

### FEUILLE D'EXERCICES n° 9

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

$$(1) \quad a^{n-1} \not\equiv 1 \pmod{n},$$

on sait que  $n$  n'est pas premier. Ceci fournit un premier test de non-primauté : on prend des  $a$  au hasard entre 2 et  $n-2$  et on calcule  $a^{n-1} \pmod{n}$ . 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

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

#### 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  $561 = 3 \cdot 11 \cdot 17$ .
- 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) Soit  $p$  un nombre premier et  $m$  un nombre naturel non nul. Soit  $n = p^2 m$ . Montrer que

$$(1 + pm)^{n-1} \not\equiv 1 \pmod{n}.$$

En déduire que tout nombre de Carmichael est sans facteur carré.

2) On rappelle que si  $p$  est premier,  $(\mathbb{Z}/p\mathbb{Z})^*$  est cyclique. Soit  $n$  un entier sans facteur carré.

a) On suppose que pour tout nombre premier  $p$  divisant  $n$ , l'entier  $p - 1$  divise  $n - 1$ . Soit  $a$  un entier premier à  $n$ . Montrer que

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

b) On suppose que  $n$  est de Carmichael. Soit  $p$  un diviseur premier de  $n$ . Soit  $g$  un entier dont la classe modulo  $p$  engendre  $(\mathbb{Z}/p\mathbb{Z})^*$ . Montrer qu'il existe un entier  $a$  premier à  $n$  tel que  $a \equiv g \pmod{n}$ . En déduire que  $p - 1$  divise  $n - 1$ .

3) En déduire 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  $n$ , l'entier  $p - 1$  divise  $n - 1$ .*

4) Montrer que tout nombre de Carmichael est impair et produit d'au moins trois nombres premiers distincts.

5) Vérifier que  $561 = 3.11.17$ ,  $1729 = 7.13.19$  et  $29341 = 13.37.61$  sont des nombres de Carmichael.

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

7) 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  $a$ .

8) On suppose que  $n$  est de Carmichael. On applique le test de non-primauté 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-primauté. Montrer qu'on peut facilement en déduire un facteur non trivial de  $n$ .