102
120
121

Théorème de Dirichlet faible

- Théorie de Galois, GOZARD, p 84
- Oraux X-ENS Algèbre 1, FGN, p 136

GOZ 67 **Déf** : On note $\mu_n = \{z \in \mathbb{C} ; z^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{C}$.

On appelle racine primitive n-ième de l'unité tout générateur de μ_n, càd tout élément $\xi \in \mu_n$ tel que $\xi^d \neq 1$ pour $1 \leq d < n$.

On note μ_n^* cet ensemble.

Déf : Soit $n \in \mathbb{N}^*$. On appelle n-ième polynôme cyclotomique le polynôme :

$$\Phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi)$$

Théorème de Dirichlet faible : Soit $n \geq 1$. Alors il existe une infinité de nombres premiers p vérifiant $p \equiv 1 \ [n]$.

Dém :

GOZ 84 FGN1 136 On montre que si p est un nombre premier qui divise $\Phi_n(a)$, où $a \in \mathbb{Z}$, mais aucun $\Phi_d(a)$ où d décrit l'ensemble des diviseurs stricts de n, alors $p \equiv 1 \ [n]$

Soit p premier qui vérifie l'hypothèse.

Comme $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ et que $p \mid \Phi_n(a)$ alors $p \mid a^n - 1$

Ainsi dans $\mathbb{F}_p^*$: $\bar{a}^n = \bar{1}$

Soit w l'ordre de $\bar{a}$ dans $\mathbb{F}_p^*$. Alors on a que $w \mid n$.

On montre que $w = n$.

On suppose que $w < n$. On a dans $\mathbb{F}_p$ on a :

$$\bar{a}^w - \bar{1} = \prod_{d \mid w} \overline{\Phi_d(a)}$$

$||x| - |y|| \leq |x - y|$

le $a = 3N!$ ne sert pas de manière pure : cela permet d'avoir un grand nombre qui contient tous les facteurs 1° jusqu'à N. Et le "3" permet que $|\Phi_n(a)| \geq 2$ donc admet un diviseur premier

Mais alors on a que $\bar{a}^m - \bar{1} = \bar{0}$ et comme $\mathbb{F}_p$ est un corps donc intègre, il existe $d | m$ donc qui divise n tel que $\overline{\Phi_d(a)} = \bar{0}$ c'à d $p | \Phi_d(a)$. Or d est un diviseur strict de n. Contradiction.

Donc $m = n$.

Ainsi $\bar{a}$ est d'ordre n dans $\mathbb{F}_p^*$ qui est d'ordre $p-1$, donc d'après le théorème de Lagrange : $n | p-1$.

Donc $p \equiv 1 \ [n]$.

Boz 84

On montre le théorème

Soit $N \in \mathbb{N}^*$. On pose $a = 3N!$

Comme $\Phi_n(x) \in \mathbb{Z}[x]$, alors $\Phi_n(a)$ est entier et : $|\Phi_n(a)| = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} |a - e^{2i\frac{k\pi}{n}}|$

$$\geq \pi \left| |a| - |e^{2i\frac{k\pi}{n}}| \right|$$

$$\geq \pi |a - 1|$$

$$\geq a - 1 \quad \text{car } a \geq 3$$

$$\geq 2$$

Soit p un diviseur premier de $\Phi_n(a)$ (existe car $\Phi_n(a) \neq \pm 1$)

- Si $p \leq N$, alors p divise a car est contenu dans $N!$

  Ainsi p divise tout entier de la forme $\sum_{i=1}^{k} z_i a^i$ avec $z_i \in \mathbb{Z}$ (car ce nombre est un multiple de a)

  En particulier, p divise $(\Phi_n(a) - \Phi_n(0))$ car $\Phi_n(0)$ correspond au terme constant.

  Ainsi p divise $\Phi_n(0) = \pm 1$ (car $\Phi_n \in \mathbb{Z}[x]$

et $x^n - 1 = \prod_{d|n} \Phi_d(x)$ donc

$-1 = \prod_{d|n} \Phi_d(a)$ et c'est un produit d'entiers)

Or p est premier, contradiction.

Donc $p > N$.

- On suppose qu'il existe s diviseur strict de n tq $p \mid \Phi_s(a)$.

Comme $x^n - 1 = \prod_{d|n} \Phi_d(x)$ et que $\Phi_n(x)$ et $\Phi_s(a)$, alors $p^2 \mid a^n - 1$ et donc $\bar{a}$ est racine de multiplicité ≥ 2 du polynôme $x^n - \bar{1}$ de $\mathbb{F}_p[x]$.

Ainsi $x^n - \bar{1} \in \mathbb{F}_p[x]$ possède une racine multiple.

~~C'est absurde car $x^n - \bar{1}$ est premier avec sa dérivée $\bar{n} x^{n-1}$ dans $\mathbb{F}_p[x]$ (d'après le théorème~~

Or la dérivée de $x^n - \bar{1}$ est $\bar{n} x^{n-1}$.

On peut supposer que p ne divise pas n en prenant N assez grand car $p > N$. Ainsi comme $\bar{a}$ est non nul (car p ne divise pas a car sinon $p \leq N$), alors $\bar{a}$ ne peut pas être racine de cette dérivée.

Donc $\bar{a}$ n'est pas racine double.

Contradiction.

Ainsi p divise $\Phi_n(a)$ mais aucun $\Phi_s(a)$ où s décrit l'ensemble des diviseurs stricts de n.

Donc $p \equiv 1 [n]$.

En conclusion, pour tout $N \in \mathbb{N}^*$, il existe p

premier tel que $p > N$ et $p \equiv 1 [n]$.
Ainsi il existe une infinité de nombres premiers de la forme $kn + 1$ avec $k \in \mathbb{N}^*$.

Remarques :

1) Le théorème de Dirichlet peut dit :
$\forall a, b \in \mathbb{N}^*$ tel que $a \wedge b = 1$, il existe une infinité de nombres premiers de la forme $a + kb$ où $k \in \mathbb{N}^*$.
Ici on a pris $a = 1$ et $b = n$.