Université de Bordeaux — **Algèbre et calcul formel – Master**
Mathématiques — Année 2023–2024

FEUILLE D'EXERCICES n° 7

Rappelons que si p est premier, tout a non divisible par p vérifie $a^{p-1} \equiv 1 \mod p$. Ainsi, un entier n étant donné, si l'on trouve un $a \in [[1, n-1]]$ tel que

$$a^{n-1} \not\equiv 1 \mod n, \tag{1}$$

on sait que n n'est pas premier. Ceci fournit un premier test de non-primalité : on prend des a au hasard entre 1 et $n-1$ et on calcule $a^{n-1} \mod n$. Dès que l'un d'entre eux vérifie (1), on sait que n est composé. On dit alors que a est un témoin de non primalité de Fermat pour n. Si, en revanche, au bout d'un certain nombre d'essais, (1) n'a toujours pas été vérifiée, on peut juste dire que n a des chances d'être premier. Hélas, de nombreux nombres composés peuvent passer à travers ce test, en particulier les nombres dits de Carmichael.

Définition 1. On appelle *nombre de Carmichael* tout nombre composé n vérifiant

$$a^{n-1} \equiv 1 \mod n \quad \text{pour tout } a \text{ premier à } n.$$

Exercice 1 – [Quelques exemples]

1) Que vaut $2^{14} \mod 15$? En déduire que 2 est un témoin de non primalité de Fermat pour 15.

2) Soit a un entier premier à $561 = 3.11.17$. En utilisant la factorisation $560 = 2^4 \cdot 5 \cdot 7$, calculer a^{560} modulo chacun des entiers 3, 11 et 17 ? En déduire que 561 est un nombre de Carmichael.

3) Que vaut 2^{35} modulo les entiers 3, 11 et 17 ? En déduire que 2 est un témoin de Rabin-Miller pour 561.

4) Montrez que $1729 = 7.13.19$ et $29341 = 13.37.61$ sont des nombres de Carmichael.

Exercice 2 – [Test de Fermat]

Soit n un nombre entier composé qui n'est pas un nombre de Carmichael.

1) Rappeler pourquoi le cardinal $M(n)$ de l'ensemble des menteurs de Fermat pour n est inférieur ou égal à $\varphi(n)/2$.

2) Vérifier que $M(15) = \varphi(15)/2$.

Le **critère de Korselt** caractérise les nombres de Carmichael. Vous l'admettrez pour le reste de ce TD, il sera démontré dans la prochaine feuille TD :

Théorème 2 (Critère de Korselt)**.** *Un entier est un nombre de Carmichael si et seulement s'il est composé, sans facteur carré, et si pour tout premier p divisant n, l'entier $p-1$ divise $n-1$.*

Exercice 3 – [Nombres de Carmichael]

1) Que fait l'algorithme `Mystere` suivant ?

Algorithme 1. Mystere

Entrées: n : entier naturel non nul
Sorties: `true` ou `false`

```
1: F=factor(n)
2: if len(F)<=1 :
3:   return false
4: for f in F :
5:   if f[1]>1 :
6:     return false
7: for f in F :
8:   if (n-1) % (f[0]-1) != 0 :
9:     return false
10: return true
```

2) Écrire `Mystere` sur sage, et une fonction qui prend en entrée un entier N et rend en sortie la liste des N plus petits nombres de Carmichaël.

Dresser la liste des 30 premiers nombres de Carmichael que l'on stockera dans une liste pour la suite du travail.

Exercice 4 – [Test de Fermat]

1) Programmer le test de non primalité de Fermat qui prend n et un entier a comme paramètres et qui calcule $a^{n-1} \mod n$. Si le résultat est différent de 1, on sait que n est composé. Essayer ce test sur l'entier $n = 10^{20} + 67$ avec plusieurs entiers a pris au hasard.

2) Programmer le test qui consiste à appliquer la fonction précédente à un certain nombre k d'entiers a compris entre 1 et $n-1$ choisis au hasard (par exemple $k = 10$). Si au bout des k essais on n'a aucun résultat négatif, on ne peut rien dire d'autre que « n est peut-être premier ». On dit parfois que n est pseudo-premier.

3) Le tester sur les nombres <10000 (et vérifier que ceux qui n'ont pas été identifiés comme composés ne sont pas toujours premiers). Comparer le nombre d' entiers pseudo-premiers au nombre d'entiers véritablement premiers.

4) Le tester sur les nombres de Carmichael définis dans l'exercice précédent.

Exercice 5 – [Test de Rabin-Miller]

1) On améliore ce test de la façon suivante (test de Rabin-Miller). On décompose $n-1$ sous la forme $n-1 = 2^e q$ avec q impair. Comme précédemment, on prend des entiers au hasard entre 2 et $n-2$. Or, si n est premier on a

(i) soit $a^q \equiv 1 \mod n$,

(ii) soit il existe i vérifiant $0 \leqslant i < e$ et $a^{2^i q} \equiv -1 \mod n$.

Dès qu'un a ne vérifie ni (i) ni (ii), i.e. dès que $a^q \not\equiv 1 \mod n$ et $a^{2^i q} \not\equiv -1 \mod n$ pour tout $0 \leqslant i < e$, on sait que n est composé. Programmer le test de Rabin-Miller et comparer les résultats obtenus avec ceux que donnaient le test de Fermat itéré dans l'exercice précédent.