Nombres Carmichael

Contexte : Est ce que le théorème de Fermat est encore vrai si on ne suppose pas p premier ? Non, par exemple c'est faux pour $n = 4$ car $3^4 = (-1)^4 = 1[4]$. Néanmoins il y a des nombres non premiers pour lesquels la propriété est vraie : par exemple 561 est le plus petit de ces nombres. On les appele nombres de Carmichael. Le développement suivant démontre quelques propriétés de ces nombres. Il a été montré récemmenent qu'il en existe une infinité.

Théorème 1 (Korselt)**.** *Soit n un entier naturel. Les assertions suivantes sont équivalentes :*
- *n est un nombre de Carmichael.*
- *n est sans facteur carré et $\forall p \in \mathcal{P} | n, p-1|n-1$.*

Proposition 2. *Soit n un nombre de Carmichael, alors il est impair et composé d'au moins trois facteurs premiers.*

Proposition 3. *Soit $n = pqr$ un nombre de Carmichael tel que $p < q < r$ soit trois nombres premiers. Alors q et r sont bornées en p.*

Commençons par prouver le théorème :

Démonstration. Soit n un nombre de Carmichael. Commençons par montrer qu'il est sans facteur carré. Supposons qu'il existe un nombre premier p tel que $p^2|n$. Or par définition, $p^n = p[n]$ donc $p^2|p^n - p$ donc $p^2|p$ car $n \geq 2$. Mais c'est impossible. Donc n est sans facteur carré. On pose $n = p_1 \cdots p_s$ où les p_i sont des nombres premiers distincts. Alors comme $\mathbb{Z}/p_i\mathbb{Z}^*$ est cyclique alors il existe $b_i \in \mathbb{Z}/p_i\mathbb{Z}^*0$ tel que b_i est d'ordre $p_i - 1$ dans $\mathbb{Z}/p_i\mathbb{Z}^*$. Par le théorème des restes chinois il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $b = b_i[p_i]$ pour tout i. Donc $b^n = b[n]$ car n est de Carmichael. Donc $b_i^n = b_i[p_i]$ pour tout i. Donc $p_i - 1|n-1$ pour tout i.

Soit n sans facteur carré tel que si p un nombre premier divise n alors $p-1|n-1$. On pose $n = p_1 \cdots p_s$ où les p_i sont premiers. Soit a un entier. Alors pour tout i : $a^{p_i - 1} = 1[p_i]$ si p_i ne divise pas a et $a^n = a[p_i]$. Or $p_i - 1|n-1$ donc $a^n = a[p_i]$ dans les deux cas. Donc $a^n = a[n]$ et n est un nombre de Carmichael.

□

Prouvons la première proposition :

Démonstration. Si n était pair alors on aurait $(-1)^n = 1[n]$ ce qui est impossible car $n \geq 3$.

Supposons que $n = pq$ avec $p < q$ deux nombres premiers. Alors $q-1|n-1$ or $n - 1 = pq - 1 = (p-1)q + q - 1$. Donc $q-1|p-1$ car $q-1$ est premier avec q. Donc $q - 1 \leq p - 1$. C'est exclu. Donc n admet au moins trois facteurs.

□

Prouvons la seconde : [attention la solution propose un léger raccourci à la preuve de Gourdon]

Démonstration. $q-1$ divise $n - 1 = pqr - 1 = (pr-1)q + (q-1)$ donc $q-1|pr-1$ comme avant. De même $r-1|pq-1$. On en déduit : [ACHTUNG GROS TRICK] $(q-1)(r-1)$ divise $(pr-1)(pq-1) - p^2(r-1)(q-1) = 1 - pr - pq - p^2(1-r-q) = p^2(r+q) - pr - pq + 1 - p^2$. Donc $(q-1)(r-1) \leq p^2(r+q) \leq 2p^2r$. D'où : $qr \leq 2p^2r + r + q - 1 \leq 2r(p^2+1)$ car $q \leq r$. Donc en

divisant par r on a : $q \leq 2(p^2+1)$. Or $r-1 \leq pq-1$. Donc $r \leq pq \leq 2p(p^2+1)$. Donc r et q sont bornées en p.

□

Références : Gourdon - Algèbre (page)

Remarque de présentation : Dans le cadre de la leçon 121 nombre premiers on pourra présenter les trois résultats. Néanmoins dans la leçon 120 $\mathbb{Z}/n\mathbb{Z}$ il est préférable de remplacer le troisième résultat qui n'utilise aucunement les congruences par un lemme fondamental (et admis) pour le premier théorème :

Lemme 4. *Soit p premier. $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique.*

Démonstration. On note $O(d)$ les élements de $\mathbb{Z}/p\mathbb{Z}^*$ d'ordre d. Alors $\sum_{d|p-1} |O(d)| = p-1$. Soit $d|p-1$. Si $O(d)$ est non vide, alors il existe $x \in \mathbb{Z}/p\mathbb{Z}^*$ tel que x soit d'ordre d. Donc $\langle x \rangle$ est inclus dans les racines du polynôme sur $\mathbb{Z}/p\mathbb{Z}$ $X^d - 1$. Or on est sur un anneau intègre donc $X^d - 1$ admet au plus d racines. Donc par cardinalité, les racines du polynôme sont exactement les élements de $\langle x \rangle$. Si $y \in O(d)$ est un autre élement. Alors $y \in \langle x \rangle$ car y est racine du polynôme $X^d - 1$. Or $\langle x \rangle \sim \mathbb{Z}/d\mathbb{Z}$ est cyclique et admet donc $\varphi(d)$ générateurs. Donc $|O(d)| \leq \varphi(d)$. Donc :

$$\sum_{d|p-1} |O(d)| \leq \sum_{d|p-1} \varphi(d) = p-1$$

Donc $|O(d)| = \varphi(d)$ pour tout d divisant $p-1$. Donc en particulier $O(d-1)$ n'est pas vide et donc $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique.

□