

**FEUILLE D'EXERCICES n° 8**  
Tests de Fermat, de Rabin-Miller

**Attention.** Pour calculer une expression du type

$$a^k \bmod nn,$$

tous les calculs doivent être faits modulo  $n$ . Il est catastrophique de calculer d'abord l'entier  $a^k$ , puis de le réduire modulo  $n$  : si  $k$  est de l'ordre de  $n$ , on passe d'une complexité polynomiale en  $\log n$  à une complexité *exponentielle*, en temps comme en espace.

**Exercice 1** – [FERMAT]

Soit  $n$  un nombre premier et soit  $a$  un entier premier à  $n$ , alors  $a^{n-1} \equiv 1 \pmod{n}$ .

- 1) Écrire une fonction qui prend en entrée  $n$  et  $a$ , et qui utilise ce test pour décider si  $n$  est composé ou s'il peut être premier.
- 2) Soit  $k$  un entier positif. Écrire une fonction qui utilise  $k$  fois le test précédent pour décider si  $n$  est composé ou s'il 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).

**Exercice 2** – [NOMBRES DE CARMICHAËL]

Un entier naturel composé  $n$  est dit de Carmichaël si pour tout  $a$  premier à  $n$ , on a  $a^{n-1} \equiv 1 \pmod{n}$ .

On montre facilement que si  $n$  est un entier composé qui n'est pas de Carmichaël, et si l'on choisit  $a$  uniformément au hasard dans  $\mathbb{Z}/n\mathbb{Z}$ , la probabilité de détecter que  $n$  est composé en utilisant le test de Fermat est supérieure à  $1/2$ . Des tests indépendants successifs permettent donc de détecter que  $n$  est composé avec probabilité arbitrairement proche de 1.

Restent les nombres de Carmichaël. Pour caractériser ces nombres, on dispose du critère suivant.

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

- 1) Soit  $n$  un nombre de Carmichael. Montrer que  $n$  est impair. Montrer que  $n$  a au moins trois facteurs premiers.
- 2) À l'aide du critère de Korselt, dresser la liste des 30 premiers nombres de Carmichael.
- 3) Appliquer le test de l'exercice précédent à ces nombres.

**Exercice 3** – [RABIN-MILLER]

1) On améliore le test de Fermat 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 choisit  $a$  uniformément au hasard entre 2 et  $n - 2$ . Or, si  $n$  est premier on a

(i) soit  $a^q \equiv 1 \pmod{n}$ ,

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

Dès qu'un  $a$  ne vérifie ni (i) ni (ii), on sait que  $n$  est composé.

2) Écrire une fonction qui prend en entrée  $n$  et  $a$ , et qui utilise ce test pour décider si  $n$  est composé ou s'il peut être premier.

3) Soit  $k$  un entier positif. Écrire une fonction qui utilise  $k$  fois le test précédent pour décider si  $n$  est composé ou s'il peut-être premier.

4) Appliquer ce dernier test à la liste des nombres de Carmichael dressée dans l'exercice précédent.

**Exercice 4** – [RAFFINEMENT DU TEST DE RABIN-MILLER]

Supposons que  $n$  soit un nombre composé, et 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  $n$ .

1) Supposons maintenant  $n$  de Carmichael et  $a$  premier à  $n$ . Alors il existe un entier  $i$  dans  $\{1, \dots, e\}$  tel que

$$a^{q^{2^i}} \equiv 1 \pmod{n} \quad \text{et} \quad a^{q^{2^{i-1}}} \not\equiv 1 \pmod{n}.$$

Montrer que  $\text{pgcd}(a^{q^{2^{i-1}}} - 1, n)$  est un facteur non trivial de  $n$ .

2) Proposer un raffinement du test de Rabin-Miller 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  $n$ .