Université Bordeaux 1 — **Algèbre et calcul formel – Agrégation**
Mathématiques — Année 2021–2022

FEUILLE D'EXERCICES n° 3

Les anneaux $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

Exercice 1 – Expérimenter les commandes suivantes. Sur Jupyter, il faut une seule commande par cellule pour voir le résultat.

```
ZZ (c'est l'anneau ℤ)
A=IntegerModRing(12); A
A=Integers(12); A
A.list()
A.list_of_elements_of_multiplicative_group()
A.multiplicative_group_is_cyclic()
euler_phi(12)
a=A(5)
a^(10^10)
a.multiplicative_order()
```

Définir les anneaux `Zx` $= \mathbb{Z}[x]$, `Zxy` $= \mathbb{Z}[x,y]$ et `Z6t` $= (\mathbb{Z}/6\mathbb{Z})[t]$.

Exercice 2 – [Test de Fermat]
On rappelle le théorème de Fermat : si n est un nombre premier, alors pour tout a premier à n,

$$a^{n-1} \equiv 1 \mod n.$$

1) Soit $n = 2^{2^8} + 1$. En utilisant le théorème précédent, montrer que n n'est pas premier. Le vérifier à nouveau. en utilisant les fonctions `is_prime` et `factor`.

2) Même exercice avec $n = \frac{10^{41}+1}{11}$.

Exercice 3 – [Nombres de Fermat]

1) Soit $n = 2^{2^4} + 1$. Quel est l'ordre multiplicatif de 3 modulo n ? En déduire que n est premier.

2) Soit k un entier naturel. Le k-ème nombre de Fermat est l'entier $2^{2^k} + 1$. Il est clair que F_0 est premier. Le critère de Pépin donne une condition nécessaire et suffisante pour que F_k soit premier quand $k \geqslant 1$.

Théorème 1. [Critère de Pépin] *On suppose que $k \geqslant 1$. Alors F_k est premier si et seulement si*

$$3^{\frac{F_k-1}{2}} \equiv -1 \mod F_k$$

En utilisant ce critère, dresser la liste des entiers $k \in [[0, 14]]$ tels que F_k est premier.

3) Démontrer le sens indirect "$\Leftarrow$" du théorème 1.

4) Démontrer le sens direct.

Exercice 4 – [Nombres de Mersenne]
Pour tout nombre entier p, on note $M_p = 2^p - 1$. De tels nombres M_p sont appelés nombres de Mersenne. Si M_p est premier, on dit que M_p est un nombre de Mersenne premier.

1) Montrer que si M_p est premier, alors p est premier.
On admet le théorème suivant.

Théorème. (Test de Lucas) *Soit p un nombre premier impair. Soit L la suite définie de la manière suivante. $L_0 = 4$, et pour tout $n \geqslant 0$, $L_{n+1} = L_n^2 - 2$. Alors M_p est premier si et seulement si M_p divise L_{p-2}.*

2) Écrire une procédure Lucas qui étant donné un nombre premier p détermine si M_p est premier. Pour comparer l'efficacité de votre procédure avec celle de vos voisins, essayer par exemple `time Lucas(19937)`

3) En utilisant la procédure ci-dessus, établir la liste des 20 plus petits nombres de Mersenne premiers, ou plutôt la liste des 20 plus petits nombres premiers p tels que M_p est un nombre de Mersenne premier.

Exercice 5 – [Méthode ρ de Pollard]
Cette méthode vise à trouver un facteur non trivial d'un entier n donné. Soit $f(x) = x^2 + 1$. On choisit un entier x_0, et on pose $y_0 = x_0$. Pour $n \geqslant 0$, on pose $x_{n+1} = f(x_n) \bmod n$ et $y_{n+1} = f^2(y_n) \bmod n$. À chaque étape, on calcule $\mathrm{pgcd}(x_i - y_i, n)$, et on arrête dès que ce pgcd est différent de 1. Si en plus il est différent de n, c'est un facteur non trivial de n.

1) Écrire une procédure qui utilise cette méthode pour trouver un facteur non trivial d'un entier donné n.

2) Appliquer cette procédure à $10^{20} + 67$ et comparer entre vous les temps d'exécution obtenus.

Exercice 6 – [RSA]
X a choisi deux nombres premiers $p_1 = \frac{10^{31}+1}{11}$ et $p_2 = \frac{10^{53}+1}{11}$, qu'il garde secrets et en a fait le produit $n = p_1 p_2$. (Cet entier est trop petit, et puis p_1 et p_2 sont trop particuliers. On peut factoriser n trop facilement ... Tant pis. C'est juste une expérience.)

Y veut partager un nombre secret s strictement inférieur à n avec X. Pour cela, il lui envoie $s^{17} \bmod n$. On suppose que X reçoit 1111. Calculer alors s. (On doit trouver $s = 650966664 \ldots 3537769$.)

Exercice 7 – [Preuve du test de Lucas]
Le but de cet exercice est de démontrer le théorème 1 de l'exercice 4. Soit n un nombre premier impair ≥ 3 ; on pose donc $M_n = 2^n - 1$ et on considère la suite (L_n) définie dans l'exercice 4.

1) Soit p le plus petit diviseur premier de M_n. Soit K un corps de décomposition de $P = X^2 - 4X + 1$ sur $\mathbb{F}_p$. On note α et β les racines de P dans K. Montrer que la classe de L_i dans $\mathbb{F}_p$ est égale à $\alpha^{2^i} + \beta^{2^i} \mod p$ pour tout $i \geq 0$.

2) On suppose que M_n divise L_{n-2}.

a) Déterminer l'ordre de α dans le groupe K^*.

b) En déduire que $p = M_n$, et donc que M_n est premier.

3) Montrons maintenant la réciproque. On suppose que M_n est premier, donc que $p = M_n$. On choisit une racine carrée $\sqrt{3}$ de 3 et une racine carrée $\sqrt{2}$ de 2 dans K, puis on pose $a = \dfrac{1+\sqrt{3}}{\sqrt{2}}$ dans K.

a) Montrer que l'on peut choisir α de sorte que $a^2 = \alpha$.

b) Montrer que $\alpha^{2^{n-1}} = -1$.

c) En déduire que $L_{n-2} \equiv 0 \bmod M_n$.