Théorème de Dirichlet (faible)

Leçons : 102, 120, 121, 141

Réf. : FGN, Algèbre 1 4.18 p 31

Perrin, Cours d'algèbre p 81 (pour m.q. $\Phi_n \in \mathbb{Z}[X]$)

Th. : (Dirichlet faible)

Soit $n \in \mathbb{N}$, $n \geq 1$.

Alors il existe une infinité de nombres premiers congrus à 1 modulo n.

Notations :

- $P_n = X^n - 1 \in \mathbb{Q}[X]$, $K = D_{\mathbb{Q}}(P_n)$ $(\neq \emptyset)$
- $\mu_n = \{\text{racines } n\text{-ièmes de l'unité}\} = \{\text{racine de } P_n \text{ dans } K\}$
- $\mu_n^* = \{\text{racines } n\text{-ièmes primitives de l'unité}\}$
- $\Phi_n = \prod_{\zeta \in \mu_n^*} (X - \zeta)$ le n-ième poly. cyclotomique, $\Phi_n \in K[X]$.
- on admet que $X^n - 1 = \prod_{d \mid n} \Phi_d$, et on pose $F_n = \prod_{\substack{d \mid n \\ d < n}} \Phi_d$

1) M.q. $\Phi_n \in \mathbb{Z}[X]$ par récurrence sur n : on en a besoin pour pouvoir écrire " $p \mid \Phi_n(a)$ " où p premier, $a \in \mathbb{Z}$ et pour projeter dans $\mathbb{F}_p$.

$n \geq 1$. Soit (H_n) : $\forall k \leq n$, $\Phi_k \in \mathbb{Z}[X]$.

- $n = 1$: $\Phi_1 = X - 1$ donc (H_1) vérifiée.
- soit $n \geq 2$. OSP (H_{n-1}) vérifiée. M.q. (H_n) est aussi vérifiée.

On a : $P_n = \Phi_n F_n$ dans $K[X]$

$P_n \in \mathbb{Z}[X]$, et par hypothèse de récurrence, $F_n \in \mathbb{Z}[X]$.

F_n étant unitaire, on peut effectuer la division euclidienne de P_n par F_n.

$\exists\, Q, R \in \mathbb{Z}[X]$ / $P_n = QF_n + R$ avec $\deg(R) < \deg(F_n)$ ou $R = 0$

On a $\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset K[X]$, donc on a également $P_n = QF_n + R$ dans $K[X]$.

D'où $\Phi_n F_n = QF_n + R$

$$\underbrace{F_n(\Phi_n - Q)}_{\deg \geq \deg F_n \text{ si } \Phi_n - Q \neq 0} = \underbrace{R}_{=0 \text{ ou } \deg(R) < \deg F_n}$$

donc $\boxed{\Phi_n = Q \in \mathbb{Z}[X] \text{ et } (H_n) \text{ est vérifiée.}}$

2) Soit $a \in \mathbb{Z}$, p premier tq $p \mid \Phi_n(a)$ et $\forall d \mid n, d < n, p \nmid \Phi_d(a)$

Π.q. $p \equiv 1 [n]$.

- $p \mid \Phi_n(a)$ donc $p \mid a^n - 1$ donc $a^n \equiv 1 [p]$ donc $a^n \wedge p = 1$

donc $\boxed{a \wedge p = 1}$.

Soit $\bar{a}$ la classe de a dans $\mathbb{F}_p$.

$a \wedge p = 1$ donc $\bar{a} \in \mathbb{F}_p^\times$, et $\bar{a}^n = \bar{a}^n = \bar{1}$ donc $\boxed{o(\bar{a}) \mid n}$ (ordre dans $\mathbb{F}_p^\times$)

- Π.q. $o(a) = n$ par l'absurde

Si $o(\bar{a}) < n$, alors $\exists d \mid n, d < n$ tq $o(a) = d$.

On a donc $\bar{a}^d = \bar{1}$

donc $\bar{0} = \bar{a}^d - \bar{1} = \overline{a^d - 1} = \overline{\prod_{k \mid d} \Phi_k(a)} = \prod_{k \mid d} \overline{\Phi_k(a)}$

et $\mathbb{F}_p$ étant intègre, $\exists k \mid d$ tq $\overline{\Phi_k(a)} = \bar{0}$

donc $\exists k \mid n, k < n$ tq $p \mid \Phi_k(a)$ absurde.

donc $\boxed{o(\bar{a}) = n}$

- $\bar{a}$ est d'ordre n dans $\mathbb{F}_p^\times$ de cardinal $p - 1$

donc $n \mid p - 1$

donc $\boxed{p \equiv 1 [n]}$

3) Montrer par l'absurde le Th. de Dirichlet faible

a°/ Se ramener à chercher a et p du 2)

On suppose qu'il existe un nombre fini q de nombres premiers congrus à 1 modulo n

Si $q = 0$, on pose $N = n$

Si $q \geq 1$, on pose $N = n p_1 \dots p_q$ où $p_1 \dots p_q$ sont les ...

S'il existe $a \in \mathbb{Z}$, p premier tq $p \mid \Phi_N(a)$ et $\forall d \mid N, d < N$, $p \nmid \Phi_d(a)$

alors $p \equiv 1 \ [N]$

donc $p \wedge p_i = 1$ donc $\boxed{p \neq p_i \ \forall \ 1 \leq i \leq q}$

et $\exists \lambda \in \mathbb{Z} \ / \ p + (\lambda p_1 \dots p_q) n = 1$ donc $\boxed{p \equiv 1 \ [n]}$

b°/ Trouver de tels a et p

Φ_N et $F_n = \prod_{\substack{d \mid N \\ d < N}} \Phi_d$ sont scindés sur K (et à racines simples, mais ça ne sert à rien)

On $\mu_N = \prod_{d \mid N} \mu_d^*$, donc $\boxed{\Phi_N \wedge F_N = 1 \text{ dans } K[X]}$.

On a $\Phi_N, F_N \in \mathbb{Q}[X]$ et le pgcd est invariant par extension de corps (algorithme d'Euclide est le même), donc $\boxed{\Phi_N \wedge F_N = 1 \text{ dans } \mathbb{Q}[X]}$.

D'après le Théorème de Bézout,

$\exists U_1, V_1 \in \mathbb{Q}[X] \ / \ U_1 \underbrace{\Phi_N}_{\in \mathbb{Z}[X]} + V_1 \underbrace{F_N}_{\in \mathbb{Z}[X]} = 1$

Soit $a \in \mathbb{Z} \ / \ U_2 = a U_1 \in \mathbb{Z}[X]$

$V_2 = a V_1 \in \mathbb{Z}[X]$

On a alors : $U_2 \Phi_N + V_2 F_N = a$ dans $\mathbb{Z}[X]$

donc $\boxed{U_2(a) \Phi_N(a) + V_2(a) F_N(a) = a \text{ dans } \mathbb{Z}}$ (*)

++ Rq : . Si $U_2(a) = a\,U_1(a) = 0$ ou $V_2(a) = a\,V_1(a) = 0$, on remplace a par $b = ka$ tq b ne soit racine ni de U_1 ni de V_1

. De même on choisit a tq $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$

Soit p premier tq $p \mid \Phi_N(a)$.

Alors $p \mid a^N - 1$ donc comme au 2), $\underline{a \wedge p = 1}$.

p ne divise alors pas $F_N(a)$ car sinon d'après (*), on aurait $p \mid a$

Donc | pour tout $d \mid N$, $d < N$, $p \nmid \Phi_d(a)$

donc $p \equiv 1\ [N]$ et d'après 3) a°/ | $p \equiv 1\ [n]$, $p \neq p_i$ $\forall 1 \leq i \leq q$

ce qui conclut le raisonnement par l'absurde