Université Bordeaux 1 | **Algèbre et calcul formel – Master**
Mathématiques | Année 2012–2013

FEUILLE D'EXERCICES n° 9

Rappelons que si p est premier, tout a non divisible par p vérifie $a^{p-1} \equiv 1 \mod p$. Ainsi, un entier $n \geqslant 4$ étant donné, si l'on trouve un a vérifiant $1 < a < n-1$ et

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

on sait que n n'est pas premier. Ceci fournit un premier test de non-primalité : on prend des a au hasard entre 2 et $n-2$ et on calcule $a^{n-1} \mod n$. Dès que l'un d'entre eux vérifie (1), on sait que n est composé. 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 – [Deux exemples]

1) Vérifier que 2 est un témoin de Fermat pour 15.

2) Vérifier que 2 n'est pas un témoin de Fermat pour $561 = 3.11.17$.

3) Vérifier que 2 est un témoin de Rabin-miller pour 561.

4) Montrer que 561 est un nombre de Carmichael.

Exercice 2 – [Test de Fermat]

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

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

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

Exercice 3 – [Nombres de Carmichael]

1) Montrer qu'un nombre de Carmichael est sans facteur carré.

2) Montrer qu'un entier composé sans facteur carré est un nombre de Carmichael si et seulement si pour tout premier p divisant n, $p-1$ divise $n-1$. [*Si p est premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique*].

On a donc le théorème suivant :

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, $p-1$ divise $n-1$.*

3) Montrer qu'un nombre de Carmichael est impair et produit d'au moins trois nombres premiers distincts.

4) Vérifier que 561, 1729 et 29341 sont des nombres de Carmichael.

5) Supposons que p, $2p-1$ et $3p-2$ soient tous trois premiers. Montrer que $p = 3$ ou $p \equiv 1 \mod 6$, et que dans ce dernier cas $p(2p-1)(3p-2)$ est un nombre de Carmichael.

6) Montrer que la Définition 1 est équivalente à la suivante.

Définition 3. On appelle *nombre de Carmichael* tout nombre composé n vérifiant $a^n \equiv a \pmod{n}$ pour tout a.

7) On suppose que n est de Carmichael. On applique le test de non-primalité de Rabin-Miller à n et on suppose qu'il est positif, i.e. qu'on dispose de $a \in \mathbb{Z}/n\mathbb{Z}$ qui est témoin de non-primalité. Montrer qu'on peut facilement en déduire un facteur non trivial de n.