Quelques cas particuliers du théorème de Dirichlet

Introduction

Dans ce problème, on s'intéresse au résultat suivant.

Théorème de la progression arithmétique (Dirichlet, 1838) : Si $(m,n) \in \mathbb{N} \times \mathbb{N}^*$ est un couple d'entiers tel que $m \wedge n = 1$, alors il existe une infinité de nombres premiers $p \in \mathbb{N}$ vérifiant $p \equiv m\,[n]$.

La démonstration complète de ce résultat dépasse largement les limites du programme. L'objectif de ce problème est de démontrer certains cas particuliers de ce théorème. Dans la suite du problème, on désignera par $\mathscr{P}$ l'ensemble des nombres premiers. Si $(m,n) \in \mathbb{N} \times \mathbb{N}^*$ est un couple d'entiers, on note

$$\mathscr{P}_n(m) = \{p \in \mathscr{P} \mid p \equiv m\,[n]\}.$$

Avec ces notations, le théorème de Dirichlet est équivalent à l'infinité de l'ensemble $\mathscr{P}_n(m)$ pour tout couple $(m,n) \in \mathbb{N} \times \mathbb{N}^*$ avec $m \wedge n = 1$.

I. Généralités

Dans cette partie, on traite les cas élémentaires du théorème de Dirichlet. On fixe un entier $n \in \mathbb{N}^*$.

1. Justifier que pour montrer l'infinité de l'ensemble $\mathscr{P}_n(m)$ pour tout $m \in \mathbb{N}$ avec $m \wedge n = 1$, il suffit de traiter le cas où $m \in [\![0, n-1]\!]$ avec $m \wedge n = 1$.
2. Justifier que $\mathscr{P}_1(0)$ est infini.
3. Justifier que $\mathscr{P}_2(1)$ est infini.

II. Les cas $(m,n) \in \{(2,3),(3,4),(5,6)\}$

Dans cette partie, on considère le polynôme $P(X) = 3X - 1 \in \mathbb{Z}[X]$.

1. Montrer que si $p \in \mathscr{P}$ vérifie $p \neq 3$, alors $p \equiv 1\,[3]$ ou $p \equiv 2\,[3]$.
2. On fixe un entier $a \in \mathbb{N}^*$.
   a) Montrer que $P(a)$ est un entier vérifiant $P(a) \geqslant 2$.
   b) Montrer qu'il existe un diviseur premier $p \in \mathscr{P}$ de $P(a)$ tel que $p \equiv 2\,[3]$.
3. On raisonne pas l'absurde en supposant que l'ensemble non vide $\mathscr{P}_3(2)$ admet un plus grand élément que l'on note $q \in \mathbb{N}$.
   a) Montrer que $P(q!)$ et $q!$ admettent un diviseur premier commun.
   b) En déduire que $\mathscr{P}_3(2)$ est infini.
4. En adaptant la démonstration précédente, montrer que $\mathscr{P}_4(3)$ et $\mathscr{P}_6(5)$ sont infinis.

III. Le cas $(m,n)=(1,4)$

Dans cette partie, nous allons démontrer que l'ensemble $\mathscr{P}_4(1)$ est infini. On commence par établir un résultat intermédiaire que nous utiliserons ensuite.

1. Soit $p \in \mathscr{P}$ avec $p>2$. On suppose qu'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv -1\,[p]$.

a) Montrer que $(-1)^{\frac{p-1}{2}} \equiv 1\,[p]$.

b) En déduire que $p \equiv 1\,[4]$.

2. On introduit le polynôme $Q(X)=X^2+1$.

a) Montrer que si $a \in \mathbb{N}^*$ et si $p \in \mathscr{P}$ est un diviseur de $Q(a)$, alors $p=2$ ou $p \equiv 1\,[4]$.

b) En utilisant un raisonnement analogue à **II.3**, en déduire que $\mathscr{P}_4(1)$ est infini.

IV. Cas où n est premier et $m=1$

Dans cette partie, on suppose que n est un nombre premier. Nous allons montrer que $\mathscr{P}_n(1)$ est infini. On considère le polynôme

$$\Phi_n(X)=\sum_{k=0}^{n-1} X^k \in \mathbb{Z}[X].$$

1. Montrer que $(X-1)\cdot\Phi_n(X)=X^n-1$.

2. Soit $a \in \mathbb{N}^*$. Soit $p \in \mathscr{P}$ un facteur premier de l'entier $\Phi_n(a) \geqslant 2$.

a) Montrer que $a^n \equiv 1\,[p]$.

Dans la suite, on note $m \in \mathbb{N}^*$ le plus petit entier naturel non nul tel que $a^m \equiv 1\,[p]$.

b) Soit $k \in \mathbb{N}$ tel que $a^k \equiv 1\,[p]$. En utilisant la division euclidienne de k par m, montrer que l'entier m divise k.

c) En déduire que $m=1$ ou $m=n$.

d) Montrer que si $m=n$, alors $p \equiv 1\,[n]$.

e) Montrer que si $m=1$, alors p divise n.

3. On raisonne pas l'absurde en supposant que $\mathscr{P}_n(1)$ est fini. On note $q \in \mathbb{N}$ le plus grand élément de l'ensemble $\mathscr{P}_n(1) \cup \{0\}$. En considérant l'entier $\Phi_n(n\cdot q!)$, en déduire que $\mathscr{P}_n(1)$ est infini.

Fin