Propriété .1 *Il existe une infinité de nombres premiers congrus à 3 modulo 4.*

Démonstration : Supposons le contraire. Soient $p_1, \ldots, p_n$ les nombres premiers congrus à 3 modulo 4. Considérons $N = 4p_1 \ldots p_n + 3$. On a $N \equiv 3[4]$. Un produit d'entiers $\equiv 1[4]$ l'est encore, donc N a un diviseur premier qui n'est pas $\equiv 1[4]$. N possède donc un diviseur premier $\equiv 3[4]$. Mais les p_i ne divisent pas N, contradiction.

Propriété .2 *Il existe une infinité de nombres premiers congrus à 1 modulo 4.*

Démonstration : Pour tout entier $n \geq 2$, considérons $N = n!^2 + 1$. Soit p un nombre premier vérifiant $p \leq n$. Alors p divise $n!$, donc $N \equiv 1[p]$. Donc p ne divise pas N.

Prenons maintenant un diviseur premier p de N. Ce nombre est donc supérieur à n (et impair). On a $n!^2 + 1 \equiv 0[p]$, donc -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$. On en déduit que $\pm 1 = (-1)^{\frac{p-1}{2}} \equiv 1[p]$. Comme p est impair, on a $-1 \not\equiv 1[p]$ donc $(-1)^{\frac{p-1}{2}} = 1$. Ainsi, $\frac{p-1}{2}$ est pair et $p \equiv 1[4]$.

Résumons nous : pour tout $n \geq 2$, il existe p premier congru à 1 modulo 4 tel que $p > n$. L'ensemble de ces nombres premiers est non majoré, donc infini.