Les nombres de Carmichaël

On se propose d'introduire les nombres de Carmichaël, que l'on appelle aussi des « menteurs de Fermat ».

Pour tester si un entier naturel est premier, les algorithmes simples, comme le crible d'Érathostène, ne sont pas utilisables en pratique pour des entiers assez grands. On cherche donc à élaborer d'autres tests, plus efficaces. On étudiera ici comment une propriété des nombres premiers peut conduire à un test de primalité de nature probabiliste.

I. Rappel : le corollaire du petit théorème de Fermat (1640)

Si p est un nombre premier, alors pour tout nombre entier naturel a premier avec p on a $a^{p-1} \equiv 1$ [p].

On peut remarquer que, comme p est un nombre premier, « a premier avec p » signifie « a non divisible par p».

II. Question

On s'interroge sur une réciproque possible du petit théorème de Fermat.

« Si n est un nombre entier naturel tel que pour tout entier naturel a premier avec n on a $a^{n-1} \equiv 1$ [n], alors peut-on affirmer que n est un nombre premier ? »

La réponse est non.

Contre-exemple : $n = 561$ (Carmichaël, 1909).

Les entiers n non premiers qui vérifient cette propriété sont appelés nombres de Carmichaël.

En 1994, un mathématicien a démontré qu'il existe une infinité de nombres de Carmichaël.

III. Étude du cas $n = 561$

Démontrons que 561 est un nombre de Carmichaël c'est-à-dire que pour tout entier naturel a premier avec 561 $a^{560} \equiv 1$ [561].

On observe d'abord que 561 n'est pas un nombre premier.
Sa décomposition en facteurs premiers est donnée par : $561 = 3 \times 11 \times 17$.

On va utiliser la propriété suivante :

$3 - 1 \mid 561 - 1$

$11 - 1 \mid 560$

$17 - 1 \mid 560$

Soit a un entier naturel premier avec 561.
a est alors premier avec 3, 11, 17.

Donc d'après le corollaire du petit théorème de Fermat, on a :

$a^2 \equiv 1$ [3]
$a^{10} \equiv 1$ [11]
$a^{16} \equiv 1$ [17]

Donc en élevant les deux membres de chaque congruence à un même exposant :

$a^{560} \equiv 1$ [3]
$a^{560} \equiv 1$ [11]
$a^{560} \equiv 1$ [17]

Donc 3, 11 et 17 divisent $a^{560} - 1$.

Comme 3, 11 et 17 sont deux à deux premiers entre eux, $3 \times 11 \times 17 \mid a^{560} - 1$.

Propriété :

Si un entier est divisible par des entiers premiers entre eux deux à deux, alors il est divisible par leur produit.

D'où $561 \mid a^{560} - 1$ soit $a^{560} \equiv 1$ [561].

IV. Étude du cas $n = 1105$

Démontrons que 1105 est un nombre de Carmichaël.

Il s'agit donc de démontrer que pour tout entier naturel a premier avec 1105, on a $a^{1104} \equiv 1$ [1105].

La décomposition en facteurs premiers de 1105 est donnée par : $1105 = 5 \times 13 \times 17$.

On va utiliser la propriété suivante :

$5 - 1 \mid 1104$

$13 - 1 \mid 1104$

$17 - 1 \mid 1104$

Soit a un entier naturel premier avec 1105.

a est alors premier avec 5, 13, 17.

Donc d'après le corollaire du petit théorème de Fermat, on a :
$a^4 \equiv 1$ [5]
$a^{12} \equiv 1$ [13]
$a^{16} \equiv 1$ [17]

Donc en élevant les deux membres de chaque congruence à un même exposant :

$a^{1104} \equiv 1$ [5]
$a^{1104} \equiv 1$ [13]
$a^{1104} \equiv 1$ [17]
Donc 5, 13 et 17 divisent $a^{1104} - 1$.
Comme 5, 13 et 17 sont deux à deux premiers entre eux, $5 \times 13 \times 17 \mid a^{1104} - 1$.

D'où $1105 \mid a^{1104} - 1$ soit $a^{1104} \equiv 1$ [1105].

V. Quelques généralités sur les nombres de Carmichaël

1°) Définition

On appelle nombre de Carmichaël (ou nombre pseudo-premier) un entier naturel *n* non premier tel que pour tout entier naturel *a* premier avec *n* on a $a^{n-1} \equiv 1$ [*n*].

2°) Commentaires

• Il n'y a pas de définition plus simple d'un nombre de Carmichaël.
En particulier, il n'y a pas de formule pour trouver les nombres de Carmichaël.

• Pour démontrer qu'un nombre est un nombre de Carmichaël, il faut faire la même démarche que ce que nous avons fait dans les paragraphes **III** et **IV**. On peut aussi s'en sortir avec un algorithme.

• Les nombres de Carmichaël possèdent certaines propriétés que nous n'étudierons pas dans ce chapitre.

• En 1994, on a prouvé qu'il en existe une infinité. 561 est le plus petit d'entre eux et ils sont très rares : il n'y en a que 2163 inférieurs à 25 millions !

3°) Application

On cherche si un entier donné naturel *p* est premier.

Le **test de primalité de Fermat** s'effectue en choisissant au hasard un entier *a* tel que $1 < a \leqslant p - 1$:

- si a^{p-1} n'est pas congru à 1 modulo *p*, on est sûr que *p* n'est pas premier.
- si a^{p-1} est congru à 1 modulo *p*, il est possible que *p* soit premier mais il est possible qu'il ne le soit pas !

Même si pour tout entier naturel *a* tel que $1 \leqslant a \leqslant p - 1$ [*p*], on ne peut déclarer *p* que comme « probablement premier ».

Le test de primalité de Fermat est un test probabiliste. Pour un certain nombre d'applications, il est tout à fait suffisant de savoir qu'un nombre est probablement premier à condition que le taux d'erreur soit assez faible. Les tests probabilistes actuels ont une probabilité d'erreur inférieure, dit-on, à la probabilité que le système informatique qui réalise le test commette une erreur.

Les sept premiers nombres de Carmichael sont :
$561 = 3 \times 11 \times 17$
$1\,105 = 5 \times 13 \times 17$
$1\,729 = 7 \times 13 \times 19$
$2\,465 = 5 \times 17 \times 29$
$2\,821 = 7 \times 13 \times 31$
$6\,601 = 7 \times 23 \times 41$
$8\,911 = 7 \times 19 \times 67$.

Robert Daniel Carmichaël : mathématicien américain

Robert Daniel Carmichael

Robert Daniel Carmichael (1er mars 1879 - 2 mai 1967) est un mathématicien américain.
Carmichael est né à Goodwater (en), Alabama en 1879. Il étudie au College de Lineville (en) où il reçoit son B. A. en 1898 tout en travaillant à son doctorat à l'université de Princeton, qu'il reçoit en 1911. Sa thèse, écrite sous la direction de George David Birkhoff, fut considérée comme la première contribution significative d'un américain aux équations différentielles.
Physicien au début de sa carrière (il étudie la théorie de la relativité dont l'initiateur fut Albert Einstein), mathématicien et philosophe, Carmichael se consacra tout particulièrement, dès 1914, à la théorie des nombres (aux nombres premiers en particulier), à l'analyse diophantienne et à la théorie des groupes. Il enseigna à l'université de l'Indiana de 1911 à 1915 et à l'université de l'Illinois de 1915 à 1947.
Dans le cadre de l'étude de la primalité d'un entier naturel (savoir si un nombre est premier et sinon connaître sa factorisation) et de la distribution des nombres premiers dans l'ensemble des entiers naturels, Carmichael recherche et étudie les propriétés des nombres de Carmichael, aussi appelés nombres absolument pseudo-premiers.