

Thème : Arithmétique**1. L'exercice proposé au candidat**

On se propose d'étudier l'existence des solutions $(x, y) \in \mathbb{N}^2$ de l'équation $(E) : x^2 - y^2 = n$, où n est un entier naturel non nul.

- 1) a) Montrer que (E) admet au moins une solution si et seulement s'il existe deux entiers naturels p et q de même parité tels que $n = pq$ (on pourra utiliser l'identité $x^2 - y^2 = (x + y)(x - y)$).
- b) En déduire que si n est un entier impair, (E) admet au moins une solution.
- 2) Montrer que n est un nombre premier impair si et seulement si le couple $\left(\frac{n+1}{2}, \frac{n-1}{2}\right)$ est l'unique solution de (E) .

2. Le travail demandé au candidat

En aucun cas, le candidat ne doit rédiger sur sa fiche sa solution de l'exercice. Celle-ci pourra néanmoins lui être demandée partiellement ou en totalité lors de l'entretien avec le Jury

Pendant sa préparation, le candidat traitera les questions suivantes :

- Q.1) Dégager les outils nécessaires à la résolution de cet exercice.
- Q.2) Quels aménagements apporteriez-vous à l'énoncé pour l'utiliser dans une classe de terminale scientifique ?

Sur ses fiches, le candidat rédigera et présentera :

- Sa réponse à la question Q.2).
- L'énoncé d'un ou plusieurs exercices se rapportant au thème « **Arithmétique** ».

3. Quelques références aux programmes

Classe de Terminale S, enseignement de spécialité

L'arithmétique est un champ des mathématiques très vivant dont les applications récentes sont nombreuses ; c'est un domaine au matériau élémentaire et accessible conduisant à des raisonnements intéressants et formateurs. C'est un lieu naturel de sensibilisation à l'algorithmique où la nécessité d'être précis impose rigueur et clarté du raisonnement.

Contenus	Modalités de mise en œuvre	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 œuvre 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 : $a > b (n)$ ou $a > b \pmod{n}$, et on établira les compatibilités 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 Bézout. 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.