13min30 sans demo sur $\Phi_d$ et sans infinité nb 1°

# THÉORÈME DE DIRICHLET FAIBLE

10

Gou Alg Pb 10 p 92

**Prérequis:**
- Lagrange
- multiplicité racines
- polynômes cyclotomiques.

**Lemme:** Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{N}$. Soit $p$ un nombre premier divisant $\Phi_n(a)$ où $\Phi_n$ est le $n$° polynôme cyclotomique. Alors on a $p | n$ ou $p \equiv 1 [n]$.

**Dém:** On a $X^n - 1 = \prod_{d|n} \Phi_d$ (on peut le démontrer cf def pt uné des poly cyclo)

$= \Phi_n \times \prod_{\substack{d|n \\ d \neq n}} \Phi_d$ d'où $a^n - 1 = \Phi_n(a) \times \prod_{\substack{d|n \\ d\neq n}} \Phi_d(a)$

Comme $p | \Phi_n(a)$ par hypothèse, et que $\Phi_d \in \mathbb{Z}[X]$, alors $p | a^n - 1$ i.e $a^n \equiv 1 [p]$.

On note $m$ l'ordre de $\bar{a}$ dans le sous-groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$, comme $a^n \equiv 1 [p]$ alors $m | n$. On a alors deux cas.

- Si $m = n$, alors $\bar{a}$ est d'ordre $n$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ donc par théorème de Lagrange, $n \,|\, |(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$ i.e. $p \equiv 1 [n]$.

- Sinon $m < n$. On note $I = \{d \in \mathbb{N},\ d|n,\ d \neq n\ d \nmid m\}$. alors

$X^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \left(\prod_{d|m} \Phi_d\right) \times \left(\prod_{d \in I} \Phi_d\right) = \Phi_n \cdot (X^m - 1)\left(\prod_{d\in I} \Phi_d\right).$

Comme $p | \Phi_n(a)$ et $a^m \equiv 1 [p]$, $\bar{a}$ est racine de $\Phi_n$ et de $X^m - \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. donc $\bar{a}$ est racine au moins double de $X^n - \bar{1}$.

Ainsi $(X - \bar{a}) | X^n - \bar{1}$ et $(X - \bar{a}) | \bar{n} X^{n-1}$ donc $X - \bar{a} | \bar{n} X^{n-1} \times X - \bar{n}(X^n - \bar{1}) = \bar{n}$ dans $\mathbb{Z}/p\mathbb{Z}$. Ce n'est possible que si $n \equiv 0 [p]$ i.e $p | n$. regarder les degrés.

Si $p \nmid n$ alors $X^n - \bar{1} \wedge \bar{n} X^{n-1} = 1$ donc $X^n - 1$ est à racines simples sur $\mathbb{F}_p$ 3

**Thm de Dirichlet faible:** Soit $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers $p$ tels que $p \equiv 1 [n]$.

**Dém:** On raisonne par l'absurde et on suppose qu'il n'y a qu'un nombre fini de nombres premiers de cette forme. On les note $p_1, \dots, p_r$.

On pose $a = 3 n p_1 \cdots p_r > n$ car $p_i \geq 2$. ← problème: faut avoir montré que $r \geq 1$ pour avoir $a > n$.

- Comme on a $X^n - 1 = \prod_{d|n} \Phi_d$, en évaluant en zéro, $-1 = \prod_{d|n} \Phi_d(0)$

or $\Phi_d \in \mathbb{Z}[X]$ donc $\Phi_n(0) = \pm 1$

Et de plus, $\Phi_n(a) \equiv \Phi_n(0) [a]$. c'est vrai pour tout polynôme. $\Phi_n(0)$ est le coeff constant de $\Phi_n$

Donc $\Phi_n(a) \equiv \pm 1 [a]$.

à faire en entier peut être

• Si $n = 1$, on a le résultat car il y a une infinité de nombres premiers :

Supposons qu'il n'y en ait qu'un nb fini $q_1, \dots, q_m$. On pose $N = q_1 \cdots q_m + 1$.

Comme $N > 1$, il existe $p$ premier divisant $N$. On a $p \mid N$ et $p$ est l'un des $q_i$ donc $p \mid N - q_1 \cdots q_m = 1$. C'est absurde

• Sinon, $n \geq 2$. On note $\mu_n^*$ l'ensemble des racines primitives $n$-ièmes de l'unité

On a $\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$ d'où $\Phi_n(a) = \prod_{\zeta \in \mu_n^*} (a - \zeta)$

ainsi $|\Phi_n(a)| = \prod_{\zeta \in \mu_n^*} |a - \zeta| \geq \prod_{\zeta \in \mu_n^*} (a - \underbrace{|\zeta|}_{=1}) > 1$ car ~~$a \geq n \geq 2$~~ $a > 2$

or $\Phi_n(a) \in \mathbb{Z}$ donc $|\Phi_n(a)| \geq 2$.

• Ainsi il existe $p$ un nombre premier divisant $\Phi_n(a)$. Alors d'après le lemme, on a $p \mid n$ ou $p \equiv 1 [n]$

→ Si $p \equiv 1 [n]$ alors $p$ est l'un des $p_i$ donc $p \mid a$. Or $\Phi_n(a) \equiv \pm 1 [a]$

d'où $\Phi_n(a) \equiv \pm 1 [p]$. or $\Phi_n(a) \equiv 0 [p]$. C'est absurde

→ d'où $p \mid n$ mais alors $p \mid a$ et on arrive aussi à une absurdité.

Donc dans tous les cas, on obtient une absurdité.

(Si il reste du temps, on peut montrer les propriétés sur les polynômes cyclotomiques.)

+ faire explicat° du a

Dans anneaux $\mathbb{Z}/_n\mathbb{Z}$ = on fait en plus $X^n - 1 = \prod_{d \mid n} \Phi_d$

Dans nb premiers = on démontre avant le cas $n = 1$ ~~[illegible]~~ en expliquant que la démo a moins de prérequis.