Montrer que pour tout $x \in \mathbb{F}_q^*$, $x^{\frac{q-1}{2}} = 1$ ou -1. On pose

$$E_1 = \{x \in \mathbb{F}_q^* \ : \ x^{\frac{q-1}{2}} = 1\} \quad \text{et} \quad E_{-1} = \{x \in \mathbb{F}_q^* \ : \ x^{\frac{q-1}{2}} = -1\}$$

c) Montrer que $(\mathbb{F}_q^*)^2 \subset E_1$. En déduire que $E_1 = (\mathbb{F}_q^*)^2$ et $E_{-1} = \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$.

2. Soit n un entier composé (c'est-à-dire non premier et supérieur à 2). On pose

$$M(n) = \{x \in (\mathbb{Z}/n\mathbb{Z})^* \ : \ x^{n-1} = 1\}$$

On a vu en TD que si n n'est pas de Carmichaël, alors card $M(n) \leq \varphi(n)/2$, où $\varphi(n) =$ card $(\mathbb{Z}/n\mathbb{Z})^*$. On a vu aussi que $M(15) = \varphi(15)/2 = 4$. Nous allons trouver d'autres entiers n qui vérifient cette égalité $M(n) = \varphi(n)/2$.

a) Écrire sur sage une fonction qui prend en entrée un nombre premier p et rend en sortie `true` si $q = 2p - 1$ est premier et `false` sinon. Utiliser ensuite cette fonction pour trouver les 10 plus petits couples de tels nombres premiers (p, q) (inutile de les écrire sur votre copie). On pourra utiliser les fonctions `is_prime` et `next_prime`.

Soit $(p, q) = (p, 2p - 1)$ un couple de nombres premiers. On pose $n = pq$.

b) Montrer que $n - 1 = (p - 1)(2p + 1)$. En déduire que pour tout $x \in \mathbb{F}_p^*$, $x^{n-1} = 1$ et que pour tout $x \in \mathbb{F}_q^*$, $x^{n-1} = x^{\frac{q-1}{2}} \in \{-1, 1\}$.

c) En utilisant le théorème des restes chinois et le **1**, montrer que $M(n) = \varphi(n)/2$.

d) Soit $p = 1000249$. On prend au hasard des éléments de $\mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ avec une loi uniforme. Quelle est la probabilité qu'un tel élément ne soit pas inversible ? Vérifier sur sage que sur 1000 essais, le nombre d'éléments appartenant à $M(n)$ est proche de 500 (en élevant chacun de ces éléments à la puissance $n - 1$). Attention à ne pas faire de grosses exponentiations dans $\mathbb{Z}$.

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.

b) Soit $P(x) = x^{16} - x + 1 \in \mathbb{F}_{17}[x]$ En calculant sur sage le pgcd du **a)**, vérifier que 2 est l'unique racine de P dans $\mathbb{F}_{17}$.

2. Dans la suite de l'exercice, on considère un polynôme P de $\mathbb{Z}[x]$, et on cherche à calculer les racines de P dans $\mathbb{Z}/p^n\mathbb{Z}$, où n désigne un entier naturel non nul. On cherche donc à calculer les entiers r tels que $P(r) \equiv 0 \mod p^n$.

Si r est un tel entier, que vaut $P(r) \mod p$?

3. Réciproquement, soit r un entier tel que $P(r) \equiv 0 \mod p$. On considère le cas particulier où

$$P'(r) \not\equiv 0 \mod p \tag{1}$$

et on cherche à calculer un entier r' tel que $r' \equiv r \mod p$ et $P(r') \equiv 0 \mod p^n$.

L'algorithme `Relevement` suivant résout ce problème.

Si a et b sont des entiers tels que $b \neq 0$, on note $\mathrm{rem}(a, b)$ le reste de la division de a par b.

Algorithm 1. Relevement

Entrées: p : nombre premier, P : polynôme de $\mathbb{Z}[x]$, r : entier tel que $P(r) \equiv 0 \mod p$, n : élément de $\mathbb{N} \setminus \{0, 1\}$

Sorties: Un entier r' tel que $r' \equiv r \mod p$ et $P(r') \equiv 0 \mod p^n$

1: $i = 1$, $q = p$, $a = \mathrm{rem}(r, p)$
2: Tant que $i < n$:
3: $\quad s =$ entier tel que $sP'(a) \equiv 1 \mod q$
4: $\quad t = \mathrm{rem}\left(-s\dfrac{P(a)}{q}, q\right)$
5: $\quad a = r + tq$
6: $\quad q = q^2$, $i = 2i$
7: Sortir $\mathrm{rem}(a, p^n)$

Soient i_k et q_k les valeurs respectives de i et q lors du k-ème passage au pas 5. Montrer que $i_k = 2^{k-1}$ et $q_k = p^{2^{k-1}}$. La preuve de l'algorithme est l'objet de la question **7**.

4. Soit $P(x) = x^3 + x + 1$. Calculer $P(0)$, $P(1)$ et $P(2)$ modulo 3 pour trouver r_0 tel que $P(r_0) \equiv 0 \mod 3$, puis expliquer sur papier le calcul de t_0, puis de r_1, où les t_k et r_k sont les valeurs successives de t et r dans `Relevement` (l'entier r_1 doit donc vérifier les congruences $r_1 \equiv r_0 \mod 3$ et $P(r_1) \equiv 0 \mod 9$).

5. Écrire sur sage la fonction `Relevement`.

6. En utilisant **1. b)** et `Relevement`, calculer l'unique racine de $x^{16} - x + 1$ modulo 17^7.

7. a) Suivant la formule de Taylor pour les polynômes, rappeler ce que vaut $P(x + h)$ en fonction des dérivées successives de P évaluées en x (on notera $d = \deg P$).

Soient a, t, m des entiers tels que $m > 0$. Montrer que

$$P(a + tp^m) \equiv P(a) + tp^m P'(a) \mod p^{2m}$$

b) Soit k un entier tel que $k \geq 0$. On suppose avoir trouvé un entier r_k qui vérifie $r_k \equiv r \mod p$ et $P(r_k) \equiv 0 \mod p^{2^k}$. Expliquer pourquoi la condition (1) assure que $P'(r_k)$ est premier à p^{2^k}. En déduire qu'il existe un entier t_k unique modulo p^{2^k} tel que

$$\frac{P(r_k)}{p^{2^k}} + t_k P'(r_k) \equiv 0 \mod p^{2^k}$$

Soit alors $r_{k+1} = r_k + t_k p^{2^k}$. Montrer que $r_{k+1} \equiv r \mod p$ et $P(r_{k+1}) \equiv 0 \mod p^{2^{k+1}}$.

c) Soit $k = \lceil \log n \rceil$, c'est-à-dire l'entier tel que $2^{k-1} < n \leq 2^k$. Montrer que $r' = \mathrm{rem}(r_k, p^n)$ est l'unique entier modulo p^n tel que $r' \equiv r \mod p$ et $P(r') \equiv 0 \mod p^n$.

Commandes sage.

- **Calculs dans $\mathbb{Z}/n\mathbb{Z}$.** Pour définir l'anneau $A = \mathbb{Z}/n\mathbb{Z}$, on a le choix entre plusieurs possibilités. On peut utiliser la commande

  `A=Integers(n)`

  ou bien

  `A=IntegerModRing(n)`

  Alors, si k est un entier, `A(k)` est sa classe modulo n dans $\mathbb{Z}/n\mathbb{Z}$.

  Encore une possibilité pour travailler dans $\mathbb{Z}/n\mathbb{Z}$. Si k est un entier, la commande

  `mod(k,n)`

  désigne la classe de k modulo n.

  Dans tous les cas, si a est un élément de $\mathbb{Z}/n\mathbb{Z}$,

  `lift(a)`

  est l'entier $k \in [[0, n-1]]$ dont la classe modulo n est a.
- **Nombres premiers.**

  `is_prime(p)`

  indique si p est premier.

  `next_prime(n)`

  donne le plus petit nombre premier strictement supérieur à n.
- **Dérivée d'une fonction.** Pour calculer la dérivée d'une fonction $f(x)$:

  `diff(f,x)`