

DOSSIER N° 91

Question :

Présenter un choix d'exercices sur le thème suivant :

Exemples de présentation et d'utilisation de congruences au niveau de la Terminale L et de la Terminale S.

Pour au moins l'un de ces exercices, la résolution pourra faire appel à l'utilisation d'une calculatrice.

Consignes de l'épreuve :

Pendant votre préparation (deux heures), vous devez rédiger **sur les fiches mises à votre disposition**, un résumé des commentaires que vous développerez dans votre exposé et **les énoncés** de vos exercices. La qualité de ces fiches interviendra dans l'appréciation de votre épreuve. Le terme " exercice " est à prendre au sens large ; il peut s'agir d'applications directes du cours, d'exemples ou contre-exemples venant éclairer une méthode, de situations plus globales ou plus complexes utilisant éventuellement des notions prises dans d'autres disciplines.

Vous expliquerez dans votre exposé (25 minutes maximum) la façon dont vous avez compris le sujet et les objectifs recherchés dans les exercices présentés : acquisition de connaissances, de méthodes, de techniques, évaluation. Vous analyserez la pertinence des différents outils mis en jeu.

Cet exposé est suivi d'un entretien (20 minutes minimum).

Annexes :

Vous trouverez page suivante, en annexe, quelques références aux programmes ainsi qu'une documentation conseillée.

Ces indications ne sont ni exhaustives, ni impératives ; en particulier, les références au programme ne constituent pas le plan de l'exposé.

ANNEXE DU DOSSIER N° 94

Références aux programmes :

Extraits de programmes de Terminales :

| | | |
|---|---|--|
| <p>Terminale L : Divisibilité dans \mathbb{Z}. Congruences : définition et compatibilité avec l'addition et la multiplication.</p> | <p>On utilisera la notation : $a \equiv b \text{ modulo}(n)$. On expliquera quelques critères de divisibilité. On étudiera un problème de clé de contrôle, par exemple la clé du numéro INSEE ou la clé RIB qu'on pourra calculer avec un tableur.</p> | <p>On pourra à ce propos donner quelques aperçus sur la cryptographie.</p> |
| <p>Terminale S : Divisibilité dans \mathbb{Z}. (...) Congruences dans \mathbb{Z}.</p> | <p>On étudiera quelques algorithmes simples et on les mettra en oeuvre sur calculatrice ou tableur : recherche d'un PGCD, ...</p> | <p>On montrera l'efficacité du langage des congruences. On utilisera les notations : $a \equiv b (n)$ ou $a \equiv b \text{ modulo}(n)$, et on établira les compatibilités avec l'addition et la multiplication. Toute introduction de $\mathbb{Z}/n\mathbb{Z}$ est exclue.</p> |

Emploi des calculatrices programmables : l'emploi des calculatrices programmables (...) en Mathématiques a pour objectif, non seulement d'effectuer des calculs, mais aussi de contrôler des résultats, d'alimenter le travail de recherche et de favoriser une bonne approche de l'informatique.

Les élèves doivent savoir utiliser leur matériel personnel dans les situations liées au programme de la classe. Cet emploi combine les capacités suivantes qui constituent un savoir-faire de base et sont seules exigibles :

- Savoir effectuer les opérations arithmétiques sur les nombre et savoir comparer des nombres ;
- (...)
- Savoir recourir à une instruction séquentielle ou conditionnelle et, en classe, de Terminale, à une instruction itérative, comportant éventuellement un test d'arrêt (...).

Documentation conseillée :

Manuels de Terminales L et de Terminales S ; annales de baccalauréat. Accompagnement des programmes - Terminales L.

**Il ne s'agit en aucun cas d'une correction,
mais seulement de mon point de vue sur le sujet.**

L'arithmétique est une science difficile dont les conjectures ont résister longtemps, et pour certaines résistent encore aux mathématiciens. Alors que tout la prédispose à être une étude des nombres *pour l'honneur de l'esprit humain*, elle trouve sans cesse de nouvelles applications. Elle intervient dès que nous faisons une transaction électronique ou que nous écoutons un CD et est ainsi omniprésente dans notre quotidien.

Pour ce qui est de son enseignement, elle semble partager, avec la géométrie, le statut de *lieu privilégié de l'apprentissage du raisonnement*. Pourtant, si la géométrie possède de nombreux outils de démonstrations élémentaires, ceux de l'arithmétique nécessitent souvent des notions plus abstraites (congruence, groupe, ...).

Dans ce dossier, nous nous proposons d'étudier et d'utiliser un de ces outils : les congruences. A travers le choix de mes exercices, j'ai voulu insister sur l'efficacité du langage des congruences et sur l'étendue des domaines applicatifs dans lesquels elles interviennent.

La notion de congruence touche à un concept difficile et non formalisé dans le secondaire : celui de relation d'équivalence. On peut noter qu'une relation d'équivalence a déjà été rencontrée au collège lors de l'apprentissage des vecteurs. Mais le contexte algébrique rend les congruences plus difficiles d'accès. C'est peut-être ce qui explique qu'elles ne soient introduites qu'en Terminales L et S spécialité. Nous donnons ci-dessous un aperçu de l'introduction de la notion de congruence.

Etant donné un entier n , on dit que a est congru à b modulo n si a et b ont des restes égaux par la division euclidienne par n . On montre alors que :

$$a \equiv b \text{ modulo}(n) \iff b - a \text{ est divisible par } n$$

Les propriétés des multiples de n nous permettent alors de montrer que la congruence est compatible avec l'addition et la multiplication :

$$\left. \begin{array}{l} a \equiv b \text{ modulo}(n) \\ c \equiv d \text{ modulo}(n) \end{array} \right\} \Rightarrow (b-a)+(d-c) \text{ est divisible par } n \Rightarrow a+c \equiv b+d \text{ modulo}(n)$$

$$\left. \begin{array}{l} a \equiv b \text{ modulo}(n) \\ c \equiv d \text{ modulo}(n) \end{array} \right\} \Rightarrow (bd-bc)+(bc-ac) \text{ est divisible par } n \Rightarrow ac \equiv bd \text{ modulo}(n)$$

On dispose alors d'un outil remarquable (moralement celui de groupe cyclique) qui va nous permettre de justifier les règles de divisibilité par 3, 9, mais aussi la fameuse preuve par 9 qui n'est rien d'autre qu'une vérification, modulo 9, d'une l'opération effectuée sur des entiers.

EXERCICES :

Exercice 1 : Quelques règles de divisibilité.

Terracher 02, Terminale S, n° 72, 73, 74 page 357?

Soit a et b deux entiers.

- 1-) Montrer que $10a + b \equiv 3(a - 2b) \pmod{7}$.
- 2-) En déduire que $10a + b$ est divisible par 7 si et seulement si $a - 2b$ l'est.
- 3-) Sans calculatrice, tester la divisibilité par 7 de 638 et 588.

Exercice 2 : Code barre.

Bréal 02, Terminale S spé, page 84.

A tout article commercialisé, on attribue un code barre à 13 chiffres :

$$a_0 a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12} a_{13}$$

Les douze premiers chiffres identifient le produit et le lieu de fabrication. Le treizième est une clé, destinée à détecter d'éventuelles erreurs de lectures. Elle est fabriquée de telle sorte que :

$$a_0 + 3a_1 + a_2 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + a_{13} \equiv 0 \pmod{10}$$

- 1-) Démontrer qu'une erreur de lecture d'un chiffre est détectée par la clé.
- 2-) Montrer que si $2a - 2b \equiv 0 \pmod{10}$, l'interversion de deux chiffres voisins dans le code n'est pas détectée par la clé.

Exercice 3 : Numéro ISBN.

Terracher 02, Terminale S, n° 80 page 358.

L'ISBN est un nombre qui permet de coder tous les ouvrages édités. Il est constitué de 10 symboles pris dans les chiffres $0, \dots, 9$ et X qui désigne 10. Les neuf premiers chiffres identifient l'éditeur, le lieu d'édition, ... Le dernier est une clé qui est telle que :

$$\sum_{i=1}^{10} i a_{11-i} \equiv 0 \pmod{11}$$

1-) Montrer que si une erreur de lecture se produit sur un chiffre et un seul, cette erreur est détectée par la clé.

2-) Montrer que si deux chiffres consécutifs sont échangés, l'erreur est détectée par la clé.

Exercice 4 : Code Hamming.

Terracher 02, Terminale S, n° 81 page 358.

On désire fabriquer un code correcteur d'erreur, c'est à dire à même de détecter une erreur et de la corriger automatiquement. Mettons que le message à véhiculer est un nombre à 10 chiffres $a_1 \dots a_{10}$. On ajoute, à la fin de ces dix chiffres un clé constituée de deux symboles, a_{11} et a_{12} , pouvant être un chiffre ou X (désignant 10) et définis comme suit :

- a_{11} est le reste de $\sum_{i=1}^{10} a_i$ par la division par 11,
- a_{12} est le reste de $\sum_{i=1}^{10} i \times a_i$ par la division par 11.

1-) On suppose que, lors de la communication, une erreur de lecture s'est produite sur un et un seul des chiffres a_i . Quelles incidence cette erreur a-t-elle sur les clés ? Montrer que l'on peut alors la corriger.

2-) Corriger l'erreur dans 0380552117X5.

Exercice 5 : Rivest Adleman Shamir.

Bréal 02, Terminale S spé, page 82.

Soit p et q deux nombres premiers. On pose $n = pq$.

1-) Soit a un entier premier à p et r un entier congru à 1 modulo $p - 1$. A l'aide du théorème de Fermat, montrer que :

$$a^r \equiv a \pmod{p}$$

2-) Montrer que si r est un entier congru à 1 modulo $(p - 1)(q - 1)$, alors, pour tout entier x :

$$x^r \equiv x \pmod{n}$$