Algorithme d'Euclide

Exercice 1. Révisions

1. Déterminer la liste de tous les nombres premiers inférieurs à 10000 de la forme a^2+1 avec $a \in \mathbb{Z}$.
2. Écrire une fonction prenant en entrée un entier $n \in \mathbb{N}^*$ et renvoyant la liste des carrés dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ (on rappelle que cet anneau est défini par la commande `Zmod(n)`).

Exercice 2. Algorithme d'Euclide

1. Implanter une fonction `div_eucl(a,b)` de division euclidienne pour les entiers positifs (on demande qu'elle renvoie le quotient et le reste). Comparer ensuite avec les commandes `//` et %.
2. Implanter l'algorithme d'Euclide pour les entiers sous forme d'une fonction `euclide(a,b)` (on ne demande pas pour l'instant que l'algorithme renvoie des coefficients de Bézout mais simplement le pgcd du couple d'entiers donné en entrée). Comparer avec `gcd`.
3. Modifier légèrement la fonction `euclide(a,b)` pour qu'apparaisse en sortie le nombre de divisions euclidiennes nécessaires au calcul du pgcd. Vérifier que pour tout $1 \leqslant n \leqslant 100$, le calcul de $\mathrm{pgcd}(F_{n+1}, F_n)$ nécessite n divisions euclidiennes, où F_n est le n-ième nombre de Fibonacci. On rappelle que la suite de Fibonacci (F_n) est définie par $F_0 = F_1 = 1$ et par la récurrence $F_{n+2} = F_{n+1} + F_n$ pour tout $n \geqslant 0$.

Exercice 3. Algorithme d'Euclide étendu

1. Écrire l'algorithme d'Euclide étendu pour les entiers (on pourra se restreindre au cas d'un couple d'entiers *positifs* (a, b)) sous forme d'une fonction `euclide_etendu(a,b)`.
2. Comparer avec `xgcd`.
3. Écrire une fonction `inverse_mod(a,m)` permettant de calculer l'inverse d'un entier a modulo m. Si a n'est pas premier avec m, on utilisera la commande

   ```
   raise ValueError("Le nombre {} n'est pas inversible modulo {}".format(a,m))
   ```

   où la méthode `format` appliquée à une chaîne de caractères remplace les `{}` par la valeur des expressions données comme arguments (ici a et m). On comparera la réponse à la commande `inverse_mod(2,4)` avec la réponse habituelle de `Sage` en cas d'erreur.

Exercice 4. Nombre d'or

La commande `R.<X>=PolynomialRing(QQ)` définit `R` comme $\mathbb{Q}[X]$ et `X` comme l'indéterminée associée. On note ϕ le nombre d'or (c'est la solution positive de $X^2 = X + 1$).

1. Montrer que si $P \in \mathbb{Q}[X]$ alors il existe $Q \in \mathbb{Q}[X]$ de degré au plus 1 tel que $P(\phi) = Q(\phi)$.
2. Montrer que si P est premier avec $X^2 - X - 1$ alors il existe $Q \in \mathbb{Q}[X]$ de degré au plus 1 tel que $\frac{1}{P(\phi)} = Q(\phi)$.

3. Simplifier les expression suivantes

$$\phi^7 + 2\phi^6 + \phi^4 + 1, \quad \frac{1}{\phi^7 - 1}, \quad \frac{\phi^4 - \phi + 1}{\phi^7 - 1}$$

sans utiliser de formule explicite pour ϕ. On veut obtenir des expressions polynomiales en ϕ de petit degré.

Exercice 5. Générateurs de $\mathbb{Z}/p\mathbb{Z}^*$

1. Soit $n \geqslant 2$ un entier. Quels sont les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$? Combien y a-t-il de tels générateurs ?
2. Soit p un nombre premier. Combien $\mathbb{Z}/p\mathbb{Z}^*$ a-t-il de générateurs ? (On rappelle que $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique.)
3. Écrire une fonction `Sage` qui détermine un générateur de $\mathbb{Z}/p\mathbb{Z}^*$ en testant des éléments au hasard jusqu'à en trouver un qui convienne. On pourra utiliser `randint` pour tirer un entier au hasard.
4. Modifier la fonction de la question précédente pour renvoyer également le nombre de tirages aléatoires effectués.
5. Comparer les résultats théoriques et pratiques obtenus dans cet exercice. On pourra utiliser `euler_phi` pour calculer l'indicatrice d'Euler.

Exercice 6. Décomposition sans carré d'un polynôme

Soit $P \in \mathbb{Q}[X]$. On note $P = P_1^{r_1} \cdots P_k^{r_k}$ sa décomposition en facteurs irréductibles. La *partie sans carré* de P est $P_1 \cdots P_k$. On dit que P est *sans carré* s'il est égal à sa partie sans carré.

1. Expliquer comment trouver la partie sans carré d'un polynôme sans le factoriser.
2. Écrire une procédure calculant la partie sans carré d'un polynôme.
3. Montrer que tout polynôme $P \in \mathbb{Q}[X]$ de degré n peut s'écrire $P = Q_1(Q_2)^2 \cdots (Q_n)^n$ où les $Q_i \in \mathbb{Q}[X]$ sont sans carré et premiers entre eux. On parle de *décomposition sans carré*.
4. Écrire une procédure calculant la décomposition sans carré d'un polynôme sans le factoriser.
5. La formule de la première question est-elle encore valable dans $\mathbb{Z}/p\mathbb{Z}[X]$ avec p premier ?

Exercice 7. Équations diophantiennes

Écrire une fonction de résolution des équations diophantiennes $ax + by = c$ où a, b et c sont des entiers (on cherche les solutions entières de cette équation).