Théorème de Dirichlet faible

CloudSea

Cadre

On montre que pour tout n, il existe une infinité de nombres premiers congrus à 1 modulo n

Recasages :
- [[102 Groupe des complexes de module 1]]
- [[120 Anneau Z sur nZ]]
- [[121 Nombres premiers]]

Référence : Oraux x ens algèbre 1

Déroulé du développement

Montrer que les polynômes cyclotomiques sont dans $\mathbb{Z}[X]$

Pour tout diviseur d de n, $\mathbb{U}_d$ est le seul sous groupe de $\mathbb{U}_n$ d'ordre d. Donc les éléments d'ordre d sont exactement les générateurs de $\mathbb{U}_d$
Donc $\mathbb{U}_n = \bigsqcup_{d|n} \mathbb{U}_d^\times$, donc

$$X^n - 1 = \prod_{z \in \mathbb{U}_n} (X - z) = \prod_{d|n} \prod_{\zeta \in \mathbb{U}_d^\times} (X - \zeta) = \prod_{d|n} \phi_d$$

Montrons que $\phi_n \in \mathbb{Z}[X]$
$n = 1$
ok $\phi_1 = X - 1$

Et si $\forall k \leq n, \phi_k \in \mathbb{Z}[X]$, on a $X^n - 1 = \phi_n P$ où $P = \prod_{d|n, d<n} \phi_d \in \mathbb{Z}[X]$ par hypothèse de récurrence
Donc ϕ_n est le quotient de la division euclidienne de $X^n - 1$ par P dans $\mathbb{C}[X]$. Donc

comme $X^n - 1$ et P sont dans $\mathbb{Z}[X]$, on a $\phi_n \in \mathbb{Z}[X]$

Soit a un entier, montrer que si p divise $\phi_n(a)$ mais aucun des $\phi_d(a)$ avec d diviseur strict de n, alors p est congru à 1 modulo n

$\phi_n | X^n - 1$ donc $\phi_n(a)$ divise $a^n - 1$. Donc dans $\mathbb{F}_p$ on a $\overline{a}^n = 1$, donc l'ordre de $\overline{a}$ dans $\mathbb{F}_p^*$ divise n, on va montrer que c'est exactement n

Soit d un diviseur strict de n
Dans $\mathbb{F}_p$ on a

$$\overline{a}^d - 1 = \prod_{\delta | d} \overline{\phi_\delta(a)}$$

Par hypothèse, les $\overline{\phi_\delta(a)}$ sont tous non nuls, donc comme $\mathbb{F}_p$ est intègre, on a $\overline{a}^d \neq 1$
Donc $\overline{a}$ est bien d'ordre n

Donc par théorème de Lagrange, n divise $p - 1$. Donc p est bien congru à 1 modulo n

En déduire Dirichlet Faible

On suppose par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers congrus à 1 modulo n à savoir $p_1, \cdots, p_k$
Soit $N = np_1 \cdots p_k$, on va construire a entier et p premier tels que p divise $\phi_N(a)$ mais aucun des $\phi_d(a)$ pour d diviseur strict de N

Soit $P = \prod_{d|N, d<N} \phi_d$
P est premier avec ϕ_N dans $\mathbb{C}[X]$ (en effet il n'y a pas de racines en commun), donc dans $\mathbb{Q}[X]$
Donc Bézout donne $U, V \in \mathbb{Q}[X]$ tels que $\phi_N U + PV = 1$
Soit a entier tel que $aU, aV \in \mathbb{Z}[X]$ (par exemple le ppcm de tous les coefficients). Comme $\phi_N \neq 0$ et $\phi_N \neq \pm 1$, on peut même choisir a tel que $\phi_N(a) \neq 0, -1$ ou 1, on a donc dans $\mathbb{Z}$

En notant $U_1 = aU$ et $V_1 = aV$, on a donc dans $\mathbb{Z}$ l'égalité

$$a = \phi_N(a) U_1(a) + P(a) V_1(a) \quad (*)$$

Par hypothèse, $\phi_N(a)$ admet un diviseur premier p
Donc dans $\mathbb{F}_p$, on a $\overline{a}^N - 1 = 0$, donc $\overline{a}^N \neq 0$, donc $\overline{a} \neq 0$
Or dans $\mathbb{F}_p$, $(*)$ devient $\overline{a} = \overline{P(a)}\ \overline{V_1(a)}$, donc $\overline{P(a)} \neq 0$, donc p ne divise aucun $\phi_d(a)$

pour d diviseur strict de N

Donc par le point précédent, on a que p est congru à 1 modulo N. Donc p est congru à 1 modulo n, et modulo tous les p_i, donc il est différent de tous les p_i, absurde

Version révisions

On se propose de montrer que pour tout n, il existe une infinité de nombres premiers congrus à 1 modulo n

1. Montrer que $X^n - 1 = \prod_{d|n} \phi_d$
2. En déduire que les polynômes cyclotomiques sont à coefficients dans $\mathbb{Z}$
3. Soit a un entier tel que p divise $\phi_n(a)$ mais aucun des $\phi_d(a)$ avec d diviseur strict de n
   3.1 Montrer que dans $\mathbb{F}_p$, on a $\overline{a}^n = 1$, et que $\overline{a}^d = 1$ pour aucun d diviseur strict de n
   3.2 En déduire que p est congru à 1 modulo n

On suppose par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers congrus à 1 modulo n à savoir $p_1, \cdots, p_k$
Soit $N = np_1 \cdots p_k$ et $P = \prod_{d|N, d<N} \phi_d$

4. Montrer qu'il existe $U, V \in \mathbb{Q}[X]$ tels que $\phi_N U + PV = 1$
5. Montrer qu'il existe $a \in \mathbb{Z}$ tel que $aU, aV \in \mathbb{Z}[X]$ et $\phi_N(a) \neq 0, -1$ ou 1
6. Soit p un facteur premier de $\phi_N(a)$, en multipliant l'égalité de 4. par a et en évaluant en a, montrer que $P(a)$ n'est pas multiple de p
7. En déduire une contradiction