

Algèbre générale.

Cyclicité du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$.

Soit p un nombre premier.

1. Soit q un nombre premier qui divise $p - 1$. Etablir l'existence d'un élément de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ d'ordre q .
2. Soit q un nombre premier et $\alpha \in \mathbb{N}^*$ tels que $q^\alpha | p - 1$. Montrer l'existence d'un élément de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ d'ordre q^α .
3. En déduire que $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est cyclique.

Version faible du théorème de la progression arithmétique de Dirichlet.

On note $\Phi_1 = X - 1$ et pour $n \geq 2$, $\Phi_n = \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} (X - e^{2ik\pi/n})$ le n ième polynôme

cyclotomique.

1. Montrer que Φ_n est à coefficients entiers.
2. Que peut-on dire d'un nombre premier p divisant $\Phi_n(a)$, où $a \in \mathbb{Z}$, mais aucun des $\Phi_d(a)$ où d décrit l'ensemble des diviseurs de n ?
3. En déduire que pour tout $n \geq 1$ fixé, il existe une infinité de nombres premiers de la forme $\lambda n + 1$, avec λ entier.

Anneau des entiers de Gauss.

Soit $\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss.

1. Montrer que $\mathbb{Z}[i]$ est euclidien, muni du stathme $\varphi(a + ib) = a^2 + b^2$.
2. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
3. Calculer le pgcd de $14 + 3i$ et de $1 + 37i$.

Polynômes irréductibles de $\mathbb{Q}[X]$ de degré arbitrairement grand.

1. On définit le contenu $c(P)$ de $P \in \mathbb{Z}[X]$ comme étant le pgcd de ses coefficients.
 - (a) Soient $P_1, P_2 \in \mathbb{Z}[X]$. Montrer que $c(P_1 P_2) = c(P_1) c(P_2)$.
 - (b) Soient $Q_1, Q_2 \in \mathbb{Q}[X]$ tels que $Q_1 Q_2 \in \mathbb{Z}[X]$. Montrer qu'il existe $P_1, P_2 \in \mathbb{Z}[X]$, associés à Q_1 et Q_2 , tels que $Q_1 Q_2 = P_1 P_2$.
2. Soit $P(X) = p_0 + \dots + p_n X^n \in \mathbb{Z}[X]$ de degré $n \geq 1$. On suppose qu'il existe p un nombre premier divisant tous les p_i pour $1 \leq i \leq n - 1$ mais ne divisant pas n tel que p^2 ne divise pas p_0 . Montrer que P est irréductible dans $\mathbb{Q}[X]$.
3. On pose $P_p(X) = X^{p-1} + \dots + X + 1$ où p est un nombre premier. Montrer que P_p est irréductible dans $\mathbb{Q}[X]$ et conclure qu'il existe des polynômes irréductibles de degré arbitrairement grand dans $\mathbb{Q}[X]$.

Carrés.

On désigne par p un nombre premier ≥ 3 .

1. Etablir, si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, qu'il existe des éléments x tels que $x^4 = 1$.
En déduire que $p \equiv 1[4]$.
2. On suppose $p \equiv -1[4]$. Montrer que -1 n'a pas de racine carrée dans $\mathbb{Z}/p\mathbb{Z}$, puis montrer que $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ peut être muni d'une structure de corps à p^2 éléments contenant un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et des racines carrées de -1 .