Marien LAURENT Université Paul Sabatier - Toulouse 3

AG - Nombres de Carmichael

Recasages. 120, 121, 127
Références. Gourdon pour Carmichael. Rombaldi parle de la cyclicité.

Le petit théorème de Fermat affirme que si p est un nombre premier, alors pour tout $a \in \mathbb{Z}$, $a^p \equiv a[p]$. La réciproque est-elle vraie ? Non, par exemple le nombre $561 = 3 \times 11 \times 17$ vérifie bien que pour tout $a \in \mathbb{Z}$, $a^{561} \equiv a[561]$ par le théorème des restes chinois. En effet, le petit théorème de Fermat donne

$$\begin{cases} a^{561} \equiv a[3] \\ a^{561} \equiv a[11] \\ a^{561} \equiv a[17] \end{cases}$$

et comme 3, 11 et 17 sont deux à deux premiers entre eux, il existe une unique solution du système modulo 561. On a donc un nombre non premier qui vérifie le test de Fermat.

Définition. On appelle nombre de Carmichael tout entier naturel $n \geq 2$ non premier tel que pour tout $a \in \mathbb{Z}$, $a^n \equiv a[n]$.

Théorème. Soit $n \geq 2$ un entier naturel. n est un nombre de Carmichael si, et seulement si, il existe $r \geq 3$, $(p_i)_{1 \leq i \leq r}$ premiers distincts tels que $n = p_1 \cdots p_r$, et pour tout $i \in \{1, \cdots, r\}$, $p_i - 1$ divise $n - 1$.

Preuve. Soit $n \geq 2$.
$\boxed{\Longrightarrow}$ Supposons que n est un nombre de Carmichael.

- Comme n est supposé non premier, il admet au moins un diviseur premier p distinct de n. Par l'absurde, supposons que $p^2 | n$. Comme $p^n \equiv p(n)$, n divise $p^n - p$, donc par transitivité p^2 divise $p^n - p$. Or p^2 divise p^n car $n \geq 2$, donc p^2 divise p. Absurde. Donc n s'écrit comme produit de r nombres premiers distincts.
- Soit p diviseur premier de n. $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique d'ordre $p - 1$. Il existe $a \in \mathbb{N}$ tel que $\overline{a}$ l'engendre, et l'ordre de $\overline{a}$ est exactement $p - 1$. Comme $a^n \equiv a(n)$ et que a est inversible, on déduit que $a^{n-1} \equiv 1[n]$, et comme $p | n$, $a^{n-1} \equiv 1[p]$ donc l'ordre de $\overline{a}$, $p - 1$, divise $n - 1$.
- Enfin montrons que $r \geq 3$. Par l'absurde, si $r = 2$, alors il existe p, q premiers distincts, $n = pq$. Mais alors
$$n - 1 = pq - 1 = pq - p + p - 1 = p(q - 1) + p - 1 \iff n - 1 - p(q - 1) = p - 1,$$
et comme $q - 1$ divise $n - 1$ et lui-même, il divise $p - 1$. De même $p - 1$ divise $q - 1$ et finalement $p = q$. Absurde par le premier item !

$\boxed{\Longleftarrow}$ Supposons que $n = p_1 \cdots p_r$, et pour tout $i \in \{1, \cdots, r\}$, $p_i - 1$ divise $n - 1$. Soit $i \in \{1, \cdots, r\}$ et $a \in \mathbb{Z}$. Si p_i ne divise pas a, alors il est premier avec a et d'après le petit théorème de Fermat, $a^{p_i - 1} \equiv 1(p_i)$, et comme $p_i - 1 | n - 1$, $a^{n-1} \equiv 1(p_i)$ et donc $a^n \equiv a(p_i)$. C'est aussi vrai si p_i divise a. Ainsi, pour tout p_i,

$a^n \equiv a[p_i]$ donc chaque p_i divise $a^n - a$. Comme les (p_i) sont deux à deux premiers entre eux, alors $n = p_1 \cdots p_r$ divise $a^n - a$ donc $a^n \equiv a(n)$. n est donc un nombre de Carmichael. □

On a utilisé le fait suivant : Soient des entiers a_i deux à deux premiers entre eux, et b un entier. Le produit $a_1 \cdots a_r$ divise b si, et seulement si, chaque a_i divise b.

Proposition. Si p est un nombre premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.
Preuve. On écrit

$$(\mathbb{Z}/p\mathbb{Z})^\times = \bigsqcup_{d|p-1} G_d$$

où G_d désigne le nombre d'éléments d'ordre d dans le groupe multplicatif. De là, pour tout d,

- ou bien $G_d = \emptyset$ et alors $0 = |G_d| \leq \varphi(d)$ (l'indicatrice d'Euler),
- ou bien G_d est non vide : montrons alors que $|G_d| \leq \varphi(d)$. Notons R_d les racines du polynôme $X^d - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Soit $x \in G_d$, par définition x est d'ordre d donc appartient à R_d, et même le sous groupe $\langle x \rangle$ est dans R_d car pour tout $k \in \mathbb{Z}$, $(x^k)^d = x^{kd} = 1$. On a donc

  $$\langle x \rangle \subset R_d,$$

  le premier étant, par définition, de cardinal d, et le deuxième étant de cardinal au plus d car ce sont les racines d'un polynôme de degré d sur un corps. Donc c'est une égalité, et

  $$R_d = \langle x \rangle \sim \mathbb{Z}/d\mathbb{Z}.$$

  On peut conclure : si un élément y est dans G_d, il est en particulier dans R_d, donc isomorphe à un élément de $\mathbb{Z}/d\mathbb{Z}$. Mais il est de plus d'ordre d, donc il est isomorphe à un élément d'ordre d de $\mathbb{Z}/d\mathbb{Z}$, *i.e* à un générateur de $\mathbb{Z}/d\mathbb{Z}$. Comme il y a $\varphi(d)$ générateurs, nécessairement $|G_d| \leq \varphi(d)$.
  Ainsi,

  $$p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times| = |\bigsqcup_{d|p-1} G_d| = \sum_{d|p-1} |G_d| \leq \sum_{d|p-1} \varphi(d) = p - 1.$$

  Donc c'est une égalité et donc $\sum_{d|p-1} \varphi(d) - |G_d| = 0$, et comme tout est positif, pour tout d, $|G_d| = \varphi(d)$. En particulier, G_{p-1} est non vide donc il y a un élément d'ordre $p - 1$, et donc $\mathbb{Z}/p\mathbb{Z}^\times$ est cyclique. □

Il faut savoir redémontrer que $\sum \varphi(d) = p - 1$. Il faut connaître l'exemple du 561 comme nombre de Carmichaël.