

Dev n° 12

Ref : Jean Etienne Rombaldi
 "Mathématiques par l'agrégation :
 Algèbre et géométrie"
 p 329 / 330

Titre : Théorème de KorseltDéfinition :

On appelle nb de Carmichael tout entier $n \geq 3$ non premier tel que
 $a^{n-1} \equiv 1 [n] \quad \forall a$ premier avec n . (1^{er} $n = 561 = 3 \cdot 11 \cdot 17$)

Notre but est le thm suivant :

Thm : (Korselt)

Soit $n \geq 3$ un entier. On a équivalence entre :

- ① $\exists r \geq 3$ entier et $p_1, \dots, p_r \in \mathcal{P}$ t.q. $3 \leq p_1 < \dots < p_r$ et
 $n = p_1 \times \dots \times p_r$ et $\forall j \in \{1, \dots, r\}, p_j - 1 \mid n - 1$.
- ② n est un nombre de Carmichael.

Pour ceci, démontrons avant, les deux lemmes suivants :

Lemme (1) :

Un nb de Carmichael est impair.

Lemme (2) :

Un nb de Carmichael est sans facteur carré.

Demo : (Lemme 1)

Soit n nb de Carmichael.

Par l'absurde, s.q. n soit pair.

Alors, $n-1$ est impair : $(-1)^{n-1} = -1 \neq 1$ def nb carmichael
 car $n \neq 2$ comme n non premier

Donc, n n'est pas un nombre de Carmichael. $\sum \square$

Demo : (Lemme 2)

Soit n nb de Carmichael.

Par l'absurde, s.q. n admettent un facteur carré.

Donc, $\exists p \geq 3$ premier et $q \geq 1$ t.q. $n = p^2 q$.

On a :

$$(1+pq)(1-pq) = 1 - p^2 q^2 = 1 - qn \equiv 1 [n].$$

Donc,

$$x = 1+pq \in \mathbb{Z}_n \text{ est inversible d'inverse } 1-pq.$$

Donc,

$x = 1 + pq \in \mathbb{Z}/n\mathbb{Z}$ est inversible d'inverse $1 - pq$.

Comme $pq \not\equiv 0 [n]$ ($n = p^2q$ & pq) $\Rightarrow x = pq + 1 \not\equiv 0 + 1 [n]$
 $\Rightarrow x \neq 1 [n]$.

Et:

$$x^p = (1 + pq)^p = \sum_{k=0}^p \binom{p}{k} (pq)^k \quad \text{Binôme de Newton}$$
$$= 1 + p^2q + p^2q \sum_{k=2}^p \binom{p}{k} p^{k-2} q^{k-1} \equiv 1 [n]$$

On en déduit que x est d'ordre p dans $(\mathbb{Z}/n\mathbb{Z})^\times$

Comme n est un nb de Carmichael, on a $x^{n-1} \equiv 1 [n]$ et
 $p \mid (n-1) \Rightarrow p \mid (p^2q-1)$ IMPOSSIBLE.

Donc, n est sans facteur carré. $\square$

Demo: (thm)

$\boxed{1 \Rightarrow 2}$ $n = p_1 \times \dots \times p_r$, avec $3 \leq p_1$ est donc non premier.

Soit $k \in \mathbb{Z}$ t.q. $k \wedge n = 1$.

$\forall j \in \{1, \dots, r\}$, on a:

$p_j \nmid k$: $p_j \wedge k = 1 \Rightarrow k^{p_j-1} \equiv 1 [p_j]$ (thm Fermat)

Comme $n-1$ multiple de p_j-1 , on a:

$$k^{n-1} \equiv 1 [p_j].$$

Donc $\text{pperm}(p_1, \dots, p_r)$ divise $k^{n-1} - 1$.

Or $n = \text{pperm}(p_1, \dots, p_r)$.

Donc $k^{n-1} \equiv 1 [n]$.

$\boxed{2 \Rightarrow 1}$ S.q. n est un nombre de Carmichael.

Donc, n non premier, impair et sans facteur carré.

Donc, $\exists r \geq 2$ t.q. $n = p_1 \times \dots \times p_r$ avec $3 \leq p_1 < \dots < p_r$.

•) P.g. $p_i-1 \mid n-1 \quad \forall i \in \{1, \dots, r\}$:

$\forall i \in \{1, \dots, r\}$, $(\mathbb{Z}/p_i\mathbb{Z})^\times$ est cyclique d'ordre p_i-1 .

Donc, $\exists x_i \in (\mathbb{Z}/p_i\mathbb{Z})^\times$ d'ordre p_i-1 .

Par le thm des restes chinois, $\exists \tilde{x} \in \mathbb{Z}/n\mathbb{Z}$ vérifiant:

$$\forall i \in \{1, \dots, r\}, \quad \tilde{x} \equiv x_i [p_i]$$

Tout les x_i étant inversibles, $\tilde{x}$ l'est aussi dans $\mathbb{Z}/n\mathbb{Z}$.

Donc, $\tilde{x} \wedge n = 1$, et on a par h. $\tilde{x}^{n-1} \equiv 1 [n]$

Donc, $\forall i \in \{1, \dots, r\}$, $\tilde{x}^{n-1} \equiv 1 [p_i]$.

Donc, $\forall i \in \{1, \dots, r\}$, $x_i^{n-1} \equiv 1 [p_i]$

Donc, $p_i-1 \mid n-1$.

•) P.g. $r \geq 3$:

Par l'absurde, s.q. $r=2$.

Alors, $n = p_1 p_2$, avec $p_i-1 \mid n-1$.

On a,

$$n-1 = p_1(p_2-1) + (p_1-1)$$
$$= p_2(p_1-1) + (p_2-1)$$

Comme $p_i-1 \mid n-1$ on a donc $p_1-1 \mid p_2-1$ (par Gauss)

$$n-1 = p_1(p_2-1) + (p_1-1) \\ = p_2(p_1-1) + (p_2-1)$$

Comme $\begin{cases} p_1-1 \mid n-1 \\ p_2-1 \mid n-1 \end{cases}$ on a donc $\begin{cases} p_1-1 \mid p_2-1 \\ p_2-1 \mid p_1-1 \end{cases}$ (par Gauss)

Absurde !

Donc $r \geq 3$. $\square$

Annexe:

* Règles de calcul congruence :

↳ Si $a \equiv b[n]$ et $b \equiv c[n] \Rightarrow a \equiv c[n]$

$n \mid a-b$ et $n \mid b-c \Rightarrow n \mid a-b+b-c = a-c$

↳ Si $a \equiv b[n]$ et $a' \equiv b'[n]$ alors : $a+a' \equiv b+b'[n]$

$a-a' \equiv b-b'[n]$

$aa' \equiv bb'[n]$

$a^p \equiv b^p[n], \forall p \in \mathbb{N}$.

↳ si $p_1 \wedge p_2 = 1$, et $a \equiv b[p_1]$ et $a \equiv b[p_2] \Rightarrow a \equiv b[p_1 p_2]$

↳ $x \equiv 1[p_1]$ et $x \equiv 1[p_2]$ avec $p_1 \wedge p_2 = 1 \Rightarrow x \equiv 1[p_1 p_2]$

$\begin{cases} x-1 = m_1 p_1 \\ x-1 = m_2 p_2 \end{cases} \Rightarrow x-1 = p_1 p_2 m_3 \Leftrightarrow x \equiv 1[n].$

↳ $x \equiv 1[p_1 p_2]$ avec $p_1 \wedge p_2 \Rightarrow x \equiv 1[p_1]$ et $x \equiv 1[p_2]$

$x-1 = p_1 p_2 k \Rightarrow \begin{cases} x-1 = p_1 k_1 \Leftrightarrow x \equiv 1[p_1] \\ x-1 = p_2 k_2 \Leftrightarrow x \equiv 1[p_2] \end{cases}$

Démo: (thm)

1 $\Rightarrow$ 2 $n = p_1 \dots p_r$ avec $r \geq 3$ et donc n non premier.
Soit $k \in \mathbb{Z}$ t.q. $k \wedge n = 1$.

$\forall j \in \{1, \dots, r\}$ on a $p_j \nmid k$ soit $p_j \wedge k = 1$.

Donc, $k^{p_j-1} \equiv 1 [p_j]$ par Fermat.

Comme $n-1$ multiple de p_j-1 on a:

$$k^{n-1} \equiv 1 [p_j].$$

Et $p_1 \wedge \dots \wedge p_r = 1$, donc $k^{n-1} \equiv 1 [n]$

2 $\Rightarrow$ 1 $n = p_1 \dots p_r$ avec $r \in \mathbb{N}$ et $r \geq 2$ et $p_1 < \dots < p_r$.

•) $\prod_{j=1}^r p_j - 1 \mid n - 1$:

$\forall i \in \{1, \dots, r\}$, $(\mathbb{Z}/p_i\mathbb{Z})^*$ cyclique d'ordre $p_i - 1$.

Donc $\exists x_i \in (\mathbb{Z}/p_i\mathbb{Z})^*$ d'ordre $p_i - 1$:

$$x_i^{p_i-1} \equiv 1 [p_i].$$

Par le thm des restes chinois $\exists x \in \mathbb{Z}/n\mathbb{Z}$ vérifiant:

$$\forall j \in \{1, \dots, r\}, x \equiv x_j [p_j]$$

Tout les x_j étant inversibles $\Rightarrow x$ l'est dans $\mathbb{Z}/n\mathbb{Z}$.

$$\text{Donc, } x \wedge n = 1 \text{ et } x^{n-1} \equiv 1 [n]$$

$$\text{Donc, } \forall i \in \{1, \dots, r\}, x^{n-1} \equiv 1 [p_i]$$

$$\Rightarrow x_i^{n-1} \equiv 1 [p_i]$$

$$\text{Donc, } p_i - 1 \mid n - 1.$$

•) $\prod_{j=1}^r p_j \geq 3$:

Par l'absurde s.g. $r=2$.

Alors $n = p_1 p_2$ avec $p_i - 1 \mid n - 1$ (*)

$$\text{On a, } n - 1 = p_1(p_2 - 1) + (p_1 - 1)$$

$$= p_2(p_1 - 1) + (p_2 - 1)$$

Par (*), on a $p_1 - 1 \mid p_2 - 1$ et $p_2 - 1 \mid p_1 - 1 \Rightarrow \text{①}$

Korselt

12

Def: n nb de Carmichael si $\forall a$ premier avec n on a $a^{n-1} \equiv 1 [n]$ et n non premier

Thm: (Korselt)

$n \geq 3$.

① $\exists r \geq 3$ et $p_1, \dots, p_r \in \mathcal{P}$ t.q. $3 \leq p_1 < \dots < p_r$ et $n = p_1 \dots p_r$ et $\forall j \in \{1, \dots, r\}, p_j - 1 \mid n - 1$.

② n nb de Carmichael.

Lemme:

(1) n nb Carmichael est impair

(2) Sans facteur carré

Démo: (Lemme)

(1) Par l'absurde s.g. n est pair.

Alors, $n-1$ impair et $(-1)^{n-1} = -1 \neq 1$

(2) Par l'absurde, $n = p^2 q$ avec $p \in \mathcal{P}$.

$$\text{On a, } (1 + pq)(1 - pq) = 1 - p^2 q^2 = 1 - nq \equiv 1 [n]$$

Donc, $x = 1 + pq \in \mathbb{Z}/n\mathbb{Z}$ inversible.

Comme $pq \not\equiv 0 [n] \Rightarrow x \not\equiv 1 [n]$.

$$\text{Et: } x^p = 1 + p^2 q + p^2 \sum_{k=2}^{p-1} \binom{p}{k} p^{k-2} q^{k-1} \equiv 1 [n].$$

Donc, $o(x) = p$ dans $(\mathbb{Z}/n\mathbb{Z})^*$

Comme n nb de Carmichael on a $x^{n-1} \equiv 1 [n]$

Donc $p \mid n-1 \Leftrightarrow p \mid p^2 q - 1$ Impossible $\square$