PROJET K : NOMBRES DE CARMICHAEL

1. Un pseudo-test de primalité

Soit n un nombre entier.

1. Coder en Python l'algorithme suivant :
   (i) Choisir un nombre entier a dans $\{1, 2, \ldots, n-1\}$ *au hasard.*
   (*On pourra utiliser le module* `random` *et la fonction* `random.randint(a,b)`*.)*
   (ii) Si a n'est pas premier à n, recommencer l'étape (i).
   (iii) Si a est premier à n, calculer a^{n-1} modulo n.
   (*Utiliser l'algorithme d'exponentiation rapide vu à la séance 4.*)
2. Justifier que la probabilité de passer directement de l'étape (i) à l'étape (iii) est égale à $\frac{\varphi(n)}{n}$, où φ désigne la fonction indicatrice d'Euler.
3. Quel est le résultat de cet algorithme si n est premier ?
4. Que peut-on dire de n si cet algorithme fournit une réponse différente de 1 ?

2. Les nombres de Carmichael

Un *nombre de Carmichael* est un nombre entier impair et composé n tel que

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

pour tout entier a tel que $\mathrm{pgcd}(a, n) = 1$.

1. En Python, écrire une fonction `Carmichael(n)` vérifiant si un entier n est, ou non, un nombre de Carmichael. L'utiliser pour déterminer tous les nombres de Carmichael jusqu'à une borne donnée.
2. Déterminer le plus petit nombre de Carmichael.
3. Supposons maintenant que n soit un nombre entier qui n'est ni premier, ni de Carmichael.
   (i) Démontrer que l'ensemble des classes $\overline{a}$ modulo n telles que $\overline{a}^{n-1} = 1$ est un sous-groupe *strict* de $(\mathbf{Z}/n\mathbf{Z})^\times$.
   (ii) En déduire que la probabilité que l'algorithme de la première partie fournisse le nombre 1 est inférieure ou égale à $\frac{1}{2}$.
   (iii) Quelle est la probabilité que l'algorithme de la première partie, appliqué N fois de suite, fournisse à chaque reprise 1 ?
4. Expliquer précisément comment l'algorithme de la partie 1 permet de définir un test efficace détectant les nombres qui ne sont ni premiers, ni de Carmichael.

3. Une caractérisation des nombres de Carmichael

Le but de cette section est de démontrer le théorème suivant.

Un nombre entier $n \geqslant 1$ est de Carmichael si et seulement s'il est de la forme $n = p_1 \cdots p_r$, avec $r \geqslant 2$, $p_1, \ldots, p_r$ premiers distincts et $p_i - 1 | n - 1$ pour tout i.

(A) *Condition suffisante*

Soit n un nombre entier vérifiant les conditions du théorème ci-dessus. Soit a un entier premier à n.

1. Vérifier que l'on a
$$a^{n-1} \equiv 1 \pmod{p_i}$$
pour tout i.

2. En déduire que l'on a
$$a^{n-1} \equiv 1 \pmod{n}$$
(*Penser au théorème des restes chinois.*)

(B) *Condition nécessaire*

Supposons que n soit un nombre de Carmichael.

1. Considérons un nombre premier p divisant n et écrivons $n = p^k n'$ avec $k \geqslant 1$ et $p \nmid n'$.
   (i) Justifier qu'il existe un entier $a \geqslant 1$ tel que
   $$a \equiv 1 + p \pmod{p^k} \text{ et } a \equiv 1 \pmod{n'}.$$
   (ii) En déduire que l'on a $(1+p)^{n-1} \equiv 1 \pmod{p^k}$.
   (iii) En utilisant la formule du binôme, démontrer la congruence
   $$(1+p)^{n-1} \equiv 1 + (n-1)p \pmod{p^2}.$$
   (iv) Si $k \geqslant 2$, obtenir une contradiction en combinant (ii) et (iii).
2. Nous venons de prouver que n n'a pas de facteur carré. Écrivons donc maintenant $n = p_1 \cdots p_r$, avec $r \geqslant 2$ et $p_1, \ldots, p_r$ premiers deux à deux distincts. Dans ce qui suit, on désigne par p l'un des p_i.
   (i) En utilisant de nouveau le théorème chinois des restes, démontrer que l'on a
   $$a^{n-1} \equiv 1 \pmod{p}$$
   pour tout entier a premier avec p.
   (ii) En déduire $p - 1 | n - 1$. (*On pourra utiliser le fait que le groupe des éléments inversibles de l'anneau* $\mathbf{Z}/p\mathbf{Z}$ *est cyclique*).
3. En Python, écrire une fonction `Carmichael2(n)` utilisant la caractérisation que l'on vient d'obtenir pour déterminer si un entier n est un nombre de Carmichael ou non.
4. Comparer le temps de calcul des fonctions `Carmichael(n)` et `Carmichael2(n)`.

4. La méthode de construction de Chernick

1. Vérifier que, si m est un nombre entier tel que $6m+1$, $12m+1$ et $18m+1$ soient tous les trois premiers, alors
$$n = (6m+1)(12m+1)(18m+1)$$
est un nombre de Carmichael.

2. Définir une fonction `Chernick(k)` qui détermine le plus petit nombre entier $m \geqslant k$ tel que $6m+1, 12m+1$ et $18m+1$ soient tous trois des nombres premiers.

3. En déduire une fonction `Carmichael3(x)` renvoyant le plus petit nombre de Carmichael de la forme $n = (6m+1)(12m+1)(18m+1)$ tel que $n \geqslant x$.