Infinité des premiers congrus à a modulo n

Cas particuliers du théorème de progression arithmétique

Premiers congrus à 3 modulo 4

Notons $\mathbb{P}_{3[4]} := \{p \in \mathbb{P} : p \equiv 3 \bmod 4\}$ l'ensemble des premiers congrus à 3 modulo 4.

Par l'absurde, supposons que $P_{3[4]}$ fini et notons $P := \prod \mathbb{P}_{3[4]}$ leur produit. Alors, on a

$$P^2 = \left(\prod_{p \in \mathbb{P}_{3[4]}} p\right)^2 = \prod_{p \in \mathbb{P}_{3[4]}} p^2 \equiv \prod_{p \in \mathbb{P}_{3[4]}} 1 \equiv 1 \mod 4$$

car $\forall p \in \mathbb{P}_{3[4]},\ p \equiv 3 \bmod 4$ donc $p^2 \equiv 3^2 = 9 \equiv 1 \bmod 4$. Ainsi,

$$P^2 + 2 \equiv 1 + 2 \equiv 3 \mod 4$$

Soit $q \in \mathbb{P} \cap \mathrm{Div}(P^2+2)$ diviseur premier de P^2+2. Montrons que $q \notin \mathbb{P}_{3[4]}$.

En effet, si $q \in \mathbb{P}_{3[4]}$, alors $q \operatorname{div} P^2$, or $q \operatorname{div} P^2 + 2$, donc $q \operatorname{div} 2$, donc $q = 2$.

Impossible car $2 \notin \mathbb{P}_{3[4]}$ car $2 \not\equiv 3 \bmod 4$. Donc $q \equiv \{0, 1, 2\} \bmod 4$

Ainsi, par décomposition $P^2 + 2 = \prod_{q \in \mathbb{P} \cap \mathrm{Div}(P^2+2)} q^{v_q(P^2+2)}$ en facteurs premiers, $\exists v_0, v_2, v_2 \in \mathbb{N}$:

$$P^2 + 2 \equiv 0^{v_0} \cdot 1^{v_1} \cdot 2^{v_2} \equiv \{0, 1, 2\} \not\equiv 3 \mod 4$$

Contradiction.