121. Nombres premiers : questions

1. Soit $n \in \mathbf{N}^*$. Soit p un facteur premier de $(n!)^2 + 1$.

a) Comparer p et n.

b) Quelle est la congruence de p modulo 4 ?

c) Soit $\varepsilon \in \pm 1$. Montrer qu'il existe une infinité de nombres premiers de la forme $4k + \varepsilon$ avec $k \in \mathbf{N}^*$.

2. Soit A l'anneau $\mathbf{Z}[i]$ des entiers de Gauss.

a) Montrer qu'un nombre premier p n'est pas irréductible dans A si et seulement s'il est de la forme $a^2 + b^2$ avec $a, b \in \mathbf{N}$.

b) Déterminer tous les irréductibles de A (on discutera suivant la norme $N(z) := z\bar{z}$ d'un élément $z \in A$).

c) Soit $z = a + ib$ avec $a, b \in \mathbf{Z}$. On suppose que $N(z) = a^2 + b^2$ est un nomre premier. Les éléments z et $\bar{z}$ sont-ils associés dans l'anneau A ?

3. Soit p un nombre premier impair.

a) Quelle est la congruence de $p^2 - 1$ modulo 8 ?

b) Soit $Q = X^4 + 1$, vu comme un polynôme de $\mathbf{F}_p[X]$. Montrer que Q a une racine dans le corps $\mathbf{F}_{p^2}$.

c) En déduire que Q est réductible dans $\mathbf{F}_p[X]$. Est-ce encore vrai pour $p = 2$?

d) Plus généralement, montrer que si p est un nombre premier ne divisant pas un entier n, le polynôme cyclotomique Φ_n est réductible sur $\mathbf{F}_p$ si et seulement si l'ordre de p dans le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ est $< \varphi(n)$. C'est toujours le cas si $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique (et en fait réciproquement via le théorème de la progression arithmétique de Dirichlet).

4. Déterminer les entiers n pour lesquels le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique.