

120
121
122
142

14, 10"

Rombaldi
p. 329-330

Nombres de Carmichael

Lemme : Soit $(a_i)_{i=1}^n \in \mathbb{Z}^n$ 2 à 2 premières entre eux. Alors $a_1 \dots a_n = a_1 \dots a_n$.

Pour $n=2$ entiers, on a $a_1 a_2 = (a_1 \wedge a_2) \frac{(a_1 \vee a_2)}{1} = a_1 a_2$. En supposant le lemme vrai pour $n-1$

entiers, on a $a_1 \dots a_n = (a_1 \dots a_{n-1}) \wedge a_n \frac{(a_1 \dots a_{n-1}) \vee a_n}{1} = a_1 \dots a_n$.

Proposition : Un nombre de Carmichael est impair et sans facteurs carrés.

Soit $n \geq 3$ de Carmichael. Si n est pair, alors $(-1)^{n-1} = -1 \not\equiv 1 \pmod{n}$ c'est absurde.

Si $n = p^2 q$ où p premier, $q \in \mathbb{N}$, alors $\bar{x} = \overline{1+pq} \in \mathbb{Z}_{n\mathbb{Z}}^\times$ car $(1+pq)(1-pq) = 1 - p^2 q^2 \equiv 1 \pmod{n}$. De plus $(1+pq)^p \equiv 1 + p^2 q + p^2 q \sum_{k=2}^p \binom{p}{k} p^{k-2} q^{k-1} \equiv 1 \pmod{n}$, donc $\text{ord}(\bar{x}) \mid p$. Puisque $\bar{x} \neq 1$ (sinon $p^2 q \mid pq$), on a $\text{ord}(\bar{x}) = p$. Comme n de Carmichael, $\bar{x}^{n-1} \equiv 1$ et $\text{ord}(\bar{x}) \mid n-1$, ie $p \mid p^2 q - 1$ absurde.

Théorème (Korselt) : Soit $n \geq 3$, on a : $n = \prod_{i=1}^r p_i$ où p_i premier, $r \geq 3$ et $p_i - 1 \mid n-1 \forall i \in \{1, r\}$

$\Leftrightarrow n$ non premier et $\forall a \in \mathbb{Z} \ a^n \equiv a \pmod{n} \Leftrightarrow n$ est de Carmichael.

($\Rightarrow$) Si $n = \prod_{i=1}^r p_i$ où p_i premier et $r \geq 3$ alors n non premier. Soit $a \in \mathbb{Z}$, alors $\forall i \in \{1, r\}$

* Soit $p_i \nmid a$ et $a^n \equiv a \pmod{p_i}$

+ Soit $p_i \mid a$ et $a^{n-1} \equiv 1 \pmod{p_i}$. Puisque $p_i - 1 \mid n-1$, on a $a^{n-1} \equiv 1 \pmod{p_i}$

$\Rightarrow$ Dans les 2 cas $a^n \equiv a \pmod{p_i}$ et $\forall i \in \{1, r\} \ p_i \mid a^n - a$. D'après le lemme $p_1 \dots p_r = p_1 \dots p_r = n$ donc $n \mid a^n - a$ et $a^n \equiv a \pmod{n}$.

($\Rightarrow$) Si n non premier vérifie $\forall a \in \mathbb{Z} \ a^n \equiv a \pmod{n}$, alors pour $a \wedge n = 1$ on a $\bar{a} \in \mathbb{Z}_{n\mathbb{Z}}^\times$. On en déduit que $\bar{a}^{n-1} \equiv 1 \pmod{n}$ et n de Carmichael

($\Rightarrow$) Si n de Carmichael, par la proposition $n = \prod_{i=1}^r p_i$ où p_i premieres, $r \geq 2$. Puisque $\forall i \in \{1, r\}$

$\mathbb{Z}_{p_i\mathbb{Z}}^\times$ cyclique, $\exists [x_i]_{p_i} \in \mathbb{Z}_{p_i\mathbb{Z}}^\times$ generateurs. Par le lemme Chinois $\exists x \in \mathbb{Z}$ tel que $\forall i \in \{1, r\}$

$[x]_{p_i} = [x_i]_{p_i}$. Alors $x \not\equiv 0 \pmod{p_i}$ et $p_i \nmid x$, donc $x \wedge n = 1$. On en déduit que $x^{n-1} \equiv 1 \pmod{n}$, et

$\forall i \in \{1, r\} \ x^{n-1} \equiv x_i^{n-1} \equiv 1 \pmod{p_i}$. Donc $\text{ord}([x_i]_{p_i}) \mid n-1$, de $p_i - 1 \mid n-1$

Si $r=2$ et $n = p_1 p_2$ avec $p_1 < p_2$. Puisque $p_1 - 1 \mid n-1$ et $n-1 = p_1 p_2 - 1 = p_1(p_2 - 1) + p_1 - 1$, on a $p_1 - 1 \mid p_1 - 1$. C'est absurde donc $r \geq 3$.

- * $n=2$ $a_1 a_2 = (a_1 n a_2) \pmod{n} \rightarrow a_1 n \dots 1 a_n = (a_1 \dots a_{n-1}) n a_n \pmod{n} = a_1 \dots a_n \pmod{n} = 1 \pmod{n}$
- * $n \geq 3$ pair $\rightarrow (-1)^{n-1} = -1 \pmod{n} \rightarrow n = p^2 q \rightarrow x = 1+pq \in \mathbb{Z}_n \setminus \{1\} \rightarrow x^{n-1} \equiv 1 \pmod{n} \rightarrow x \neq 1 \rightarrow p|n-1 \nmid \text{Carm}$
- * $(\Rightarrow) \forall a \in \mathbb{Z}_n, \exists j | a \Rightarrow a^{n-1} = a \pmod{n}$, $\exists j | a \Rightarrow a^{n-1} \equiv 1 \pmod{n} \rightarrow \exists j | a^{n-1} = a \rightarrow n | a^{n-1} - a \checkmark$
- * $(\Rightarrow) a | n \Rightarrow a \in \mathbb{Z}_n \Rightarrow a^{n-1} \equiv 1 \pmod{n}$ Carmi
- * $(\Rightarrow) n = \prod p_i, R \geq 2, \exists n_j$ gen de $\mathbb{Z}_{p_i} \Rightarrow$ un chinois $\exists n, (n_j) = (p_j) \rightarrow x \equiv 0 \pmod{p_i} \rightarrow x^{n-1} \equiv 1 \pmod{n} \rightarrow \exists j | a^{n-1} = a \rightarrow n | a^{n-1} - a \checkmark$

Définition: Un nombre $n \in \mathbb{N}$ est de Carmichael s'il n'est pas premier et vérifie

$$\forall a \in \mathbb{Z}_n, a^{n-1} \equiv 1 \pmod{n}$$

Exemples: 561, 1105, 1729 sont de Carmichael

- * $561 = 3 \times 11 \times 17$ et $\forall a \in \mathbb{Z}_n, a^{560} \equiv 1 \pmod{n}$ donc $a^{560} \equiv 1 \pmod{3} = a^{560} \equiv 1 \pmod{11} = a^{560} \equiv 1 \pmod{17} = 1$. Par Fermat $a^2 \equiv 1 \pmod{3}, a^{10} \equiv 1 \pmod{11}, a^{16} \equiv 1 \pmod{17}$, or 2 | 560, 10 | 560 et 16 | 560 donc $a^{560} \equiv 1 \pmod{3}, a^{560} \equiv 1 \pmod{11}, a^{560} \equiv 1 \pmod{17}$ donc $a^{560} \equiv 1 \pmod{561}$ et 561 de Carmichael
- * $1105 = 5 \times 221 = 5 \times 13 \times 17$ où 4 | 1104, 12 | 1104 et 16 | 1104