Dossier 2-16

Thème : Arithmétique

L'exercice

Pour tout entier naturel n supérieur ou égal à 2, on pose $A(n) = n^4 + 1$.
L'objet de l'exercice est l'étude des diviseurs premiers de $A(n)$.

1. (a) Étudier la parité de l'entier $A(n)$.
   (b) Montrer que, quel que soit l'entier n, $A(n)$ n'est pas un multiple de 3.
   (c) Montrer que tout entier d diviseur de $A(n)$ est premier avec n.
   (d) Montrer que, pour tout entier d diviseur de $A(n)$ on a : $n^8 \equiv 1 \mod d$.
2. Soit d un diviseur de $A(n)$. On note s le plus petit des entiers naturels non nuls k tels que $n^k \equiv 1 \mod d$.
   (a) En utilisant la division euclidienne de k par s, montrer que s divise k.
   (b) En déduire que s est un diviseur de 8.
   (c) Montrer que si de plus d est premier, alors s est un diviseur de $d - 1$. On pourra utiliser le petit théorème de Fermat.
3. On suppose l'entier n pair. Soit p un diviseur premier de $A(n)$. En examinant successivement les cas $s = 1$, $s = 2$ puis $s = 4$, conclure que p est congru à 1 modulo 8.
4. Appliquer ce qui précède à la recherche des diviseurs premiers de $A(12)$.
   Indication : la liste des nombres premiers congrus à 1 modulo 8 débute par 17, 41, 73, 89, 97, 113, 137, ...

Un extrait des programmes officiels

Programme de terminale scientifique (enseignement de spécialité). BO n°4 du 30 août 2001

Contenus	Modalités de mise en oeuvre	Commentaires
Arithmétique		
Divisibilité dans $\mathbb{Z}$. Division euclidienne. Algorithme d'Euclide pour le calcul du PGCD. Congruences dans $\mathbb{Z}$. Entiers premiers entre eux.	On fera la synthèse des connaissances acquises dans ce domaine au Collège et en classe de Seconde. On étudiera quelques algorithmes simples et on les mettra en oeuvre sur calculatrice ou tableur : recherche d'un PGCD, décomposition d'un entier en facteurs premiers, reconnaissance de la primalité d'un entier.	On montrera l'efficacité du langage des congruences. On utilisera les notations : $a \equiv b \quad (n)$ ou $a \equiv b$ (modulo n) et on établira les compatibilité avec l'addition et la multiplication. Toute introduction de $\mathbb{Z}/n\mathbb{Z}$ est exclue.
Nombres premiers. Existence et unicité de la décomposition en produit de facteurs premiers. PPCM.	On démontrera que l'ensemble des nombres premiers est infini.	L'unicité de la décomposition en facteurs premiers pourra être admise.
Théorème de Bezout. Théorème de Gauss.	Sur des exemples simples, obtention et utilisation de critères de divisibilité. Exemples simples d'équations diophantiennes. Applications élémentaires au codage et à la cryptographie. Application : petit théorème de Fermat	L'arithmétique est un domaine avec lequel l'informatique interagit fortement ; on veillera à équilibrer l'usage de divers moyens de calculs : à la main, à l'aide d'un tableur ou d'une calculatrice.

Le travail à exposer devant le jury

1- Analyser les méthodes et les savoirs mis en jeu dans l'exercice.

2- Expliciter la place de cet exercice dans le cadre des programmes.

3- Proposer plusieurs exercices sur le thème de l'arithmétique, pouvant donner lieu à un traitement différent selon le niveau considéré.