

Feuille d'exercices n° 3

Compléments sur les nombres de Carmichael

On appelle *indicatrice de Carmichael* d'un entier $n \geq 2$ le maximum $\lambda(n)$ des ordres des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$.

On dit qu'un entier naturel n est un *nombre de Carmichael* si

1. n n'est pas premier, et
2. $a^{n-1} = 1 \pmod n$ pour tout entier a premier à n .

Exercice 1 (théorème de Carmichael). Soit $n \geq 2$ un entier naturel.

1. Montrer que $a^{\lambda(n)} = 1 \pmod n$ pour tout entier a premier à n . *Indication* : si a et b sont deux éléments d'ordres u et v dans $(\mathbb{Z}/n\mathbb{Z})^*$ alors $(\mathbb{Z}/n\mathbb{Z})^*$ contient un élément d'ordre $u \vee v$.
2. Réciproquement, si m vérifie $a^m = 1 \pmod n$ pour tout entier a premier à n , alors m est multiple de $\lambda(n)$.
3. En déduire la définition suivante équivalent des nombres de Carmichael : n est un nombre de Carmichael si n n'est pas premier et si $\lambda(n)|n-1$.

Exercice 2 (sur l'indicatrice de Carmichael). Les formules suivantes permettent de calculer l'indicatrice de Carmichael d'un nombre dont la décomposition en facteurs premiers est connue.

1. $\lambda(2) = 1$, $\lambda(4) = 2$ et $\lambda(2^k) = 2^{k-2}$ pour tout $k \geq 3$.
2. Si p est premier impair alors $\lambda(p^k) = \phi(p^k) = (p-1)p^{k-1}$.
3. $\lambda(rs) = \lambda(r) \vee \lambda(s)$ si $r \wedge s = 1$.

Exercice 3 (sur la structure des nombres de Carmichael). Soit $n \geq 2$ un nombre de Carmichael.

1. Montrer que n ne peut pas être multiple de 4. *Indication* : évaluer l'indicatrice $\lambda(n)$.
2. Montrer que tout nombre premier impair p diviseur de n vérifie $p-1|n-1$. En déduire que n ne peut pas être pair.
3. Soit p un nombre premier divisant n . Montrer que si p^2 divise n , alors $p(p-1)$ divise $\lambda(n)$ et conclure à une contradiction. En déduire que tout nombre de Carmichael est sans facteur carré.
4. Montrer qu'il n'existe pas de nombre de Carmichael avec seulement deux facteurs premiers. *Indication* : remarquer que si $q-1|pq-1$ alors $q-1|p-1$.
5. Soit p un nombre premier divisant n . Montrer que n/p est congru à 1 modulo $p-1$.

Exercice 4 (certains nombres de Carmichael).

1. Trouver les nombres de Carmichael de la forme $n = 3pq$ avec $3 < p < q$. *Indication* : partir de $n = 1 \pmod{q-1}$ et $n = 1 \pmod{p-1}$ pour déterminer p et q . Trouver les nombres de Carmichael de la forme $n = 5pq$ avec $5 < p < q$.
2. Soit $n = pqr$ avec $p < q < r$ premier est un nombre de Carmichael. Montrer qu'il existe des entiers t et u vérifiant $pr-1 = (q-1)t$ et $pq-1 = (r-1)u$. Calculer r en fonction de p , q et t , et montrer que

$$q = 1 + \frac{(p-1)(p+u)}{tu-p^2}.$$

En déduire qu'il existe un nombre fini de nombres de Carmichael de la forme pqr avec $p < q < r$ et p fixé.