VM
9/04/15

Progression arithmétique de Dirichlet 102, 120, 121

Réf: FGN

Théorème : Pour tout $n \geq 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.

dém : Soit $n \in \mathbb{N}$.

Supposons qu'il existe (qu'un nombre fini) $p_1, \dots, p_q$ de nombres premiers vérifiant $p_i \equiv 1 [n]$.

Lemme : Soit $N \geq 1$. Soit $a \in \mathbb{Z}$. Si un nombre premier p divise $\Phi_N(a)$ mais ne divise aucun des $\Phi_d(a)$ pour d divisant N, $d \neq N$, alors $p \equiv 1 [N]$.

(un peu plus fort)

dém : Soit p un tel nombre.

Comme $X^N - 1 = \prod_{d \mid N} \Phi_d(X)$, et que $\Phi_d \in \mathbb{Z}[X]$

$\forall d$, on a $a^N - 1 = \prod_{d \mid N} \Phi_d(a)$. Comme p divise $\Phi_N(a)$, p divise aussi $a^N - 1$.

Dans $\mathbb{Z}/p\mathbb{Z}$, on a ainsi $\bar{a}^N = 1$. Soit d l'ordre de $\bar{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$: d divise alors N.

On a $\bar{a}^d - 1 = \prod_{d' \mid d} \overline{\Phi_{d'}(a)}$

Dès que $d' \mid d$, $d' \neq N$, on a aussi $d' \mid N$, $d' \neq N$, donc par hypothèse sur p, $\overline{\Phi_{d'}(a)} \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$.

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, en particulier intègre, N divise d, donc $N = d$ est l'ordre de $\bar{a}$ dans $\mathbb{Z}/p\mathbb{Z}$.

Par théorème de Lagrange, N divise $p - 1$.

Ainsi $p \equiv 1 [N]$.

□

On pose $N = n p_1 \cdots p_q$.

Il suffit de trouver p premier tel que $p \equiv 1 [N]$.

En effet, cela entraînerait que $p \equiv 1 [n]$, et $p \neq p_i$ $\forall i \leq q$, ce qui contredirait l'hypothèse et permettrait de conclure quant au nombre infini de premiers vérifiant $p \equiv 1 [n]$.

lemme [->]

Il suffit de trouver p premier et $a \in \mathbb{Z}$ tel que p divise $\Phi_N(a)$ mais p ne divise pas $\Phi_d(a)$ $\forall d | N$, $d \neq N$ (d'après le lemme).

Soit $R = \prod_{\substack{d|N \\ d \neq N}} \Phi_d$.

R et Φ_N n'ont pas de racine commune dans $\mathbb{C}$, donc sont premiers entre eux dans $\mathbb{C}[X]$, donc le sont aussi dans $\mathbb{Q}[X]$. Il existe $U, V \in \mathbb{Q}[X]$ tels que $UR + V\Phi_N = 1$. Il existe une infinité de $a \in \mathbb{Z}$ tels que $\tilde{U} = aU$, $\tilde{V} = aV \in \mathbb{Z}[X]$

et comme Φ_N n'est pas constant, on peut choisir $a \in \mathbb{Z}$ tel que $\Phi_N(a) \neq 0, 1$ ou -1. Soit p premier divisant $\Phi_N(a)$.

p existe car $\Phi_N(a) \neq 0, 1$ ou -1.

Ainsi, p divise aussi $a^N - 1$ donc $\bar{a}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$, donc p ne divise pas a.

On $\tilde{U}(a) R(a) + \tilde{V}(a) \Phi_N(a) = a$.

p divise $\Phi_N(a)$, p ne divise pas a $\Rightarrow$ p ne divise pas $\tilde{U}(a) R(a)$

donc p ne divise pas $R(a)$: en particulier, p ne divise aucun des $\Phi_d(a)$ $(d | N)$, $d \neq N$.

Donc p est a répondant au problème, ce qui conclut.