IREM 2011-2012
Atelier :

« initier à une démarche réflexive, historique et philosophique en cours de mathématiques au lycée. »

La classe : le groupe de 28 élèves « ABIBAC » d'une classe de seconde de 35 élèves.

Les objectifs en mathématiques :

- faire la distinction entre le sens commun des mots et leur sens technique en mathématiques ;
- débusquer les blocages et corriger les erreurs accumulées antérieurement ; exemples de blocages : simplification de fractions, racines carrées de sommes, notation « puissance », ...
- faire comprendre l'utilité des notations inventées pour les mathématiques.

Un constat : des blocages.

1. Penser un nombre représenté par une lettre :
   - Prouver que la somme de deux nombres inférieurs à 1 est un nombre inférieur à 2 :
     L'élève type, frais émoulu du collège unique, vous proposera comme preuve que par exemple 0,5 et 0,6 sont inférieurs à 1 et leur somme 1,1 est inférieurs à deux ; donc c'est vrai.
   - Réponse attendue (après apprentissage) :
     « Soient a et b deux nombres réels ; alors : si $a \leqslant 1$ et $b \leqslant 1$, alors $a+b \leqslant 2$ car on peut additionner membre à membre deux inégalités de même sens ».

2. La tentation de la linéarité :
   - $\sqrt{a+b}=\sqrt{a}+\sqrt{b}$; ce serait tellement pratique ! Le contre-exemple souvent présenté ($\sqrt{9+16} \neq \sqrt{9}+\sqrt{16}$) ne convainc pas vraiment ;
   - tant que $(a+b)^2=a^2+b^2$ est une réponse automatique de la part des ex-collégiens , on ne pourra pas faire comprendre que $\sqrt{a+b}$ n'est pas égal à $\sqrt{a}+\sqrt{b}$.
   - $\frac{1}{a+b} = \frac{1}{a}+\frac{1}{b}$: méconnaissance de ce qu'est vraiment « l'inverse » d'un nombre.

3. Des formules pas évidentes pour tout le monde :
   $a \times a^n = a^{n+1}$ n'est, de loin pas, un réflexe : cela demande une analyse complète (définition des puissances entières, commutativité de la multiplication, etc.)

4. L'égalité dans tous les sens :
   l'élève est souvent bloqué devant une question telle que « démontrer que $x^2+4x+1=(x+2)^2-3$ » ; il cherche à manipuler le membre de gauche pour aboutir au membre de droite, la lecture de l'égalité de droite à gauche n'étant pas spontanée.

Activités du premier semestre (août-décembre).

1. Sur les nombres : les notations usuelles ; quelques problèmes de Diophante;
2. Essai sur la genèse d'une notation : la congruence modulo un entier.
   Situation motivante : le cryptage affine (parfois appelé codage affine).
   Re-contextualisation : le problème des restes chinois.

Qu'est-ce qu'un nombre ?

Le nombre n'a au départ aucune existence propre ; on dit par exemple : un cheval, deux moutons, cinq œufs. L'invention des nombre a donc été motivée par le comptage.

C'est chez DIOPHANTE (+250) que l'on trouve pour la première fois des problèmes qui font intervenir des nombres autres qu'entiers :

1. Diviser un nombre donné en deux parties ayant une différence donnée.
2. Trouver quatre nombres tels que la somme des trois premiers excède le quatrième par un nombre donné.
3. Étant donnés deux nombres, trouver un troisième tel que les sommes des diverses paires multipliées par le troisième nombre correspondant fournissent trois nombres en progression arithmétique.
4. Trouver deux nombres tels que le carré de l'un ajouté à l'autre donne un carré.
5. Trouver deux nombres tels que leur somme et leur produit forment des nombres donnés.
6. Diviser une fraction donnée en trois parties telles que l'une quelconque d'entre elles moins le cube de leur somme donne un carré.

Solution de l'exercice 5 donnée par Diophante.
« Leur somme est 20 et leur produit 96. Supposons que la différence des deux nombres fasse $2d$. Leur somme fait 20, donc les deux nombres s'écrivent $10+d$ et $10-d$. On connaît leur produit : 96. On applique la règle de multiplication d'une soustraction par une addition : "plus par moins égale moins", d'où $100-d^2=96$. On a alors $d^2=4$, donc $d=2$. *(Pour Diophante la solution $d=-2$ n'existe pas).* Les nombres cherchés sont donc 10 + 2 et 10 – 2, c'est-à-dire 12 et 8. »

Exercices.

1. Résoudre l'exercice 5 par la même méthode avec une somme 100 et un produit 1600. Idem avec une somme 40 et un produit 76. Avec une somme 40 et un produit 300. Que se passe-t-il avec une somme 40 et un produit 398 ? Y a-t-il des cas où « ça ne marche pas » ?
2. Formaliser l'énoncé de l'exercice 5 en utilisant des « inconnues » x et y. *Se souvenir de la méthode de substitution et de l'identité* $x^2-20x+100=(x-10)^2$.
3. Chercher à résoudre les autres exercices proposés par Diophante (pour le nombre donné, choisir un exemple, comme l'a fait Diophante pour l'exercice 5 ; varier les exemples). Les solutions ne sont pas nécessairement des nombres entiers.

Découverte de nombres congrus modulo un entier.

Prérequis : la division euclidienne ; occasion de programmer la division euclidienne sur TI82 ; sur tableur, utilisation de la commande =MOD(dividende ; diviseur) pour afficher directement le reste.

Cryptage affine et décryptage.

Bon à savoir.

- Sur un tableur (Microsoft Excel ou Open Office Calc), chaque lettre de l'alphabet possède un code chiffré accessible par la commande =CODE(« Lettre »).
- Les majuscules de A à Z sont codées de 65 à 90 ; par exemple, =CODE(« B ») renvoie le nombre 66.
- Pour coder les majuscules de A à Z de 0 à 26 comme dans le cryptage affine, il suffit donc de faire =CODE(« Lettre ») – 65.
- NB.- Si la lettre à coder se trouve dans la cellule E13 par exemple, la commande =CODE(E13) renvoie le code de la lettre.
- Pour obtenir le code de la lettre cryptée, on multiplie le code de la lettre par le coefficient de la fonction, on ajoute le nombre voulu et on demande le reste de la division par 26 (rappel : ce reste est donné par la commande =MOD(nombre;26)).
- Inversement, la commande =CAR(chiffre) redonne la lettre codée. Par exemple, la commande =CAR(70) renvoie la lettre F.
- Si on a codé les lettres de 0 à 25, il faut donc utiliser la commande =CAR(x+65), qui renvoie la lettre majuscule correspondante.

Exercice 1.

On effectue le cryptage par la fonction « multiplier par 5 et ajouter 3 » ; crypter de cette façon vos nom et prénom. Par exemple, vérifier que FRANCOIS sera crypté en CKDQNVRP (sauf erreur).

Exercice 2.

Peut-on faire un cryptage efficace avec la fonction « multiplier par 4 et ajouter 3 » ? Justifier la réponse.

Exercice 3.

Parmi les nombres de 1 à 26, trouver ceux qui permettent de faire un cryptage efficace et ceux qui ne le permettent pas. Interpréter le résultat.

Exercice 4.

Pour décrypter un message obtenu par « multiplier par 5 puis ajouter 3 et calculer le reste modulo 26 », on peut faire « soustraire 3, puis multiplier par 21 et calculer le reste modulo 26 » ;

a) expliquer pourquoi la multiplication par 21 permet de faire ce décryptage ;
b) tester la méthode sur les noms cryptés à l'exercice 1.

Exercice 5.

Un message est crypté par la fonction « multiplier par 9 et ajouter 4 » ; trouver le coefficient qui permet de faire le décryptage.

Exercice 6.

Trouver les coefficients de décryptage pour tous les nombres de l'exercice 3 qui permettent de faire un cryptage efficace.

Exploitation des résultats.

Rappel : les lettres de l'alphabet étant codées de 0 à 25, un **cryptage** affine consiste à multiplier le code de chaque lettre par un entier naturel *a* qui ne soit ni pair, ni multiple de 13 (coefficient de cryptage), à ajouter un nombre *b*, et à calculer le reste modulo 26 ; ce reste, *y*, est le code de la lettre cryptée.

Décryptage : on prend le code *y* de chaque lettre du message crypté par la fonction $x \to a\,x+b$, on soustrait *b*, on multiplie par un coefficient de décryptage *a′* dépendant de *a,* on calcule le reste modulo 26 et on retrouve ainsi le message d'origine.

Tableau des coefficients de décryptage :

a	1	3	5	7	9	11	15	17	19	21	23	25
a′	1	9	21	15	3	19	7	23	11	5	17	25

Exercice 1.

a) Calculer les restes modulo 26 des produits *aa′* du tableau précédent. Que peut-on dire ?
b) Essayer de justifier par un calcul le bien-fondé de la règle de décryptage énoncée ci-dessus.

Exercice 2.

a) Donner l'ensemble E des dix premiers entiers naturels qui ont pour reste 1 dans la division euclidienne par 26.
b) Choisir au hasard deux nombres *x* et y de l'ensemble E et calculer leur différence ; répéter l'opération une dizaine de fois ; que peut-on dire des résultats obtenus ?

Information *:*
Vocabulaire proposé en 1801 par le mathématicien allemand Karl Friedrich GAUSS, dans le traité « Disquisitiones arithmeticae » (recherches arithmétiques) qu'il a publié cette année-là :

si la différence de deux nombres a et b est un multiple du nombre c,
on dit que a et b sont congrus modulo c

et il a proposé de condenser la phrase « a et b sont congrus modulo c » sous la forme $a \equiv b \ [c]$.

Questions.

1. Pourquoi peut-on dire indifféremment *« a et b sont congrus modulo c »* ou *« b et a sont congrus modulo c »* ?
2. Peut-on dire qu'un nombre *a est congru à lui-même modulo c* ?
3. Citer plusieurs nombres congrus à 105 modulo 26 ?

Exercice 3.

a) Quels sont les restes modulo 7 des nombres 10 ; 14 ; 25 ; 29 ; 30 ?
b) Écrire tous les produits possibles de ces nombres pris deux par deux et calculer les restes modulo 7 des produits obtenus. Commenter les résultats et conjecturer une règle de calcul.
c) Calculer les restes modulo 7 des nombres $2^5 ; 2^8 ; 2^{10} ; 2^{13}$. Pouvait-on prévoir les deux derniers résultats, connaissant les deux premiers ?
d) Prédire le reste modulo 7 du nombre 2^{35}. Vérifier en donnant l'écriture décimale de ce nombre et la partie entière du quotient par 7 de ce nombre.
e) Prédire alors le reste modulo 7 des nombres 2^{2011} et 2^{2012}.

Remarque : on peut présenter les résultats de la question b) de cet exercice 3 sous la forme d'un tableau carré à cinq lignes et cinq colonnes.

Ré-investissement : **Usage et utilité des congruences.**

Congruence et division.

La division euclidienne de a par b peut s'écrire $a=bq+r$, le reste r étant un nombre entier naturel strictement inférieur au diviseur b.
Comme $a-r=bq$ on peut dire, selon les mots inventés par K.F. GAUSS, que a et r sont congrus modulo b ; en fait, parmi tous les entiers congrus à a modulo b, r est le seul qui soit positif et strictement inférieur à b.

Congruence et égalité.

On connaît les règles de l'égalité : tout nombre est égal à lui-même ; si un nombre a est égal à un nombre b, alors b est égal à a ; si a est égal à b et que b est égal à c, alors a est égal à c ; on peut additionner un même nombre aux deux membres d'une égalité ; on peut multiplier par un même nombre les deux membres d'une égalité, etc.
Pour les congruences on a des règles tout à fait analogues :

1. $\forall a\in\mathbb{Z},\ a\equiv a\ [b]$
2. $a\equiv a'\ [b] \Leftrightarrow a'\equiv a\ [b]$
3. Si $a\equiv a'\ [b]$ et $a'\equiv a''\ [b]$ alors $a\equiv a''\ [b]$
4. Si $a\equiv a'\ [b]$ alors $a+c\equiv a'+c\ [b]$
5. Si $a\equiv a'\ [b]$ alors $ac\equiv a'c\ [b]$

Exercice.

1. Démontrer les propriétés 3., 4. et 5. ci-dessus.
2. Démontrer que l'on peut additionner membre à membre deux congruences modulo b.
3. Démontrer que l'on peut multiplier membre à membre deux congruences modulo b.
4. Application : on s'intéresse aux restes modulo 5 de tous les produits possibles de deux entiers naturels, aussi bien $mod\,(3\times 4\,;5)$ que $mod\,(58\times 122\,;5)$; quels sont les restes $mod\,(a\times b\,;5)$ qu'il suffit de connaître pour trouver facilement tous les autres ?
5. Autre application : la preuve par 9 (un savoir-faire devenu obsolète depuis l'apparition sur le marché, dans les années 1970, des calculatrices de poche).
6. Autre application : la justification des critères de divisibilité par 3, par 9, par 11, par 4, par 5, par 8, et, un peu plus complexe, par 7.

Le problème des restes chinois.
Chronologie :

- 1247 : publication du mathématicien Qin Jiushao ;
- 3-ième siècle : dans le livre de Sun Zi, le *Sunzi suanjing* : « Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ? »
  Remarque : il existe d'autres formulations de ce problème.

Exercices.
Résoudre les « équations » suivantes :

- facile : $x \equiv 3\ [5]$
- à peine moins facile : $2x \equiv 4\ [7]$
- un peu moins facile : $2x \equiv 5\ [7]$
- plus difficile : $3x \equiv 5\ [13]$; $x^2 \equiv 4\ [7]$; $x^2 \equiv 5\ [7]$.

Annexe : informations concernant le problème des restes chinois.

La forme originale du théorème, contenue dans un livre du mathématicien chinois Qin Jiushao publié en 1247, est un résultat concernant les systèmes de congruences.

Selon Zachariou, le théorème des restes chinois aurait été découvert antérieurement par les Grecs[1]. Mais on trouve trace d'un problème analogue dans le livre de Sun Zi, le *Sunzi suanjing* datant du III^{e} siècle :

> *Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il* ***reste*** *deux soldats, rangés par 5 colonnes, il* ***reste*** *trois soldats et, rangés par 7 colonnes, il* ***reste*** *deux soldats ?*

On peut penser que les Chinois, férus de calculs astronomiques, puissent être intéressés par des concordances de calendrier et qu'ils aient été amenés très tôt à s'intéresser à des questions du type :

> *Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver ?*

Si la question se pose alors qu'il reste 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune, la question se traduit par :

> *Existe-t-il un entier x tel que le reste de la division de x par 365 donne 6 et le reste de la division de x par 28 donne 3 ?*

La résolution proposée par Sun Zi pour le problème des soldats est la suivante :

> *Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.*

Mais la solution n'explique qu'imparfaitement la méthode utilisée.

Enfin, il serait dommage de ne pas présenter ce problème concernant des pirates et un trésor, très fréquemment cité pour illustrer le théorème des restes chinois :

> *Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?*

À suivre : activités du second semestre (janvier-juin)