Théorème de Dirichlet (faible)

Recasage: 102, 120, 121

Réf: FGN Algèbre 1, p 135

Polynômes cyclotomiques: $\Phi_1 = X-1$, $\forall n \geq 2$ $\Phi_n = \prod_{k \wedge n = 1} (X - e^{\frac{2ik\pi}{n}})$

(1) $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

Si $\zeta \in \mathcal{U}_n$, si d est l'ordre de ζ dans $\mathbb{C}^*$, on a $\zeta \in \mu_d^*$ et on sait que $d \mid n$.
Réciproquement, si $\zeta \in \mu_d^*$ pour un $d \mid n$, on a bien $\zeta \in \mathcal{U}_n$. Par unicité de l'ordre dans un groupe, les μ_d^* sont disjoints et on a donc $\mathcal{U}_n = \bigsqcup_{d \mid n} \mu_d^*$.
Donc $X^n - 1 = \prod_{\zeta \in \mathcal{U}_n} (X-\zeta) = \prod_{d \mid n} \prod_{\zeta \in \mu_d^*} (X-\zeta) = \prod_{d \mid n} \Phi_d$.

On montre par récurrence forte que $\Phi_n \in \mathbb{Z}[X]$. Déjà, $\Phi_1 = X-1 \in \mathbb{Z}[X]$.
Supposons que le résultat soit vrai pour tout $d < n$. Alors $P := \prod_{\substack{d \mid n \\ d < n}} \Phi_d \in \mathbb{Z}[X]$
On sait que $X^n - 1 = \Phi_n(X) P(X)$ et si on fait la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$ (ce qu'on peut faire car P est unitaire), on a $X^n - 1 = PQ + R$ avec $Q, R \in \mathbb{Z}[X]$ et $\deg R < \deg P$. Ainsi $R(X) = P(X)(\Phi_n(X) - Q(X))$ qui est de degré $\geq \deg P$ si $\Phi_n - Q \neq 0$. Donc $\Phi_n = Q \in \mathbb{Z}[X]$. □

(2) S'il existe $a \in \mathbb{Z}$ et p premier tq $p \mid \Phi_n(a)$ et $p \nmid \Phi_d(a)$ $\forall d \mid n$ strict, alors $p \equiv 1 \ [n]$

On a $a^n - 1 = \prod_{d \mid n} \Phi_d(a)$ donc par hyp. $p \mid a^n - 1$ donc l'ordre de $\bar{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ divise n. On va montrer qu'il vaut exactement n.
Soit $d \mid n$ diviseur strict. On a dans $\mathbb{F}_p$: $\bar{a}^d - 1 = \prod_{d' \mid d} \overline{\Phi_{d'}(a)}$.
Or si $d' \mid d$ alors $d' \mid n$ et $d' < n$ donc par hyp, on a $\overline{\Phi_{d'}(a)} \neq 0$
et comme $\mathbb{F}_p$ est un corps, le produit est $\neq 0$ donc $\bar{a}^d \neq \bar{1}$.
$\bar{a}$ est donc d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$.
Or le théorème de Lagrange assure que cet ordre divise $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$
donc on a bien $p \equiv 1 \ [n]$. □

Théorème (Dirichlet, 1837) : si $n \geq 1$ est fixé, il existe une infinité de nombres premiers de la forme $\lambda n + 1$ avec λ entier.

Dém: On raisonne par l'absurde en supposant qu'il en existe un nombre fini et on les numérote $p_1, \dots, p_q$.

Idée: on cherche un p tel que $p \equiv 1 [N]$ avec $N = n p_1 \cdots p_q$ de sorte que l'on ne puisse pas avoir $p = p_i$ et tel que $p \equiv 1 [n]$.

Soit $B = \prod_{\substack{d \mid N \\ d < N}} \Phi_d$. Cherchons $a \in \mathbb{Z}$ et p premier tels que $p \mid \Phi_N(a)$ et $p \nmid B(a)$.

Le pgcd est invariant par extension de corps

B est premier avec Φ_N dans $\mathbb{C}[X]$ donc dans $\mathbb{Q}[X]$. Ils sont scindés dans $\mathbb{C}[X]$ sans racine commune.

D'après le théorème de Bézout, il existe $U, V \in \mathbb{Q}[X]$ tq $1 = U\Phi_N + VB$.

Il existe ensuite $a \in \mathbb{Z}$ tq $U' = aU$ et $V' = aV$ soient dans $\mathbb{Z}[X]$. Par ex. le ppcm des dénom. des coeff.

Il y a une infinité de a qui conviennent

Comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$ on peut choisir un tel a tel que $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$ et on a alors $a = U'\Phi_N + V'B = U'(a)\Phi_N(a) + V'(a)B(a)$.

Soit p premier divisant $\Phi_N(a)$. Alors p divise $a^N - 1$ donc $\bar{a}^N = \bar{1}$ dans $\mathbb{F}_p$ donc $\bar{a}$ est inversible i.e a est premier avec p.

Si $p \mid B(a)$ alors a fortiori p divise a ce qui contredit ce qu'on vient de faire, donc $p \nmid B(a)$.

Ainsi a et p vérifient les hypothèses de (2) donc $p \equiv 1 [N]$.

Comme on a $p_i \equiv p_i \not\equiv 1 [N]$ on a bien $p \neq p_i$ et $p \equiv 1 [n]$ ce qui contredit l'hypothèse initiale. □

Détails

Division euclidienne dans $\mathbb{Z}[X]$:

Si $A, B \in \mathbb{Z}[X]$ avec B unitaire, alors il existe $Q, R \in \mathbb{Z}[X]$ tq $A = BQ + R$ avec $\deg R < \deg P$.

$B = X^m + \sum_{k<m} b_k X^k$ avec $b_k \in \mathbb{Z}$. On montre par récurrence que le résultat est vrai pour $\deg A < n$.

Clairement si $\deg A < m$, il suffit de poser $Q = 0$ et $R = A$.

Supposons le résultat vrai pour $\deg A < n$ avec $n \geq m$ et soit $A \in \mathbb{Z}[X]$ de degré $< n+1$.

On pose $A = \sum_{k \leq n} a_k X^k$ et soit $A_1 = A - a_n X^{n-m} B$.

Alors $A_1 \in \mathbb{Z}[X]$ et $\deg A < n$ donc par hypothèse de récurrence, il existe $Q_1, R_1 \in \mathbb{Z}[X]$ tq $A_1 = BQ_1 + R_1$ et $\deg R_1 < \deg B$. On pose $Q = Q_1 + a_n X^{n-m}$ de sorte que $A = A_1 + a_n X^{n-m} B = (Q_1 + a_n X^{n-m})B + R_1 = BQ + R_1$ avec $\deg R_1 < \deg B$ ce qui montre le résultat. □

$\bar{a}$ inversible dans $\mathbb{F}_p$ $\Leftrightarrow$ a premier avec p :

a et p sont premiers entre eux $\underset{\text{Bézout}}{\Leftrightarrow}$ $\exists u, v \in \mathbb{Z}$ tq $au + pv = 1$

$\Leftrightarrow \exists u \in \mathbb{Z}$ tq $\bar{a}\bar{u} = \bar{1}$ dans $\mathbb{F}_p$

$\Leftrightarrow \bar{a}$ est inversible dans $\mathbb{F}_p$.

Pourquoi le pgcd dans $\mathbb{C}[X]$ est le même dans $\mathbb{Q}[X]$:

L'algo. d'Euclide s'écrit de la même manière dans $\mathbb{C}[X]$ et dans $\mathbb{Q}[X]$.

Pourquoi existe-il $a \in \mathbb{Z}$ tq $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$? :

Il existe une infinité de $a \in \mathbb{Z}$ tq $aU, aV \in \mathbb{Z}[X]$ (tous les multiples du ppcm des dénominateurs des coefficients de U et V) et Φ_N (et $\Phi_N \pm 1$) a un nombre fini de racines.