Université de Bordeaux — **Algèbre et calcul formel – Master**
Mathématiques — Année 2016–2017

FEUILLE D'EXERCICES n° 8
Travail sur machine

Exercice 1 – [Carmichael]
Un nombre de Carmichael est un entier naturel non nul composé n tel que pour tout entier a premier à n,

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

On rappelle le critère de Korselt.

Théorème 1 (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 $n-1$.*

À l'aide du critère de Korselt, dresser la liste des 30 premiers nombres de Carmichael que l'on stockera dans une liste pour la suite du travail.

Exercice 2 – [Rabin-Miller]
On s'intéresse ici au test de Rabin-Miller et en particulier à son effet sur les nombres de Carmichael.

1) Programmer le test de composition 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.

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. 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 ».

3) Le tester sur les nombres <10000 (et vérifier que ceux qui n'ont pas été identifiés comme composés ne sont pas toujours premiers), puis sur les nombres de Carmichael définis dans l'exercice précédent. En théorie, certains d'entre eux, bien que composés, doivent passer à travers le test (à moins de tomber par chance sur un a vérifiant $\mathrm{pgcd}(a,n) > 1$, ce qui sera rare quand n aura de gros facteurs premiers en petit nombre).

4) 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 initialement programmé.

5) Supposons que n soit un nombre de Carmichael. Soit $a < n$ un témoin de non primalité de Rabin-Miller pour n. Alors si a n'est pas premier à n, le pgcd de a et n fournit un facteur non trivial de n. Supposons maintenant a premier à n. Alors il existe un entier i dans $\{1, \ldots, e\}$ tel que

$$a^{q2^i} \equiv 1 \mod n \quad \text{et} \quad a^{q2^{i-1}} \not\equiv 1 \mod n.$$

Alors $\text{pgcd}(a^{q2^{i-1}} - 1, n)$ est un facteur non trivial de n.

Proposer une alternative à l'algorithme précédent qui utilise ce fait pour rendre un facteur non trivial de n dans le cas où n est de Carmichael et où a est un témoin de non primalité de n.