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 $p = 2$?

Dans toute la suite, on note p un nombre premier ne divisant pas n, $\Phi_n \in \mathbf{Z}[X]$ le n-ième polynôme cyclotomique et $\Phi_{n,p} \in \mathbf{F}_p[X]$ la réduction de Φ_n modulo p. On note E l'ensemble des racines primitives n-ièmes de l'unité dans un corps de décomposition du polynôme $X^n - 1$ sur $\mathbf{F}_p$.

d) Montrer que

$$\Phi_{n,p} = \prod_{\zeta \in E} (X - \zeta).$$

e) En s'inspirant de c), montrer que $\Phi_{n,p}$ est réductible sur $\mathbf{F}_p$ si et seulement si l'ordre de p dans le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ est $< \varphi(n)$. Quand $(\mathbf{Z}/n\mathbf{Z})^*$ n'est pas cyclique (cf. exercice 4.), cette condition est automatique.

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

5. Soit $n \in \mathbf{N}^*$.

a) Montrer que si $2^n - 1$ est premier, alors n est premier.

b) Montrer que si $2^n + 1$ est premier, alors n est une puissance de 2.

6. On note p_n le n-ième nombre premier. Montrer que la série $\sum_{n\geq 1} 1/p_n$ est divergente (on pourra comparer avec un produit infini).

7. Parmi les assertions suivantes, dire lesquelles sont vraies et lesquelles sont fausses (en justifiant).

a) Si H est un p-Sylow distingué dans un groupe fini G (où p est un nombre premier), alors H est caractéristique dans G.

b) Si G est un groupe fini et $p_1, ..., p_r$ sont les diviseurs premiers de G, alors G est isomorphe à un produit direct $\prod_{i=1}^{r} G_i$, où G_i est un p_i-Sylow de G.

c) Soit $(A, +)$ un groupe abélien. On suppose que pour tout $x \in A$, il existe $n \in \mathbf{N}^*$ tel que $nx = 0$. Alors G est isomorphe à $\bigoplus_{p\in\mathcal{P}} A_p$, où $\mathcal{P}$ désigne l'ensemble des nombres premiers et A_p est un groupe abélien dont tout élément est d'ordre une puissance de p.