

Recoranges: 120, 121, 127Définition: On appelle nombre de Carmichael tout entier $n \geq 3$ non premier tel que $a^{n-1} \equiv 1 \pmod n$ pour tout entier a premier avec n .Lemme: Un nombre de Carmichael est impairSoit $n \geq 3$ Preuve: Soit $n \geq 3$ un nombre de Carmichael. Si n est pair, $n-1$ est impair et $(-1)^{n-1} = -1$ (et $n \neq 2$ car n est non premier) donc n n'est pas un nombre de Carmichael.Lemme: Un nombre de Carmichael est sans facteur carré.Preuve: Soit n un nombre de Carmichael. Supposons que n admette un facteur carré: $n = p^2 q$ avec p premier impair et $q \geq 1$.

$$\text{Alors } (1+pq)(1-pq) = 1 - p^2 q^2 = 1 - qn \equiv 1 \pmod n$$

Donc $x = 1+pq \in \mathbb{Z}/n\mathbb{Z}$ est inversible d'inverse $1-pq$. Comme $p^2 q \neq 0 \pmod n$ on a $x \neq \bar{1}$ et avec:

$$(1+pq)^p = 1 + p^2 q + p^2 q \sum_{k=2}^p \binom{p}{k} p^{k-2} q^{k-2} \equiv 1 \pmod n$$

Donc x est d'ordre p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Si n est de Carmichael, alors $x^{n-1} = \bar{1}$ et donc $p \mid n-1 = p^2 q - 1 \nmid$.Théorème: (Korselt) Soit $n \geq 3$. L'ASSE

- 1) $\exists r \geq 3$ et $3p_1 < \dots < p_r$ des nombres premiers tels que $n = \prod_{j=1}^r p_j$ et pour tout $j \in \{1, \dots, r\}$, $p_j - 1 \mid n-1$
- 2) $n \notin \mathcal{P}$ et pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $x^n = x$
- 3) n est un nombre de Carmichael.

Preuve: "1) $\Rightarrow$ 2)" Soit $x = \bar{k} \in \mathbb{Z}/n\mathbb{Z}$, $k \in \{1, \dots, n\}$. Pour tout $j \in \{1, \dots, r\}$, on a:

- soit $p_j \mid k$ et dans ce cas, $p_j \mid k^n$ donc $k^n \equiv k \equiv 0 \pmod{p_j}$
- soit $p_j \nmid k$, donc $p_j \nmid k-1$ donc par Fermat, $k^{p_j-1} \equiv 1 \pmod{p_j}$.

Comme $p_j - 1 \mid n - 1$, on a aussi $k^{n-1} \equiv 1 \pmod{p_j}$ et $k^n \equiv k \pmod{p_j}$.
 On a donc dans tous les cas $k^n \equiv k \pmod{p_j}$ et donc $k^n \equiv k \pmod{n}$
 car $n = \prod_{j=1}^r p_j = \text{ppcm}(p_j)$ $p_j \mid k^n - k \quad \forall j \in [1; r]$
 Donc $n = \text{ppcm}(p_j) \mid k^n - k$ donc $k^n \equiv k \pmod{n}$

"2) $\Rightarrow$ 3)" Pour $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, on peut simplifier par x et alors $x^{n-1} \equiv 1$.
 L'entier n est donc de Carmichael.

"3) $\Rightarrow$ 1)" Écrivons $n = \prod_{j=1}^r p_j$, $r \geq 2$, $3 \leq p_1 < \dots < p_r$.
 Soit $j \in [1; r]$. $(\mathbb{Z}/p_j\mathbb{Z})^\times$ est d'ordre $p_j - 1$. $\exists x_j \in (\mathbb{Z}/p_j\mathbb{Z})^\times$, $\phi(x_j) = p_j - 1$.
 Par le théorème des restes chinois, il existe $x \in \mathbb{Z}/n\mathbb{Z}$ tel que
 pour tout j , $x \equiv x_j \pmod{p_j}$ donc $x \cdot n = 1$ car aucun p_j ne divise x .
 Comme n est de Carmichael, $x^{n-1} \equiv 1 \pmod{n}$.

Donc $x_j^{n-1} \equiv 1 \pmod{p_j}$ donc pour tout j , $p_j - 1 \mid n - 1$

$$\begin{aligned} x &\equiv x_j \pmod{n} \\ &\downarrow \\ x^{n-1} &\equiv x_j^{n-1} \pmod{n} \end{aligned}$$

Montrons que $r \geq 3$: Soit $n = p_1 p_2$, $p_1 < p_2$, $n - 1 = p_1 p_2 - 1 = p_1(p_2 - 1) + p_1 - 1$
 Comme pour tout j , $p_j - 1 \mid n - 1$, $p_2 - 1 \mid p_1(p_2 - 1) + p_1 - 1$ donc
 $p_2 - 1 \mid p_1 - 1 \nlessdot$ donc $r \geq 3$.

$$x^{n-1} \equiv 1 \pmod{n} \text{ donc } n \mid x^{n-1} - 1 \text{ donc } \prod_{j=1}^r p_j \mid x^{n-1} - 1$$

donc par Euclide, $\forall j \in [1; r]$, $p_j \mid x^{n-1} - 1$

$$\text{Donc } x^{n-1} \equiv x_j^{n-1} \equiv 1 \pmod{p_j}$$