Développement : Version faible du théorème de progression arithmétique de Dirichlet.

Références : CVA, Caldero p 207.

Théorème : Soit un entier ≥ 2. Il existe une infinité de nombres premiers congrus à 1 modulo n.

Preuve :

Lemme : Soit p premier tel que $p \nmid n$. S'il existe $\bar{x} \in \mathbb{F}_p$ tel que $\overline{\Phi_n}(\bar{x}) = \bar{0} \Rightarrow n \mid p-1$.

Preuve :

Soit $\bar{x} \in \mathbb{F}_p$ tel que $\overline{\Phi_n}(\bar{x}) = \bar{0}$. On sait que $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ dans $\mathbb{Z}[X]$. (1)

Comme $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $a \mapsto \bar{a}$ est un morphisme d'anneaux qui se prolonge en un morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$, on peut regarder l'équation (1) dans $\mathbb{F}_p[X]$: $X^n - \bar{1} = \prod_{d \mid n} \overline{\Phi_d}(X)$

Comme $\overline{\Phi_n}(\bar{x}) = \bar{0}$, $\bar{x}^n - \bar{1} = \bar{0}$ ie. $\bar{x}^n = \bar{1}$. En particulier, $\bar{x}$ est non nul, donc $\bar{x} \in \mathbb{F}_p^*$.

Montrons que $\bar{x}$ est d'ordre n. Supposons qu'il existe $d < n$, $d \mid n$ tel que $\bar{x}^d = \bar{1}$, donc $\bar{x}^d - \bar{1} = \bar{0}$.

Dans ce cas $\bar{x}$ est racine de $X^d - \bar{1} = \prod_{d' \mid d} \Phi_{d'}$, Or $d' \mid d \Rightarrow d' \mid n$ donc $\bar{x}$ est racine double de $X^n - \bar{1}$, $\bar{x}$ est donc racine de la dérivée de $X^n - 1$: nX^{n-1} Or $\bar{x}$ est non nul et $n \nmid p$ donc $\bar{x}$ ne peut pas annuler nX^{n-1}. On a une contradiction, ce qui implique que $\bar{x}$ est d'ordre n.

Par le théorème de Lagrange, comme $\bar{x} \in \mathbb{F}_p^*$ qui est d'ordre $p-1$, $n \mid p-1$. □

On pose $P_{n,1} := \{ p \text{ premier} \mid p \equiv 1 [n] \}$.

Supposons que $P_{n,1}$ est fini (ou vide)

Posons $a := \begin{cases} n \prod_{p \in \mathcal{P}_{n,1}} p & \text{si } \mathcal{P}_{n,1} \text{ non vide} \\ n & \text{sinon} \end{cases}$

On a $|\phi_n(a)| \geq 2$. En effet :

- si $n=2$. $\phi_n(X) = \phi_2(X) = X+1$ et $a \geq 2$ donc $|\phi_2(a)| \geq |2+1| \geq 2$.
- si $n \geq 3$. $a \geq n \geq 3$. Soit ω une racine primitive n-ième de l'unité ($\omega \in \mu_n$). $\Rightarrow |\omega| = 1$.

$$|\phi_n(a)| = \prod_{k \wedge n = 1} |a - \omega^k| \geq \prod_{k \wedge n = 1} (|a| - |\omega^k|) \geq \prod_{k \wedge n = 1} (3-1) \geq 2 \quad \text{(inégalité triangulaire)}$$

Comme $|\phi_n(a)| \geq 2$, il existe forcément q premier qui divise $\phi_n(a)$ car $\phi_n(a)$ n'est pas inversible dans $\mathbb{Z}$.

donc $q \mid a^n - 1$ donc $q \wedge a = 1$ (sinon $q \mid 1$ ce qui est impossible).

donc $q \wedge n = 1$ car $n \mid a$.

De plus, comme $q \mid \phi_n(a)$, $\overline{\phi_n}(\bar{a}) = \bar{0}$ dans $\mathbb{F}_q$. Par le lemme, on a donc que $n \mid q-1$. Alors $q \in \mathcal{P}_{n,1}$.

Or, si $q \in \mathcal{P}_{n,1}$, alors $q \mid a$, ce qui est absurde.

Donc $\mathcal{P}_{n,1}$ est infini. □