

FEUILLE D'EXERCICES n° 3
Les anneaux \mathbb{Z} et $\mathbb{Z}/n\mathbb{Z}$

Exercice 1 – Expérimenter les commandes suivantes.

```
ZZ (c'est l'anneau  $\mathbb{Z}$ )
A=IntegerModRing(12); A
A.list()
A.list_of_elements_of_multiplicative_group()
euler_phi(6)
a=A(5)
a^(10^10)
a.multiplicative_order()
```

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

Exercice 2 – [TEST DE FERMAT]

On rappelle le théorème de Fermat : si n est un nombre premier, alors pour tout a premier à n ,

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

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

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

Exercice 3 – [TEST DE PRIMALITÉ]

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

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. $L_1 = 4$, et pour tout $n \geq 1$, $L_{n+1} = L_n^2 - 2$. Alors M_p est premier si et seulement si M_p divise L_{p-1} .*

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 $n \geq 0$, 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 $\text{pgcd}(x_i - y_i, n)$, 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 $s = 650966664 \dots 3537769$.)