COURS PI

L'école sur-mesure

de la Maternelle au Bac, Établissement d'enseignement privé à distance, déclaré auprès du Rectorat de Paris

Terminale - Module 2 - Arithmétique

Mathématiques Expertes

v.5.1

- ***Guide de méthodologie***
  pour appréhender notre pédagogie
- ***Leçons détaillées***
  pour apprendre les notions en jeu
- ***Exemples et illustrations***
  pour comprendre par soi-même
- ***Prolongement numérique***
  pour être acteur et aller + loin
- ***Exercices d'application***
  pour s'entraîner encore et encore
- ***Corrigés des exercices***
  pour vérifier ses acquis

www.cours-pi.com

Paris & Montpellier

EN ROUTE VERS LE BACCALAURÉAT

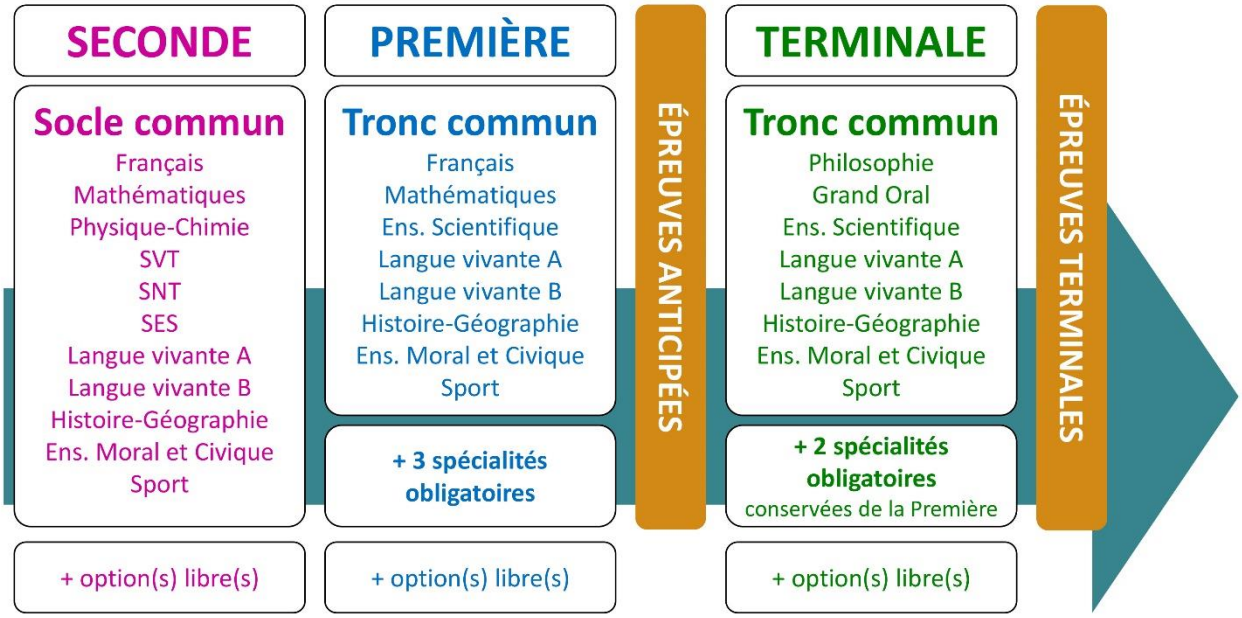
Comme vous le savez, **la réforme du Baccalauréat** est entrée en vigueur progressivement jusqu'à l'année 2021, date de délivrance des premiers diplômes de la nouvelle formule.

Dans le cadre de ce nouveau Baccalauréat, **notre Etablissement**, toujours attentif aux conséquences des réformes pour les élèves, s'est emparé de la question avec force **énergie** et **conviction** pendant plusieurs mois, animé par le souci constant de la réussite de nos lycéens dans leurs apprentissages d'une part, et par la **pérennité** de leur parcours d'autre part. Notre Etablissement a questionné la réforme, mobilisé l'ensemble de son atelier pédagogique, et déployé tout **son savoir-faire** afin de vous proposer un enseignement tourné continuellement vers l'**excellence**, ainsi qu'une scolarité tournée vers la **réussite**.

- Les **Cours Pi** s'engagent pour faire du parcours de chacun de ses élèves un **tremplin vers l'avenir**.
- Les **Cours Pi** s'engagent pour ne pas faire de ce nouveau Bac un diplôme au rabais.
- Les **Cours Pi** vous offrent **écoute** et **conseil** pour coconstruire une **scolarité sur-mesure**.

LE BAC DANS LES GRANDES LIGNES

Ce nouveau Lycée, c'est un enseignement à la carte organisé à partir d'un large tronc commun en classe de Seconde et évoluant vers un parcours des plus spécialisés année après année.



CE QUI A CHANGÉ

- Il n'y a plus de séries à proprement parler.
- Les élèves choisissent des spécialités : trois disciplines en classe de Première ; puis n'en conservent que deux en Terminale.
- Une nouvelle épreuve en fin de Terminale : le Grand Oral.
- Pour les lycéens en présentiel l'examen est un mix de contrôle continu et d'examen final laissant envisager un diplôme à plusieurs vitesses.
- Pour nos élèves, qui passeront les épreuves sur table, le Baccalauréat conserve sa valeur.

CE QUI N'A PAS CHANGÉ

- Le Bac reste un examen accessible aux candidats libres avec examen final.
- Le système actuel de mentions est maintenu.
- Les épreuves anticipées de français, écrit et oral, tout comme celle de spécialité abandonnée se dérouleront comme aujourd'hui en fin de Première.

A l'occasion de la réforme du Lycée, nos manuels ont été retravaillés dans notre atelier pédagogique pour un accompagnement optimal à la compréhension. Sur la base des programmes officiels, nous avons choisi de créer de nombreuses rubriques :

- **Suggestions de lecture** pour s'ouvrir à la découverte de livres de choix sur la matière ou le sujet
- **Réfléchissons ensemble** pour guider l'élève dans la réflexion
- **L'essentiel** pour souligner les points de cours à mémoriser au cours de l'année
- **À vous de jouer** pour mettre en pratique le raisonnement vu dans le cours et s'accaparer les ressorts de l'analyse, de la logique, de l'argumentation, et de la justification
- **Pour aller plus loin** pour visionner des sites ou des documentaires ludiques de qualité
- Et enfin ... la rubrique **Les Clés du Bac by Cours Pi** qui vise à vous donner, et ce dès la seconde, toutes les cartes pour réussir votre examen : notions essentielles, méthodologie pas à pas, exercices types et fiches étape de résolution !

MATHÉMATIQUES EXPERTES TERMINALE

Module 2 – Arithmétique

L'AUTEUR

Jonathan SELLAM

"Enseigner c'est d'abord éveiller, à la curiosité et donner l'envie d'en savoir plus".
Professeur de mathématiques qui acccompagne les élèves jusqu'à la préparation aux concours, professeur de physique dans une école d'ingénieur à Montpellier, il reste curieux de tout et surtout de l'histoire des sciences.

PRÉSENTATION

Ce **cours** est divisé en chapitres, chacun comprenant :

- Le **cours**, conforme aux programmes de l'Education Nationale
- Des **exercices d'application et d'entraînement**
- Les **corrigés** de ces exercices
- Des **devoirs** soumis à correction (et ***se trouvant hors manuel***). Votre professeur vous renverra le corrigé-type de chaque devoir après correction de ce dernier.

Pour une manipulation plus facile, les corrigés-types des exercices d'application et d'entraînement sont regroupés en fin de manuel.

CONSEILS A L'ÉLÈVE

Vous disposez d'un support de Cours complet : **prenez le temps** de bien le lire, de le comprendre mais surtout de l'**assimiler**. Vous disposez pour cela d'exemples donnés dans le cours et d'exercices types corrigés.
Vous pouvez rester un peu plus longtemps sur une unité mais travaillez régulièrement.

LES FOURNITURES

Vous devez posséder :

- une **calculatrice graphique pour l'enseignement scientifique au Lycée comportant un mode examen (requis pour l'épreuve du baccalauréat).**
- un **tableur** comme Excel de Microsoft (payant) ou Calc d'Open Office (gratuit et à télécharger sur http://fr.openoffice.org/). En effet, certains exercices seront faits de préférence en utilisant un de ces logiciels, mais vous pourrez également utiliser la calculatrice).

LES DEVOIRS

Les devoirs constituent le moyen d'évaluer l'acquisition de vos *savoirs* (« Ai-je assimilé les notions correspondantes ? ») et de vos *savoir-faire* (« Est-ce que je sais expliquer, justifier, conclure ? »).

Placés à des endroits clés des apprentissages, ils permettent la vérification de la bonne assimilation des enseignements.

Aux *Cours Pi*, vous serez accompagnés par un professeur selon chaque matière tout au long de votre année d'étude. Référez-vous à votre « Carnet de Route » pour l'identifier et découvrir son parcours.
Avant de vous lancer dans un devoir, assurez-vous d'avoir **bien compris les consignes**.
Si vous repérez des difficultés lors de sa réalisation, n'hésitez pas à le mettre de côté et à revenir sur les leçons posant problème. **Le devoir n'est pas un examen**, il a pour objectif de s'assurer que, même quelques jours ou semaines après son étude, une notion est toujours comprise.
Aux *Cours Pi*, chaque élève travaille à son rythme, parce que chaque élève est différent et que ce mode d'enseignement permet le « sur-mesure ».
Nous vous engageons à respecter le moment indiqué pour faire les devoirs. Vous les identifierez par le bandeau suivant :

Vous pouvez maintenant
faire et envoyer le devoir n°1

Il est **important de tenir compte des remarques, appréciations et conseils du professeur-correcteur**. Pour cela, il est **très important d'envoyer les devoirs au fur et à mesure** et non groupés. **C'est ainsi que vous progresserez !**

Donc, dès qu'un devoir est rédigé, envoyez-le aux *Cours Pi* par le biais que vous avez choisi :

1) Par **soumission en ligne** via votre espace personnel sur **PoulPi**, pour un envoi **gratuit**, **sécurisé** et plus **rapide**.
2) Par **voie postale** à *Cours Pi*, 9 rue Rebuffy, 34 000 Montpellier
   *Vous prendrez alors soin de joindre une **grande enveloppe libellée à vos nom et adresse**, et **affranchie au tarif en vigueur** pour qu'il vous soit retourné par votre professeur*

***N.B. :** quel que soit le mode d'envoi choisi, vous veillerez à **toujours joindre l'énoncé du devoir** ; plusieurs énoncés étant disponibles pour le même devoir.*
***N.B. :** si vous avez opté pour un envoi par voie postale et que vous avez à disposition un scanner, nous vous engageons à conserver une copie numérique du devoir envoyé. Les pertes de courrier par la Poste française sont très rares, mais sont toujours source de grand mécontentement pour l'élève voulant constater les fruits de son travail.*

SOUTIEN ET DISPONIBILITÉ

VOTRE RESPONSABLE PÉDAGOGIQUE

Professeur des écoles, professeur de français, professeur de maths, professeur de langues : notre Direction Pédagogique est constituée de spécialistes capables de dissiper toute incompréhension.

Au-delà de cet accompagnement ponctuel, notre Etablissement a positionné ses Responsables pédagogiques comme des « super profs » capables de co-construire avec vous une scolarité sur-mesure.
En somme, le Responsable pédagogique est votre premier point de contact identifié, à même de vous guider et de répondre à vos différents questionnements.

Votre Responsable pédagogique est la personne en charge du suivi de la scolarité des élèves.
Il est tout naturellement votre premier référent : une question, un doute, une incompréhension ? Votre Responsable pédagogique est là pour vous écouter et vous orienter. Autant que nécessaire et sans aucun surcoût.

QUAND PUIS-JE LE JOINDRE ?

Du lundi au vendredi : horaires disponibles sur votre carnet de route et sur PoulPi.

QUEL EST SON RÔLE ?

Orienter les parents et les élèves.
Proposer la mise en place d'un accompagnement individualisé de l'élève.
Faire évoluer les outils pédagogiques.
Encadrer et coordonner les différents professeurs.

VOS PROFESSEURS CORRECTEURS

Notre Etablissement a choisi de s'entourer de professeurs diplômés et expérimentés, parce qu'eux seuls ont une parfaite connaissance de ce qu'est un élève et parce qu'eux seuls maîtrisent les attendus de leur discipline. En lien direct avec votre Responsable pédagogique, ils prendront en compte les spécificités de l'élève dans leur correction. Volontairement bienveillants, leur correction sera néanmoins juste, pour mieux progresser.

QUAND PUIS-JE LE JOINDRE ?

Une question sur sa correction ?

- faites un mail ou téléphonez à votre correcteur et demandez-lui d'être recontacté en lui laissant un message avec votre nom, celui de votre enfant et votre numéro.
- autrement pour une réponse en temps réel, appelez votre Responsable pédagogique.

LE BUREAU DE LA SCOLARITÉ

Placé sous la direction d'Elena COZZANI, le Bureau de la Scolarité vous orientera et vous guidera dans vos démarches administratives. En connaissance parfaite du fonctionnement de l'Etablissement, ces référents administratifs sauront solutionner vos problématiques et, au besoin, vous rediriger vers le bon interlocuteur.

QUAND PUIS-JE LE JOINDRE ?

Du lundi au vendredi : horaires disponibles sur votre carnet de route et sur PoulPi.
04.67.34.03.00
scolarite@cours-pi.com

LE SOMMAIRE

Mathématiques Expertes – Module 2 – Arithmétique

COMPÉTENCES VISÉES

- Nombres premiers. Leur ensemble est infini.
- Existence et unicité de la décomposition d'un entier en produit de facteurs premiers.
- Petit théorème de Fermat.

SUGGESTIONS CULTURELLES

ESSAIS

- **Dictionnaire amoureux des mathématiques** *André Deledicq et Mickaël Launay*
- **La Science et l'Hypothèse** *Henri Poincaré*
- **Les mathématiques sont la poésie des sciences** *Cédric Villani*
- **Atlas des mathématiques** *Fritz Reinhardt et Heinrich Soeder*
- **Pourquoi le monde est-il mathématique ?** *John D. Barrow*
- **La formation de l'esprit scientifique** *Gaston Bachelard*
- **Les maths c'est magique !** *Johnny Ball*
- **17 Équations qui ont changé le monde** *Ian Stewart*
- **Alex au pays des chiffres** *Alex Bellos*
- **Le grand roman des maths :de la préhistoire à nos jours** *Mickael Launay*
- **Histoire universelle des chiffres : L'intelligence des hommes racontée par les nombres et le calcul** *Georges Ifrah*
- **Le démon des maths.** *Hans Magnus Enzensberger*
- **A propos de rien : une histoire du zéro** *Robert Kaplan*

BANDES-DESSINÉES

- **Logicomix** *Doxiádis / Papadátos / Papadimitríou*
- **Les maths en BD 1 et 2** *Larry Gonick*

PODCAST

- **L'oreille mathématique** *https://maison-des-maths.paris/podcasts/*


Le Cours

INTRODUCTION

Bienvenue dans le monde de l'arithmétique, le monde des nombres entiers, le monde de ce que l'on appelle, la théorie des nombres ! Vous allez vous initier à l'une des théories les plus anciennes, car déjà pendant l'antiquité le grand mathématicien Euclide, père de la géométrie, s'intéressait aux propriétés des nombres entiers. Cette théorie a traversé les siècles et les millénaires et quantité de mathématiciens parmi les plus illustres ont tenté de percer les mystères des nombres entiers. Ce qui est remarquable c'est l'écart vertigineux entre l'apparente simplicité de l'objet d'étude : les nombres entiers que vous connaissez depuis votre enfance et le fait que cette théorie ne soit pas encore terminée. La recherche dans ce domaine est très active et de nombreux problèmes ne sont toujours pas résolus dont, pour certains, des siècles après les avoir énoncés ! Pendant longtemps, il n'y avait pas d'application concrète à l'arithmétique et les mathématiciens s'y adonnaient car c'était une théorie belle en elle-même. Karl Friedrich Gauss surnommé le « prince des mathématiciens » disait « la mathématique est la reine des sciences et l'arithmétique est la reine des mathématiques ». Aujourd'hui, l'arithmétique est beaucoup utilisée en informatique et notamment pour tout ce qui est problème de sécurité et chiffrement. La sécurité des transactions réalisées sur internet est assurée par des résultats en arithmétique. Sans arithmétique pas d'achat sur internet sécurisé ! Elle est également utilisée aussi lorsqu'il faut corriger automatiquement des erreurs lors de transferts de données numériques. Ainsi, lorsque vous transférez des données comme un fichier par exemple il y a des algorithmes qui s'assurent de la validité des données et qui peuvent automatiquement les corriger en cas d'erreur. C'est ce que l'on appelle les codes correcteurs d'erreur. Voilà une discipline, étudiée pour elle-même et vieille de plusieurs millénaires qui produit des applications pour ce qui constitue la modernité ! Alors si vous aussi, vous voulez comprendre ces chiffrements mais aussi et surtout vous adonner à une discipline qui permet de faire des beaux raisonnements alors vous êtes au bon endroit !

Préambule : vous trouverez dans ce module douze démonstrations à connaître. Pour chaque démonstration, vous trouverez un niveau de difficulté qui lui est associé dont voici la signification :

Niveau de difficulté 1 : facile
Niveau de difficulté 2 : moyen
Niveau de difficulté 3 : difficile

CHAPITRE 1
DIVISIBILITÉ - DIVISION EUCLIDIENNE ET CONGRUENCES

Vous retrouverez dans ce chapitre deux notions connues et une nouvelle notion. Parmi les notions connues, nous commencerons en revenant aux notions de divisibilité et de multiples. Puis nous insisterons sur la notion de division euclidienne qui est la division que vous avez apprise à école primaire. Vous verrez qu'elle permet de faire beaucoup plus qu'une… division. Enfin nous terminerons sur la notion clé de ce chapitre et pratiquement du module entier qui est la congruence.

Finalement il y aura très peu de nouvelles notions mais elles seront abordées différemment de ce que vous avez l'habitude de faire. Nous ne pouvons que vous conseiller de faire tous les exercices car ils sont corrigés et montrent les méthodes et démarches de ce que l'on attend de vous et surtout comment utiliser ces outils mathématiques. Bon travail !

COMPÉTENCES VISÉES

- Divisibilité dans $\mathbb{Z}$.
- Division euclidienne d'un élément de $\mathbb{Z}$ par un élément de $\mathbb{N}^*$.
- Congruence dans $\mathbb{Z}$.

Première approche
Un exemple de code qui détecte les erreurs : le RIB

Nous allons nous intéresser à la notion de Clé dans un code.
Le RIB pour relevé d'identité bancaire est un nombre constitué de 23 chiffres. Ces 23 chiffres sont groupés en 4 groupes.
Le premier groupe noté B est constitué des 5 premiers chiffres du numéro il correspond au code Banque car chaque banque à son propre numéro qui lui est attribué.
Le deuxième groupe noté G est constitué des 5 chiffres suivants il correspond au code Guichet idem que pour les banques, un guichet a son propre code.
Le troisième groupe noté C est constitué des 11 chiffres suivants, il correspond au numéro de compte bancaire : dans une même banque, un numéro de compte bancaire est unique.
Le dernier groupe noté K est constitué des deux derniers chiffres il correspond à une clé (Key) qui permet de contrôler s'il y a eu une erreur dans le code RIB. Cette clé est calculée par rapport au 21 autres numéros. La clé K doit être un nombre entier compris entre 01 et 97.

Voici un exemple de RIB dont il manque la clé : $50020 \quad 00765 \quad 23488798210$ ..

- $B = 50020$ correspond au code banque
- $G = 00765$ correspond au code guichet
- $C = 23488798210$ correspond au numéro de compte

La clé K est définie comme ceci : En notant N le code Rib entier avec la clé, c'est-à-dire constitué des 23 numéros alors ce nombre doit être divisible par 97.
Le but du jeu est de déterminer la clé de ce RIB.

Méthode 1 : « la méthode force brute »
Une méthode très souvent utilisée en informatique est la méthode dite force brute. L'idée est très simple : tester toutes les possibilités et prendre celle qui marche. Ici il n'y a pas énormément de possibilités car il n'y a que 97 clés possibles. Finalement c'est même faisable à la main si on y prend le temps. Cette méthode est moins utilisable si le nombre de possibilités devient très grand (ce qui sera à la base des systèmes de sécurité actuels).
Trouver la clé de contrôle de ce code RIB en testant les clés une à une. Pour cela vous avez le choix : soit le faire à la main ce qui peut être long, soit utiliser un algorithme qui le fasse à votre place, ce que nous vous conseillons.
Maintenant que l'on vient de voir la méthode « force brute » passons à une autre méthode plus efficace en utilisant les mathématiques.

Méthode 2 : Avec les mathématiques.
Grâce aux mathématiques, nous allons pouvoir directement calculer la valeur de la clé. Pour cela nous avons besoin de quelques concepts comme la notion de congruences que vous verrez justement dans ce chapitre. Avec les congruences la recherche de la clé deviendra un problème simple et nous vous invitons alors à passer dans un premier temps cette activité préliminaire et à y revenir lorsque vous aurez abordé la notion de congruences. Vous verrez donc qu'avec de nouveaux outils mathématiques on peut aller beaucoup plus loin qu'en utilisant la force brute. Vers une autre écriture du nombre N :

1. Soit N le numéro complet du RIB avec les 23 numéros.
   Montrez que : $N=B\times1018+G\times1013+C\times102$Montrez que $N = B \times 10^{18} + G \times 10^{13} + C \times 10^{2} + K$

2. En déduire alors que $N \equiv K+3C+15G+89B [97]$

3. Soit R le reste de la division euclidienne de 3C+15G+89B par 97.
   Montrez alors que $K = 97 - R$

4. Retrouver alors la valeur de K

CORRECTION :

Voici un exemple d'algorithme écrit en langage python qui vous permettra de tester toutes les clés et qui renverra celle qui fonctionne :

```
# A est le code Rib sans la Clé que l'on a complété par 00 afin qu'il contienne 23 chiffres
A = 50020007652348879821000
for K in range(1,98) : # On teste pour toutes les clés entre 1 et 97
    N = A+K # Pour tester un code Rib N avec la clé K il suffit de faire la somme entre A et K
    if N%97 == 0 : # N%97 est le reste de la division euclidienne de N par 97
        print('la clé K vaut :',K)
```

```
la clé K vaut : 45
```

1. $B \times 10^{18}$ donne un nombre constitué des 5 chiffres de B suivi de 18 zéros. Ce qui donne un nombre de 23 chiffres. $G \times 10^{13}$ est constitué des 5 chiffres de G suivi de 13 zéros. La somme entre $B \times 10^{18}$ et $G \times 10^{13}$ donnera un nombre de 23 chiffres où les 5 premiers seront les chiffres de B, puis les 5 suivants seront les chiffres de B puis de 13 zéros. $C \times 10^2$ est un nombre constitué des 11 chiffres de C puis de 2 zéros et K est un nombre constitué de deux chiffres. Lorsque l'on fait la somme : $B \times 10^{18} + G \times 10^{13} + C \times 10^2 + K$, on aura un nombre constitué de 23 chiffres où les 5 premiers seront les chiffres de B, les 5 suivants les chiffres de G, puis viennent les 11 chiffres de C pour terminer avec les 2 chiffre de K. Finalement $B \times 10^{18} + G \times 10^{13} + C \times 10^2 + K$ construit le nombre N. Ainsi
$$N = B \times 10^{18} + G \times 10^{13} + C \times 10^2 + K$$

2. On a $10^2 \equiv 3[97]$ on en déduit, en utilisant les propriétés sur les congruences, que :
   $10^2 C \equiv 3C[97]$, $(10^2)^6 \equiv 3^6[97] \equiv 50[97] \Longrightarrow 10^{13} \equiv 500[97] \equiv 15[97]$ donc
   $10^{13} G \equiv 15G[97]$. On a :
   $10^2 \equiv 3[97] \Longrightarrow (10^2)^9 \equiv 3^9[97] \equiv 89[97\ ] \Longrightarrow 10^{18} B \equiv 89B[97]$
   Il ne reste plus qu'à sommer les congruences :
   $N = B \times 10^{18} + G \times 10^{13} + C \times 10^2 + K \equiv K + 3C + 15G + 89B[97]$

3. Par définition des congruences on a : $3C + 15G + 89B \equiv \mathrm{R}[97]$ or
$N \equiv K + 3C + 15G + 89B$ [97]. De plus, la clé K est définie telle que N soit divisible par 97. Cela signifie que $N \equiv 0[97]$. On a donc que $K + 3C + 15G + 89B \equiv 0[97]$ et comme
$3C + 15G + 89B \equiv R[97]$ il vient que $K + R \equiv 0[97]$ autrement dit $K + R = 97q$ avec q un entier naturel.
Mais comme $1 \leq K \leq 97$ et $0 \leq R \leq 96$ alors
$0 + 1 \leq K + R \leq 97 + 96 \Leftrightarrow 1 \leq K + R \leq 193 \Leftrightarrow 1 \leq 97q \leq 193 \Leftrightarrow \frac{1}{97} \leq q \leq \frac{193}{97}$
Or $\frac{1}{97} \approx 0{,}01$ et $\frac{193}{97} \approx 1{,}99$. Le seul entier naturel compris entre $\frac{1}{97}$ et $\frac{193}{97}$ est 1. Donc $q = 1$ et finalement $K + R = 97$ c'est-à-dire $K = 97 - R$.

4. $3C + 15G + 89B = (3 \times 23488798210) + (15 \times 00765) + (89 \times 50020) \equiv 52[97]$
52 est le reste de la division euclidienne de $3C + 15G + 89B$ par 97. On obtient alors que $K = 97 - 52 = 45$. Le numéro Rib sera alors : 50020 00765 23488798210 **45**
On retrouve bien la valeur $K = 45$ de la première partie ce qui est rassurant ! Remarquez que dans la première partie on avait utilisé toutes les clés possibles. Cela est pertinent si le nombre de clés n'est pas immense. Avec l'arithmétique, on peut calculer directement la clé ce qui est plus efficace.

01 DIVISIBILITÉ - DIVISION EUCLIDIENNE ET CONGRUENCES

Divisibilité dans $\mathbb{Z}$

Commençons par une définition d'un concept que vous connaissez déjà depuis très longtemps : la notion de diviseur.

DÉFINITION

Soient a et b deux entiers relatifs. On dit que a divise b si et seulement s'il existe un entier relatif k tel que

$$b = ka$$

On dira alors que :

- b est un multiple de a
- a est un diviseur de b

On notera alors :

$$a|b$$

Lorsque que l'on écrit que $2|10$, cela signifie que :

- 2 divise 10
- 2 est un diviseur de 10
- 10 est un multiple de 2
- 10 est divisible par 2

Ce sont quatre manières équivalentes de signifier la même notion. Il est important de la comprendre et de saisir que dans la notation $a|b$ le diviseur est a et le multiple est b.
En reprenant la définition, la justification que $2|10$ est qu'il existe un entier k tel que $10 = k \times 2$ en effet en prenant $k = 5$ on a bien l'égalité voulue. Pour prouver qu'un entier a divise un entier b, il faudra montrer l'existence d'un entier k. Pour résumer on a alors :

$$a|b \Leftrightarrow a \text{ divise } b \Leftrightarrow a \text{ est un diviseur de } b \Leftrightarrow b \text{ est un multiple de } a \Leftrightarrow b = ka, k \in \mathbb{Z}$$

Il faut savoir interpréter une égalité d'entiers. Quand on écrit que :

$$a = b \times c$$

Cela signifie que : $c|a$ et $b|a$ autrement dit que a est un multiple de c et b mais aussi que c et b sont des diviseurs de a.

DÉFINITION

Soient a et b deux entiers relatifs. On appelle combinaison linéaire d'entiers relatifs de a et b toute opération du type :

$$au + bv$$

Avec u et v des nombres entiers relatifs.

Exemples de combinaisons linéaires de a et b :

1. $2a + 3b$ est une combinaison linéaire de a et b. On prend comme valeurs : $u = 2, v = 3$
2. $a + b$ est une combinaison linéaire de a et b. On prend comme valeurs : $u = 1, v = 1$
3. $a - b$ est une combinaison linéaire de a et b. On prend comme valeurs : $u = 1, v = -1$
4. a est une combinaison linéaire de a et b. On prend comme valeurs : $u = 1, v = 0$
5. b est une combinaison linéaire de a et b. On prend comme valeurs : $u = 0, v = 1$
6. $a \times b$ est une combinaison linéaire de a et b. On prend comme valeurs : $u = b, v = 0$

Vous n'aurez pas d'autre définition pour cette première partie ! Il ne faut connaître que les définitions de multiples et diviseurs ainsi que de combinaison linéaire d'entiers relatifs. A partir des définitions nous allons voir quelques propriétés importantes :

PROPRIÉTÉS

1. Toutes combinaisons linéaires de nombres entiers relatifs est un entier relatif.

Commentaires : il vient alors que si a et b sont des entiers alors toutes opérations du types $au + bv$ avec u et v un couple d'entiers relatifs, reste un entier relatif.

2. 0 est le multiple universel : Tout nombre entier relatif non nul a divise 0.

Commentaires : on a, par exemple, que 2 divise 0 car il existe un entier relatif k tel que $0 = 2 \times k$. En l'occurrence pour $k = 0$. Cela fonctionne avec n'importe quel autre entier ! En effet, si a est un entier relatif alors on a toujours $0 = a \times 0$ et donc a divise 0.

3. 1 est le diviseur universel : 1 divise tous les entiers relatifs.

Commentaires : en effet, on a toujours l'égalité : $a = 1 \times a$ pour tout entier relatif a. Ainsi 1 divise n'importe quel entier.

4. Soient a, b, n trois entiers relatifs. Si $n = a \times b$ alors a et b sont des diviseurs de n.

Commentaires : lorsque que l'on écrit que $10 = 2 \times 5$ alors on met en évidence deux diviseurs de 10 qui sont 2 et 5. Autrement dit, en écrivant un entier comme produit de deux entiers on trouve des diviseurs deux par deux.

5. Si $a|b$ et $b \neq 0$ alors $|a| \leq |b|$

Commentaires : cette propriété signifie que tous les diviseurs d'un entier b non nul, sont plus petits ou égaux en valeur absolue que $|b|$.
On peut vérifier sur quelques exemples : 2 divise 4 et $2 \leq 4$.
La précision de la valeur absolue est importante : 2 divise -8 or $2 \geq -8$ mais en valeur absolue on a bien $2 \leq |-8| = 8$. On retiendra que si un entier est un diviseur d'un autre entier, celui-ci est forcément plus petit en valeur absolue. On peut conclure que si d est un diviseur de b un entier non nul, alors $-b \leq d \leq b$ et qu'il existe un nombre fini de diviseurs d'un entier non nul.

6. Tout entier relatif non nul b admet un nombre fini de diviseurs.

Commentaires : il est important de préciser que l'entier est non nul car on a vu que 0 était le multiple universel donc qu'il possède une infinité de diviseurs, c'est le seul entier qui admet cette propriété. Tout autre entier admet un nombre fini de diviseurs pour la simple raison qu'un diviseur d'un entier b est nécessairement un entier compris dans l'intervalle $[-b; b]$. Or cet intervalle contient un nombre fini d'entiers. En effet, le nombre maximal de diviseurs que peut admettre un entier b vaut $2b + 1$. Ainsi le nombre 10 ne peut pas avoir plus de $2 \times 10 + 1 = 21$ diviseurs, en réalité il en possède beaucoup moins mais on a une majoration simple du nombre de diviseurs d'un entier non nul.

7. $a|b \Leftrightarrow -a|b \Leftrightarrow a|(-b) \Leftrightarrow -a|(-b)$

Commentaires : cette propriété permet de se doter d'une méthode efficace pour déterminer les diviseurs d'un nombre entier. En effet, elle nous dit que les diviseurs d'un entier b sont les mêmes que l'entier $-b$. Ainsi, si l'on nous demande de trouver les diviseurs de l'entier -230 cherchons plutôt ceux de 230 puisque ce sont les mêmes ! De plus, elle dit que si a est un diviseur de b alors $-a$ est aussi un diviseur de b. On cherchera alors dans un premier temps les diviseurs positifs puis on complétera par les opposés de diviseurs que l'on a trouvés. Un exemple avec le nombre -10 :

Chercher les diviseurs de -10 revient à chercher les diviseurs de 10. Déterminons, dans un premier temps les diviseurs positifs de 10 parmi les entiers $\{0,1,2,\dots,10\}$ puisqu'un diviseur doit être inférieur à $|10| = 10$. On a que $10 = 1 \times 10$ donc les nombres 1 et 10 sont des diviseurs de 10. Puis $10 = 2 \times 5$ donc les nombres 2 et 5 sont aussi des diviseurs de 10. En testant pour 3 et 4, on remarque que ce ne sont pas des diviseurs de 10 puis en testant pour 5 on a $10 = 5 \times 2$ nous avons le produit inverse de 2×5 ce qui veut dire qu'il n'y pas d'autres diviseurs positifs de 10. Finalement les diviseurs positifs de 10 sont : $1,2,5,10$ et donc les diviseurs de 10 et de -10 sont : $-1,-2,-5,-10,1,2,5,10$.

8. Soient a, b, c trois entiers relatifs. Si $a|b$ et $a|c$ alors $a|(bu+nv), (u,v) \in \mathbb{Z}^2$

Commentaires : c'est la propriété ultime de cette première partie ! A connaître parfaitement et surtout à savoir utiliser. Vous trouverez ci-après deux cas d'utilisations qu'il est important de comprendre et de savoir-faire.

CAS D'UTILISATION

Cas d'utilisation numéro 1

Soit n un entier relatif. On cherche à déterminer tous les entiers relatifs tels que $n+1$ divise $n+8$.

Pour cela nous allons utiliser un raisonnement par **« Analyse-Synthèse ».** Dans la partie « Analyse », on suppose que l'on a une solution et on essaye d'en déduire des propriétés nécessaires de cette solution. A la fin de la « Synthèse », nous devrions avoir un ensemble de solutions potentielles. La partie synthèse consistera à tester à la main si les solutions potentielles répondent bien à la question du problème. Retenez bien ce type de raisonnement que l'on fera régulièrement en arithmétique.

Analyse :

Supposons qu'il existe un entier relatif n tel que $n+1$ divise $n+8$. Comme $n+1$ divise $n+1$ alors $n+1$ divise toutes combinaisons linéaires de $n+8$ et $n+1$. C'est-à-dire que $n+1$ divise $u(n+8)+v(n+1)$ avec u et v des entiers relatifs. En particulier en prenant $u=1, v=-1$ on obtient que $n+1$ divise $n+8-n-1=7$. Donc si $n+1|n+8$ alors $n+1|7$ donc $n+1$ est nécessairement un diviseur de 7. Or 7 a pour diviseurs : $\{-7,-1,1,7\}$. Il en résulte que $n+1$ ne peut prendre que quatre valeurs potentielles que l'on peut placer dans ce tableau :

Valeurs de $n+1$	-7	-1	1	7
Valeur de n	-8	-2	0	6

Les seules valeurs possibles de n telles que $n+1$ divise $n+8$ sont : $-8,-2,0,6$.

Synthèse : Vérifions pour chaque valeur de n trouvée dans l'analyse si $n+1$ divise $n+8$:

Valeurs de n	-8	-2	0	6
Valeurs de $n+1$	-7	-1	1	7
Valeurs de $n+8$	0	6	8	14
$n+1$ divise $n+8$?	Oui	Oui	Oui	Oui

Soit n un entier relatif. On cherche à déterminer tous les entiers relatifs tels que $n+1$ divise $n+8$.
Pour cela nous allons utiliser un raisonnement par **« Analyse-Synthèse ».** Dans la partie « Analyse », on suppose que l'on a une solution et on essaye d'en déduire des propriétés nécessaires de cette solution. A la fin de la « Synthèse », nous devrions avoir un ensemble de solutions potentielles. La partie synthèse consistera à tester à la main si les solutions potentielles répondent bien à la question du problème. Retenez bien ce type de raisonnement que l'on fera régulièrement en arithmétique.

Analyse : supposons qu'il existe un entier relatif n tel que $n+1$ divise $n+8$. Comme $n+1$ divise $n+1$ alors $n+1$ divise toutes combinaisons linéaires de $n+8$ et $n+1$. C'est-à-dire que $n+1$ divise $u(n+8)+v(n+1)$ avec u et v des entiers relatifs. En particulier en prenant $u=1, v=-1$ on obtient que $n+1$ divise $n+8-n-1=7$. Donc si $n+1|n+8$ alors $n+1|7$ donc $n+1$ est nécessairement un diviseur de 7. Or 7 a pour diviseurs : $\{-7,-1,1,7\}$. Il en résulte que $n+1$ ne peut prendre que quatre valeurs potentielles que l'on peut placer dans ce tableau :

Valeurs de $n+1$	-7	-1	1	7
Valeur de n	-8	-2	0	6

Les seules valeurs possibles de n telles que $n+1$ divise $n+8$ sont : $-8,-2,0,6$.
Synthèse : vérifions pour chaque valeur de n trouvée dans l'analyse si $n+1$ divise $n+8$:

Valeurs de n	-8	-2	0	6
Valeurs de $n+1$	-7	-1	1	7
Valeurs de $n+8$	0	6	8	14
$n+1$ divise $n+8$?	Oui	Oui	Oui	Oui

Nous observons que pour chaque valeur de n, $n+1$ divise $n+8$. Nous venons de trouver les solutions de notre problème : $n \in \{-8,-2,0,6\}$.

Observez, dans l'analyse, que nous avons choisi une combinaison linéaire particulière. En choisissant les valeurs $u=1, v=-1$, nous nous sommes retrouvés avec une combinaison linéaire sans "n". C'est la clé de la méthode : trouver un bon couple de valeurs de u et v afin de supprimer les n dans la combinaison linéaire.

Cas d'utilisation numéro 2
Déterminer tous les entiers relatifs n tel que $n-2|3n+4$:
Analyse : Soit un entier n tel que $n-2|3n+4$. Comme $n-2|n-2$, alors

$$n-2|u(3n+4)+v(n-2)$$

Avec u et v entiers relatifs. En particulier :

$$n-2|3n+4-3(n-2) \Longrightarrow n-2|3n+4-3n+6 \Longrightarrow |3n+4-3(n-2) \Longrightarrow n-2|10$$

Donc $n-2$ est un diviseur de 10. Or l'ensemble des diviseurs de 10 est : $\{-10,-5,-2,-1,1,2,5,10\}$
Les solutions potentielles n sont donc :

Valeurs de $n-2$	-10	-5	-2	-1	1	2	5	10
Valeurs de n	-8	-3	0	1	3	5	7	12

Réciproquement, vérifions si pour chaque valeur de n dans le tableau on a bien $n-2|3n+4$:

Valeurs de n	-8	-3	0	1	3	4	7	12
Valeurs de $n-2$	-10	-5	-2	-1	1	2	5	10
Valeurs de $3n+4$	-20	-5	4	7	13	20	25	40
$n+1$ divise $n+8$?	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

$n+1|3n+4$ si et seulement si $n \in \{-8,-3,0,1,3,4,7,12\}$
Ces exemples doivent être bien maîtrisés. Il sera très fréquent de rechercher une combinaison linéaire qui annule les n.

À VOUS DE JOUER 1

Trouvez les diviseurs d'un entier

Déterminez l'ensemble des diviseurs des entiers suivants :

$a = 238$	$b = 123$	$c = -68$	$d = -235$	$e = 17$	$f = 59$	$G = 656$

À VOUS DE JOUER 2

« Factoriser tu penseras ! »

Déterminez les entiers **naturels** x, y tels que $x^2 - y^2 = 8$

Aide : la clé dans les exercices de ce genre sera de **factoriser** puis d'utiliser le raisonnement par analyse synthèse.

À VOUS DE JOUER 3

« Discuter en fonction des cas tu penseras ! »

Il arrive parfois que l'on puisse démontrer une propriété **par disjonction des cas** :

Soit n un entier relatif, montrez que $n(n+1)$ est toujours un nombre pair.

Aide : rappelons qu'un entier est pair si et seulement s'il existe un entier k tel que $a = 2k$

Un entier est impair si et seulement s'il existe un entier k tel que $a = 2k + 1$

À VOUS DE JOUER 4

« Par récurrence tu raisonneras ! »

D'autres propriétés peuvent se démontrer par récurrence. Illustrons cela par cet exercice : Montrez que pour tout n entier naturel $6|n(n^2-1)$.

À VOUS DE JOUER 5

« T'entraîner tu devras »

A l'aide de ce que vous avez vu précédemment, voici une liste de questions qui vous permettra de vous entraîner.

1. Montrez par récurrence que pour tout entier naturel n : $4^n + 2$ est un multiple de 3.

2. Montrez par récurrence que pour tout entier naturel n : $3^{2n+1} + 2^{n+2}$ est divisible par 7.

3. Soit $n \geq 2$ montrez que $n-1, n+1, n^2+1$ sont des diviseurs de n^4-1

4. Déterminez les entiers naturels x et y tels que $x^2 - y^2 + 2(x+y) = 23$

02 DIVISIBILITÉ - DIVISION EUCLIDIENNE ET CONGRUENCES

Division euclidienne d'un élément de $\mathbb{Z}$ par un élément de $\mathbb{N}$

Cette partie est très courte en termes de cours et de résultats à connaître. Vous connaissez déjà, au moins par le nom, l'outil que l'on va étudier, il s'agit de la division euclidienne ! La fameuse division que vous avez étudiée lorsque vous étiez en école primaire. On va approfondir la connaissance de cet outil et s'apercevoir à quel point on peut aller beaucoup plus loin dans l'analyse des nombres entiers grâce à la division euclidienne.

PROPRIÉTÉ

Soit a un entier relatif et b un entier naturel non nul. A tout couple (a, b) il existe un unique couple d'entiers noté (q, r) tel que :

$$a = bq + r \text{ et } 0 \leq r \leq b - 1$$

Commentaires : tout est important dans cette propriété ! Elle est courte mais il faut la connaître dans ses moindres détails ! Elle signifie que l'on peut toujours décomposer un entier relatif a par rapport à un entier naturel non nul b et surtout qu'il n'y a qu'un nombre fini de décompositions possibles : autant que de valeurs de r c'est-à-dire qu'il peut y avoir en tout r décompositions possibles. Exemple si on prend deux entiers : $a = 78$ et $b = 13$ alors il existe un unique couple q et r tel que $78 = 13q + r$ avec la condition très importante : $0 \leq r \leq 12$. On trouve le couple $q = 6$ et $r = 1$ et ce couple **est unique.** Pour trouver les coefficients q et r on peut poser à la main la division de a par b.

À VOUS DE JOUER 6

Pour chaque couple a, b determinez l'unique couple q, r tel que $a = bq + r$ avec $0 \leq r \leq b - 1$.

1. $a = 1200, b = 13$

2. $a = -72, b = 19$

3. $a = 134, b = 15$

4. $a = -1789, b = 14$

5. $a = 9, b = 55$

DÉFINITION

Soit a un entier relatif et b un entier naturel non nul. Effectuer la division euclidienne de a par b, c'est trouver l'unique couple (q, r) de nombres entiers relatifs tel que

$$a = bq + r \text{ et } 0 \leq r < b$$

Vocabulaire : dans la division euclidienne de a par b :
a est le dividende, b le diviseur, q le quotient et r le reste.

Commentaires : lorsque nous avons trouvé les valeurs des couples q et r du « A vous de jouer 6 », on venait de faire les divisions euclidiennes de a par b. Le conseil que je peux vous donner est donc de bien connaître le vocabulaire c'est-à-dire les différents noms des parties dans la décomposition de a par b. Bien se souvenir de la condition sur le reste : $0 \leq r \leq b - 1$.
Voici deux cas d'utilisation de la division euclidienne de a par b dans des situations plus générales :

CAS D'UTILISATION

Cas d'utilisation 1. « Déterminer le reste d'une division euclidienne tu sauras »
Cherchons à déterminer les restes de $a = 9n + 17$ par $b = 2n + 3$ en fonction des valeurs de n avec $n \geq 0$.
Le principe est d'essayer d'écrire $9n + 13$ en fonction de $2n + 3$ afin d'obtenir une forme qui ressemble à une division euclidienne.
On a $9n + 17 = (2n + 3) \times 4 + (n + 5)$. Observons à travers cette égalité que l'on a une expression de la forme $a = bq + r$ or cette décomposition est la division euclidienne de a par b si et seulement si

$$0 \leq n + 5 \leq 2n + 2 \Longrightarrow n + 2 \geq 5 \Longrightarrow n \geq 3$$

Ainsi pour tout $n \geq 3$ le reste de a par b vaut $n + 5$. Il reste à terminer pour les autres possibilités de n que l'on va résumer dans un tableau :

n	0	1	2	≥ 3
a	17	26	35	$9n + 17$
b	3	5	7	$2n + 3$
r	2	1	0	$n + 5$

Finalement nous avons tous les restes possibles de a par b suivant les valeurs de n.

Cas d'utilisation numéro 2. « La disjonction des cas par rapport au reste tu penseras ».

Soit $A = n(n^2 + 11)$ nous souhaitons démontrer que A est un multiple de 3 pour n'importe quelle valeur de $n \geq 0$. Une première façon de faire est d'utiliser un raisonnement par récurrence. Une alternative au raisonnement par récurrence est de procéder par disjonction des cas. Ce que nous allons montrer maintenant :
Nous cherchons à montrer que A est un multiple de 3. En considérant la division euclidienne d'un entier n par 3 nous pouvons écrire que $n = 3q + r$ avec $0 \leq r \leq 2$. C'est-à-dire que n'importe quel entier n se décompose d'une de ces trois manières : $n = 3q, n = 3q + 1, n = 3q + 2$
Pour chacune de ces décompositions, nous allons discuter de l'expression de A.
2. Si $n = 3q$:

$$a = 3q(9q^2 + 5) = 3(9q^3 + 5q) = 3K$$

avec $K = 9q^3 + 5q$ qui est un entier
Conclusion : a est un multiple de 3.

3. Si $n = 3q + 1$:

$$a = (3q+1)(9q^2 + 6q + 1 + 5) = (3q+1)(9q^2 + 6q + 6)$$
$$= (3q+1)3(3q^2 + 2q + 2) = 3K'$$

Avec $K' = (3q+1)(3q^2 + 2q + 2)$

Conclusion : a est un multiple de 3.

4. Si $n = 3q + 2$:

$$a = (3q+2)(9q^2 + 12q + 4 + 5) = (3q+2)(9q^2 + 12q + 9)$$
$$= (3q+2)3(3q^2 + 4q + 3) = 3K"$$

Avec $K" = (3q+2)(3q^2 + 4q + 3)$

Conclusion : a est un multiple de 3.

Nous venons de prouver que quelle que soit la valeur de n, le nombre A est un multiple de 3.

À VOUS DE JOUER 7

« T'entraîner tu devras »

La différence entre deux entiers naturels est 538. Si l'on divise l'un par l'autre, le quotient est 13 et le reste 34. Quels sont ces deux entiers naturels ?

À VOUS DE JOUER 8

1. Trouvez les entiers naturels, dont le quotient de la division euclidienne par 5 est égal au reste.

2. Quels sont les restes et dividendes possibles lorsque le quotient de la division euclidienne entre le dividende et 3 vaut 7 ?

03 DIVISIBILITÉ - DIVISION EUCLIDIENNE ET CONGRUENCES

Congruences

Nous allons définir un nouvel outil très puissant que nous utiliserons tout au long du cours. Cet outil se nomme : les congruences. Sans exagération, il s'agit d'un outil central de ce cours d'arithmétique. C'est pourquoi il y aura plus d'exercices d'entraînements car le nombre de situations où l'on rencontrera des congruences est plus grand. Nous utiliserons des congruences jusqu'à la fin du module d'arithmétique et l'on peut dire qu'avec ce chapitre nous entrons véritablement dans le vif du sujet.

Alerte : Pour bien démarrer les congruences je vous conseille d'être à l'aise avec la notion de division euclidienne. Si ce n'est pas le cas refaire les exercices afin d'être familier avec les notions de diviseurs, multiples et surtout de reste d'une division euclidienne. En effet, en étant rapide, les congruences portent une attention très particulière à la notion de reste dans une division euclidienne et lui donne une place centrale.

DÉFINITION

Dire que a et b sont congrus modulo n signifie que a et b ont le même reste dans la division euclidienne par n. On notera alors que $a \equiv b[n]$ (lire a congru à b modulo n).

Commentaires : Cette définition mérite quelques exemples pour comprendre. Prenons l'entier 3, nous dirons que les entiers 4 et 10 sont congrus modulo 3 que l'on notera $4 \equiv 10[3]$ car le reste de la division euclidienne de 4 par 3 vaut 1 et que le reste de la division euclidienne de 10 par 3 vaut 1 également. Finalement deux entiers sont congrus modulo n si et seulement s'ils ont le même reste par n.
Remarquons que 13 est aussi congru à 4 modulo 3 tout comme 1 est congru à 4 modulo 3. Nous pouvons ainsi écrire cette suite de congruences : $10 \equiv 13[3] \equiv 4[3] \equiv 1[3]$ car tous ces nombres ont le même reste par 3.
Voyez la phrase, 21 est congru à 1 modulo 5 comme une équivalence entre 21 et 1 par rapport à 5. Du fait que les nombres 21 et 5 ont le même reste par 5 on les considérera comme équivalents vis-à-vis de la division par 5.
Ce concept n'est pas tellement nouveau.
En effet, si l'on vous demande de donner un multiple du nombre 4 : Vous pouvez répondre indifféremment 8, 16 ou 20. Bien que non égaux, ces nombres sont équivalents en ce qui concerne le fait d'être des multiples de 4. Mais être un multiple de 4 signifie que le reste de la division par 4 vaut 0. Ainsi on pourra écrire que $8 \equiv 16[4] \equiv 20[4] \equiv 0[4]$
Tous les multiples d'un nombre a sont donc congrus entre eux modulo a ! L'idée des congruences consistera à pouvoir remplacer un nombre compliqué par un nombre plus simple qui lui sera congru.
En effet à un nombre donné a il existe une infinité de nombres b qui sont congrus à a modulo c. Le principe sera de choisir parmi tous ces nombres b, le nombre le plus simple qui permettra de faciliter les calculs et de démontrer les propriétés. Avant de commencer, voyons les propriétés des congruences :

PROPRIÉTÉS

1. Soient a et b deux entiers : $a \equiv b[n]$ si et seulement si $n|(a-b)$ nous avons alors l'équivalence suivante très pratique : $a \equiv b[n] \Leftrightarrow a = kn + b$ avec k un entier. Nous avons alors que pour tout k entier $a \equiv kn + a[n]$

Commentaires : c'est une autre façon, tout à fait équivalente de définir des congruences. La dernière équivalence est très pratique pour trouver des nombres qui sont congrus entre eux. Par exemple, si l'on cherche des nombres congrus à 56 modulo 6. Ce sont des nombres a de la forme $a = 6k + 56$ avec k entier. Ainsi en remplaçant par différentes valeurs de k on obtient d'autres nombres congrus à 56 modulo 6. Par exemple, en prenant successivement comme valeur de $k = 1,2,3,-1,-2,-3$ on pourra écrire :

$$56 \equiv 62[6] \equiv 68[6] \equiv 74[6] \equiv 50[6] \equiv 44[6] \equiv 38[6]$$

4. Soient a et b deux entiers et r le reste de la division de a par n alors : $a \equiv r[n]$

Commentaire : quand on cherche un nombre congru à a modulo n, il est très souvent pertinent de choisir le reste de la division euclidienne de a par n. En effet le reste r est un nombre de choix et beaucoup de problèmes pourront se résoudre en choisissant comme nombre congru à a son reste r par n. Dans l'exemple précédent, on avait vu que

$$56 \equiv 62[6] \equiv 68[6] \equiv 74[6] \equiv 50[6] \equiv 44[6] \equiv 38[6]$$

Mais il est souvent plus intéressant de choisir parmi tous ces nombres le reste de la division euclidienne de 56 par 6. On aura alors $56 \equiv 2[6]$.
Le conseil : quand on cherchera des nombres congrus à a modulo n on choisira pratiquement toujours le reste r. Les rares cas où l'on ne choisira pas le reste, c'est si on a $a \equiv -1[n]$.
Exemple : considérons le nombre 13 et raisonnons modulo 7. On a $13 \equiv 6[7]$ car 6 est le reste de la division euclidienne de 13 par 7. Mais on a aussi $13 \equiv 6[7] \equiv 7k + 6[7]$
Et en prenant $k = -1$ on se retrouve avec $13 \equiv -1[7]$. Vous verrez alors dans les exercices qu'il sera préférable de travailler avec $13 \equiv -1[7]$.

5. Soient Si $a \equiv b[n]$ et $c \equiv d[n]$ alors :

$$a+c \equiv b+dn$$

Commentaires : on dit que les congruences sont compatibles avec l'addition.
Exemple d'utilisation : considérons un entier n tel que $n \equiv 1[7]$ et $13 \equiv -1[7]$ alors on pourra écrire que $n + 13 \equiv 1 - 1[7] \equiv 0[7]$ et on vient de montrer que si $n = 7k + 1$ alors $n + 13$ est un multiple de 7.

$$a - c \equiv b - d[n]$$

Commentaires : on dit que les congruences sont compatibles avec la soustraction.
Exemple : Considérons un entier n tel que $n \equiv 4[8]$ et $20 \equiv 4[8]$ alors $n - 20 \equiv 4 - 4[8] \equiv 0[8]$.
On vient de montrer dans cet exemple, que si un nombre $n = 8k + 4$ alors $n - 20$ est forcément un multiple de 8.

$$ac \equiv bd[n]$$

Commentaires : on dit que les congruences sont compatibles avec la multiplication.
Exemple : Considérons n tel que $n \equiv 3[6]$ et m tel que $m \equiv 2[6]$ alors

$$nm \equiv 3 \times 2[6] \equiv 6[6] \equiv 0[6]$$

Car le reste de 6 dans la division euclidienne par 6 vaut 0. On vient de montrer que si $n = 6k + 3$ et $m = 6k' + 2$ alors le produit nm est forcément un multiple de 6.

$$a^k \equiv b^k[n], k \in \mathbb{N}$$

Commentaires : on dit que les congruences sont compatibles avec la puissance entière.
Exemple : Soit n tel que $n \equiv 2[8]$ alors $n^3 \equiv 2^3[8] \equiv 8[8] \equiv 0[8]$. Nous venons de montrer que si $n = 8k + 2$ alors n^3 est un multiple de 8.

À VOUS DE JOUER 9

Pour chaque valeur de a donnée, trouvez un entier relatif x tel que :
$a \equiv x[9]$ et $-4 \leq x < 5$:

$a = 13$	$a = 87$	$a = 5$	$a = -17$	$a = -67$	$a = 87$

Voici l'outil essentiel pour utiliser les congruences de manière efficace : « **le tableau des restes modulo n tu découvriras ».**

Considérons n un entier naturel et l'on cherche à résoudre une équation sous forme de congruence. A savoir que l'on cherche à déterminer l'ensemble des entiers naturels n tel que $n^2 \equiv 1[4]$. L'outil le plus efficace reste **le tableau des restes modulo 4 !** C'est un tableau où l'on raisonnera modulo 4 et où dans chaque case on écrira le reste de la division euclidienne par 4. Comme un nombre n quelconque ne peut avoir comme reste modulo 4 que les possibilités suivantes : $0,1,2,3$ nous allons tester toutes les possibilités :

$n \equiv \cdots [4]$	0	1	2	3
$n^2 \equiv \cdots [4]$	0	1	$4 \equiv 0[4]$	$9 \equiv 1[4]$

La première ligne représente l'ensemble des restes possibles modulo 4. La deuxième ligne se déduit de la première en passant au carré. Puis on écrit le reste modulo 4 de chaque case. Ainsi si $n \equiv 3[4]$ alors $n^2 \equiv 9[4] \equiv 1[4]$ que l'on écrit dans la case correspondante. Quand le tableau est complet il ne reste plus qu'à l'analyser par rapport à notre problème. Nous cherchons pour quel entier n, $n^2 \equiv 1[4]$. Nous voyons que cela correspond à deux situations : si $n \equiv 1[4]$ ou si $n \equiv 3[4]$. Donc les entiers n tels que $n^2 \equiv 1[4]$ sont les entiers de la forme $n = 4k + 1$ ou $n = 4k + 3$.

LES CLÉS DU BAC by COURS PI

PROUVER UN CRITÈRE DE DIVISIBILITÉ GRÂCE AUX CONGRUENCES TU SAURAS

Nous allons apprendre à traiter la question suivante : comment démontrer un critère de divisibilité avec les congruences ? Nous allons traiter la question pour le critère de divisibilité par 3 pas à pas.

Le prérequis important : Soit n un entier naturel. On rappelle que tout entier peut s'écrire de manière unique :

$$n = a_p \times 10^p + a_{p-1} \times 10^{p-1} + a_{p-2} \times 10^{p-2} + \cdots + a_2 \times 10^2 + a_1 \times 10^1 + a_0 \times 10^0$$

Avec $p \in$ N et $a_0, a_1, a_2, \ldots, a_p \in \{0,1,2, \ldots, 9\}$. C'est ce que l'on appelle, **l'écriture décimale de n.**
On écrit $n = \overline{a_p a_{p-1}, a_{p-2} \ldots a_2 a_1 a_0}$ afin de ne pas confondre le nombre avec un produit. Remarque a_0 est le chiffre des unités, a_1 les chiffre des dizaines, a_2 celui des centaines et ainsi de suite.
Exemple : $n = 2345 = 2 \times 10^3 + 3 \times 10^2 + 4 \times 10^1 + 5$. Ici $a_0 = 5, a_1 = 4, a_2 = 3, a_3 = 2$.

Étape 1 : Se souvenir que tout nombre entier admet une unique écriture décimale et commencer par écrire sa décomposition : Soit n un nombre entier naturel alors il existe une suite de nombres $a_0, a_1, a_2, \ldots, a_p \in \{0,1,2, \ldots, 9\}$ telle que :

$$n = a_p \times 10^p + a_{p-1} \times 10^{p-1} + a_{p-2} \times 10^{p-2} + \cdots + a_2 \times 10^2 + a_1 \times 10^1 + a_0 \times 10^0$$

Étape 2 : Ce qui apparaît clairement dans une décomposition en écriture décimale c'est la présence des puissances de 10. Nous allons analyser les puissances de 10 modulo 3 (car l'on cherche un critère pour 3 sinon on adapte le modulo au nombre pour lequel on désire trouver un critère) et déterminer de quoi 10^p est congru modulo 3 :
On a : $10^0 = 1 \equiv 1[3], 10^1 \equiv 1[3]$
Nous avons un résultat intéressant : $10^1 \equiv 1[3]$ cela va nous permettre d'obtenir toutes les puissances de 10.
Comme $10^1 \equiv 1[3]$ alors pour tout p entier naturel non nul on a : $10^p \equiv 1^p[3] \equiv 1[3]$.
Finalement on obtient le résultat suivant : pour tout $p \in \mathbb{N}, 10^p \equiv 1[3]$.

Étape 3 : Maintenant que l'on a les restes de 10^p modulo 3 il reste à déterminer de quoi l'entier n est congru modulo 3. Pour cela on utilise les différentes propriétés des congruences :
Par compatibilité de la multiplication il vient : pour tout $p \in \mathbb{N}, a_p \times 10^p \equiv a_p \times 1[3] \equiv a_p[3]$
Comme cela fonctionne pour tout $p \in \mathbb{N}$ alors on a :

$$\begin{cases} a_0 \times 10^0 \equiv a_0[3] \\ a_1 \times 10^1 \equiv a_1[3] \\ \quad . \\ \quad . \\ a_p \times 10^p \equiv a_p[3] \end{cases}$$

Par compatibilité de la somme, en additionnant toutes les lignes entre elles cela donne :

$$a_p \times 10^p + a_{p-1} \times 10^{p-1} + \cdots + a_1 \times 10^1 + a_0 \times 10^0 \equiv a_p + a_{p-1} + \cdots + a_1 + a_0[3]$$

Donc $n \equiv a_p + a_{p-1} + \cdots + a_1 + a_0[3]$.

Étape 4 : Il reste à conclure en revenant au problème initial.
Nous cherchons un critère de divisibilité par 3. Un entier naturel n est divisible par 3 si et seulement si $n \equiv 0[3]$. $n \equiv a_p + a_{p-1} + \cdots + a_1 + a_0[3]$. Donc n est divisible par 3 si et seulement si :

$$a_p + a_{p-1} + \cdots + a_1 + a_0 \equiv 0[3]$$

Nous venons de montrer qu'un entier naturel quelconque est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Prouver, à l'aide des congruences, les critères de divisibilité suivants :

1. Un entier est divisible par 9 si, et seulement si, la somme de ses chiffres est un multiple de 9.

2. Un entier est divisible par 5 si, et seulement si, son dernier chiffre est 0 ou 5.

3. Un entier est divisible par 4 si, et seulement si, le nombre formé avec ses deux derniers chiffres est un multiple de 4.

4. Un entier est divisible par 25 si, et seulement si, le nombre formé avec ses deux derniers chiffres est un multiple de 25.

5. Un entier naturel est divisible par 11, si et seulement si, la différence entre la somme des chiffres de rang pair et la somme des chiffres de rang impair est un multiple de 11.
   Le nombre $954\,823\,057$ est-il divisible par 11 ? Donnez un nombre de 10 chiffres qui soit divisible par 11.

CORRECTION :

1. Remarquons que :
   $10 \equiv 1[9]$. Donc $10^p \equiv 1[10]$ avec p un entier. Il vient alors, par produit, que :
   $$a_p \times 10^P \equiv a_p \times 1[9] \equiv a_p[9]$$
   Donc par somme :
   $$n = a_p \times 10^p + a_{p-1} \times 10^{p-1} + a_{p-2} \times 10^{p-2} + \cdots + a_2 \times 10^2 + a_1 \times 10^1 + a_0 \times 10^0$$
   $$\equiv a_p + a_{p-1} + a_{p-2} + \cdots + a_2 + a_1 + a_0[9]$$
   Ainsi n est divisible par 9 si, est seulement si, $n \equiv 0[9]$ or comme :
   $$n \equiv a_p + a_{p-1} + a_{p-2} + \cdots + a_2 + a_1 + a_0[9]$$
   alors n est divisible par 9 si, et seulement si :
   $$a_p + a_{p-1} + a_{p-2} + \cdots + a_2 + a_1 + a_0[9] \equiv 0[9]$$
   Nous venons donc de démontrer que n est divisble par 9 si, et seulement si, la somme de ses chiffres est un multiple de 9
2. Remarquons que : $10^0 \equiv 1[5],\ 10^1 \equiv 0[4]$. Soit $k \geq 1$ alors on a :
   $$10^k = 10^{k-1} \times 10^1 \equiv 10^{k-1} \times 0[5] \equiv 5$$
   Donc par produit il vient :
   $$a_0 10^0 \equiv a_0[5], a_k 10^k \equiv 0[5], k \geq 1$$
   On en déduit alors, par somme, que :
   $$n = a_p \times 10^p + a_{p-1} \times 10^{p-1} + a_{p-2} \times 10^{p-2} + \cdots + a_2 \times 10^2 + a_1 \times 10^1 + a_0 \times 10^0$$
   $$\equiv 0 + 0 + 0 + \cdots + 0 + 0 + a_0[5]$$
   Donc $n \equiv a_0[5]$ il vient alors que n est divisible par 5 si, et seulement si, son chiffre des unités est divisible par 5 c'est-à-dire si, et seulement si, $a_0 = 0$ ou $a_1 = 5$. Nous venons de montrer que n est divisible par 5 si, et seulement si, son dernier chiffre est 0 ou 5.

3. Nous allons raisonner de la même manière en raisonnant modulo 4 on a :
   $10^0 \equiv 1[4],\ 10^1 \equiv 2[4],\ 10^2 \equiv 0[4]$. Soit $k \geq 2$ alors on a :
   $$10^k = 10^{k-2} \times 10^2 \equiv 10^{k-2} \times 0[4] \equiv 0[4]$$
   Donc par produit il vient :
   $$a_0 10^0 \equiv a_0[4], a_1 10^1 \equiv a_1 \times 2[4], a_k 10^k \equiv 0[4], k \geq 2$$
   On en déduit alors, par somme, que :
   $$n = a_p \times 10^p + a_{p-1} \times 10^{p-1} + a_{p-2} \times 10^{p-2} + \cdots + a_2 \times 10^2 + a_1 \times 10^1 + a_0 \times 10^0$$
   $$\equiv 0 + 0 + 0 + \cdots + 0 + 2a_1 + a_0[4]$$
   Considérons le nombre m formé par les deux derniers chiffres de n. On a, par l'écriture décimale de n, que $m = \overline{a_1 a_0} = a_1 \times 10^1 + a_0 \times 10^0$. Il vient alors que :
   $$m \equiv 2a_1 + a_0[4] \equiv n[4]$$
   Comme $n \equiv m[4]$. n et m ont donc même reste de la division euclidienne par 4. On vient donc de montrer que n est divisible par 4 si, et seulement si m est divisible par 4. C'est-à-dire si, et seulement si, le nombre formé avec ses deux derniers chiffres est un multiple de 4.

4. La méthode pour 25 est identique que pour 4 :
   $10^0 \equiv 1[25],\ 10^1 \equiv 10[25],\ 10^2 \equiv 0[25]$. Soit $k \geq 2$ alors on a :
   $$10^k = 10^{k-2} \times 10^2 \equiv 10^{k-2} \times 0[25] \equiv 0[25]$$
   Donc par produit il vient :
   $$a_0 10^0 \equiv a_0[25], a_1 \times 10^1 \equiv a_1 \times 10[25], a_k 10^k \equiv 0[25], k \geq 2$$
   On en déduit alors, par somme, que :
   $$n = a_p \times 10^p + a_{p-1} \times 10^{p-1} + a_{p-2} \times 10^{p-2} + \cdots + a_2 \times 10^2 + a_1 \times 10^1 + a_0 \times 10^0$$
   $$\equiv 0 + 0 + 0 + \cdots + 0 + a_1 \times 10 + a_0[25]$$
   Considérons le nombre m formé par les deux derniers chiffres de n. On a, par l'écriture décimale de n, que $m = \overline{a_1 a_0} = a_1 \times 10^1 + a_0 \times 10^0$. Il vient alors que :
   $$m \equiv a_1 \times 10 + a_0[25] \equiv n[25]$$
   Comme $n \equiv m[4]$. n et m ont donc même reste de la division euclidienne par 25. On vient donc de montrer que n est divisible par 25 si, et seulement si m est divisible par 25. C'est-à-dire si, et seulement si, le nombre formé avec ses deux derniers chiffres est un multiple de 4.

5. Le critère de divisibilité par 11 est plus subtile. Il faut remarquer que :

$$10^0 \equiv 1[11], \qquad 10^1 \equiv 10[11] \equiv -1[11]$$

Donc pour tout k entier on en déduit que :

$$10^k \equiv (-1)^k[11]$$

Il vient alors, par produit :

$$a_k \times 10^k \equiv (-1)^k \times a_k[11]$$

Donc :

$$\begin{aligned} n = a_p \times 10^p + a_{p-1} \times 10^{p-1} + a_{p-2} \times 10^{p-2} + \cdots + a_2 \times 10^2 + a_1 \times 10^1 + a_0 \times 10^0 \\ \equiv (-1)^p \times a_p + (-1)^{p-1} \times a_{p-1} + (-1)^{p-2} \times a_{p-2} + \cdots + (-1)^2 \times a_2 + (-1)^1 \times a_1 \\ + (-1)^0 \times a_0[11] \end{aligned}$$

Remarquons que si k est pair alors

$$a_k \times 10^k \equiv (-1)^k \times a_k[11] \equiv 1 \times a_k[11] \equiv a_k[11]$$

Si k est impair alors :

$$a_k \times 10^k \equiv (-1)^k \times a_k[11] \equiv -1 \times a_k[11] \equiv -a_k[11]$$

Ainsi :

$$\begin{aligned} n \equiv (-1)^p \times a_p + (-1)^{p-1} \times a_{p-1} + (-1)^{p-2} \times a_{p-2} + \cdots + (-1)^2 \times a_2 + (-1)^1 \times a_1 \\ + (-1)^0 \times a_0[11] \equiv \sum_{k\ pair} a_k - \sum_{k\ impair} a_k\,[11] \end{aligned}$$

On additionne tous les chiffres de rang impair qui constituent notre première somme. On fait de même avec les chiffres de rang impair et l'on vient de montrer que n est congru à la différence de ces deux sommes modulo 11. Il vient alors que n est divisible par 11 si, et seulement si, la différence entre la somme des chiffres de rang pair et la somme des chiffres de rang impair est un multiple de 11.

- Pour savoir si 954 823 057 est un multiple de 11 il suffit d'utiliser les critères. En notant S_{paire} la somme des chiffres de rang pair et $S_{impaire}$ la somme des chiffres de rang impair nous avons : $S_{paire} = 7 + 0 + 2 + 4 + 9 = 22$ et $S_{impaire} = 5 + 3 + 8 + 5 = 21$ nous obtenons $S_{paire} - S_{impaire} = 22 - 21 = 1$ or 1 n'est pas un multiple de 11 donc le nombre 954 823 057 n'est pas un multiple de 11.
- Pour trouver un nombre à 10 chiffres qui soit un multiple de 11, utilisons le critère : choisissons au hasard des valeurs pour les chiffres de rang pair considérons, par exemple : $a_0 = 6, a_2 = 3, a_4 = 9, a_6 = 0, a_8 = 8$

On calcule la somme notée $S_{paire} = 6 + 3 + 9 + 0 + 8 = 26$

Il reste à choisir une somme des termes de rang impair tel que $S_{paire} - S_{impaire}$ soit un multiple de 11. Choisissons, par exemple comme valeur de $S_{impaire} = 15$ comme cela, il viendra que $S_{paire} - S_{impaire} = 26 - 15 = 11$. Remarquez que c'est un choix arbitraire, vous auriez pu prendre par exemple $S_{impaire} = 5$ de telle sorte que $S_{paire} - S_{impaire} = 22$ qui est aussi un multiple de 11.

Il faut maintenant choisir des valeurs pour les chiffres de rang impair tel que la somme donne 15. Par exemple : $a_1 = 2, a_3 = 1, a_5 = 0, a_7 = 7, a_9 = 5$.

On a bien que la somme $S_{impaire} = 2 + 1 + 0 + 7 + 5 = 15$. Comme toujours c'est un choix arbitraire, d'autres configurations étaient possibles. Formons le nombre construit avec ce choix : $n = \overline{a_9 a_8 a_7 \ldots a_2 a_1 a_0} = 5\ 870\ 091\ 326$ nous sommes alors certains que c'est un multiple de 11.

EXERCICE 01

1. Déterminez en utilisant les congruences les restes de la division euclidienne par 9 des nombres suivants : $2^q, q \in \{0,1,\dots,6\}$

2. Soit r le reste de la division euclidienne d'un entier n par 6. Montrez que $2^n \equiv 2^r [9]$

3. Déterminez alors en fonction des valeurs de n le reste de la division euclidienne de 2^n par 9.

EXERCICE 02

1. Déterminez les restes de la division euclidienne de 3^n par 7.

2. Déterminez les restes de la division euclidienne par 7 des nombres suivants :
   a. 1515^{2000}

   b. 1789^{9871}

EXERCICE 03

1. Démontrez que pour tout entier naturel k : $5^{4k} - 1$ est divisible par 13

2. Démontrez que pour tout entier naturel n : $5^{2n} - 14^n$ est divisible par 11

3. Déterminez le chiffre des unités de $3^{2022}, 227^{541}, 743^{2019}$. (Aide il faut déterminer le reste de la division euclidienne de $3^{2022}, 229^{541}, 743^{2019}$ par 10).

4. Déterminez le reste de la division euclidienne de 1234^{1235} par 4.

EXERCICE 04

Montrez que pour tout $n \in \mathbb{N}^*$:

1. $7 | 3^{3n} + 2 \times 5^{3n-1}$

2. $7 | 3^{4n+2} + 5^{2n+1}$

3. $9|2^{2n-1}+3n+4$

EXERCICE 05

1. Démontrez que pour tout entier n, $7|2^{3n}-1$. En déduire que $7|2^{3n+1}-2$ ainsi que $7|2^{3n+2}-4$

2. Déterminez les restes de la division par 7 des puissances de 2.

3. Soit p un entier naturel on considère $A_p = 2^p + 2^{2p} + 2^{3p}$
   a. En considérant la division euclidienne de p par 3, déterminer les entiers p tel que A_p soit un multiple de 7.

b. On considère $a = 584$ et $b = 4358$. Montrez que ces nombres sont de la forme A_p. En déduire s'ils sont divisibles par 7 en utilisant le résultat de la question 3.a

EXERCICE 06

1. Montrez que le produit de deux entiers naturels est pair, si et seulement si, l'un au moins des deux facteurs est pair.

2. En déduire l'ensemble des entiers naturels n tel que $9|8^n + 8n + 8$

EXERCICE 07

Le but de l'exercice est de montrer que $\sqrt[3]{3}$ est un nombre irrationnel.

1. Montrez que pour tout entier x, x^3 est congru à $-1,0$ ou 1 modulo 9. Déterminez l'ensemble des entiers x tel que $x^3 \equiv 0[3]$

2. Nous allons montrer que $\sqrt[3]{3}$ est un nombre irrationnel en raisonnant par l'absurde. Supposons que $\sqrt[3]{3}$ est rationnel c'est-à-dire qu'il existe (p, q) deux entiers naturels non nuls tel que $\frac{p}{q}$ soit irréductible et que $\frac{p}{q} = \sqrt[3]{3}$.

   a. Trouvez une relation entre p^3 et q^3

   b. En déduire que $p \equiv 0[3]$

   c. Montrez que $q \equiv 0[3]$

   d. Conclure

3. En vous inspirant du raisonnement montrez que $\sqrt{2}$ est irrationnel.

Vous pouvez maintenant faire et envoyer le devoir n°1