Thème : Arithmétique

1. L'exercice proposé au candidat

Soit $\mathcal{E}$ l'ensemble des entiers compris entre 0 et 25 inclus. Dans cet exercice, chaque lettre de l'alphabet correspond à un élément de $\mathcal{E}$ à l'aide du tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On appelle codage l'application qui associe à chaque lettre de l'alphabet l'entier correspondant, et décodage l'application qui associe à chaque entier de $\mathcal{E}$ la lettre correspondante.

Soient a et b deux entiers. Soit $f : \mathcal{E} \longrightarrow \mathcal{E}$ définie par :

Pour tout x appartenant à $\mathcal{E}$, $f(x)$ est le reste de la division euclidienne de $ax + b$ par 26.

On appelle cryptage affine de clé (a, b) l'application qui associe à chaque lettre de l'alphabet une lettre de l'alphabet de la façon suivante : on code la lettre par un entier x de $\mathcal{E}$, on calcule $f(x)$ puis on décode $f(x)$.

Pour crypter un mot, on crypte chaque lettre.

1) On suppose dans cette question a premier avec 26. Soient x et x' deux éléments de $\mathcal{E}$, montrer que si $f(x) = f(x')$ alors $x = x'$.
2) On suppose dans cette question que $\text{PGCD}(a, 26) \neq 1$. Montrer qu'il existe alors au moins deux lettres différentes ayant le même cryptage.
3) On suppose maintenant que $(a, b) = (7, 2)$.
   a) Quel est le cryptage du mot **JOUR** ?
   b) Quel est le mot dont le cryptage est **QCDEY** ?

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 :

$Q.1$) Énoncer les théorèmes et les outils mis en jeu dans l'exercice.

$Q.2$) Rédiger un corrigé de la question 1) pouvant être proposé à une classe de lycée. Dégager, dans le contexte de l'exercice, l'intérêt de cette question.

$Q.3$) Utiliser la calculatrice pour proposer, dans une classe, une résolution de la question 3).

Sur ses fiches, le candidat rédigera et présentera :

(i) Sa réponse à la question $Q.2$).

(ii) Un ou plusieurs exercices se rapportant au thème « **Arithmétique** ».

3. Quelques références aux programmes

Programme de la classe de Troisième

Contenus	Compétences exigibles	Commentaires
Nombres entiers et rationnels		Cette partie d'arithmétique permet une première synthèse sur les nombres, intéressante tant du point de vue de l'histoire des mathématiques que pour la culture générale des élèves.
Diviseurs communs à deux entiers. Fractions irréductibles.	Déterminer si deux entiers donnés sont premiers entre eux. Simplifier une fraction donnée pour la rendre irréductible.	Depuis la classe de cinquième, les élèves ont pris l'habitude de simplifier les écritures fractionnaires : la factorisation du numérateur et du dénominateur se fait grâce aux critères de divisibilité et à la pratique du calcul mental. Reste à savoir si la fraction obtenue est irréductible ou non. On remarque que la somme et la différence de deux multiples d'un nombre entier sont eux-mêmes multiples de cet entier. On construit alors un algorithme, celui d'Euclide ou un autre, qui, donnant le PGCD de deux nombres entiers, permet de répondre à la question dans tous les cas. Les activités proposées ne nécessitent donc pas le recours aux nombres premiers. Les tableurs et les logiciels de calcul formel peuvent, sur ce sujet, être exploités avec profit. À côté des nombres rationnels, on rencontre au collège des nombres irrationnels comme π et $\sqrt{2}$. On pourra éventuellement démontrer l'irrationnalité de $\sqrt{2}$. Une telle étude peut également être mise à profit pour bien distinguer le calcul exact et le calcul approché.

Programme de Terminale S Spécialité Math

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 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, décompositions d'un entier en produit de facteurs premiers, reconnaissance de la primalité d'un entier.	On montrera l'efficacité du langage des congruences. On utilisera les notations : $a \equiv b \mod n$ ou $a \equiv b \pmod n$ 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 d'un entier 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 des différents moyens de calcul : à la main, à l'aide d'un tableur ou d'une calculatrice.