Un énoncé de Mersenne, une solution de Fermat

Martine Bühler(*)

L'arithmétique est de retour dans les programmes de mathématiques du secondaire, en particulier pour la spécialité « mathématiques » en terminale scientifique. Les documents d'accompagnement des programmes présentent des activités possibles de résolution d'équations diophantiennes à l'aide de congruences :

> *On pourra commencer par étudier quelques équations dont le traitement est simple :*
> • $2x^2 - y^2 = 5$. *En raisonnant modulo 5, on montre qu'il n'y a pas de solution.*
> • $7x^2 + 2y^2 = 3$. *En raisonnant modulo 7, on montre qu'il n'y a pas de solution.*
> *(Document d'accompagnement des programmes pour la classe de terminale scientifique p. 53)*

Or, en matière de factorisation des grands nombres, une idée fructueuse, reposant sur un calcul de congruences, a été développée par Fermat en 1643, en réponse à un défi que le Père Mersenne lui avait lancé. Il m'a paru intéressant d'en tirer un problème pour mes élèves spécialistes de Terminale S, problème qui pouvait leur montrer comment les congruences permettent de résoudre effectivement des équations diophantiennes. De plus, nos élèves savent que la factorisation des grands nombres est un problème d'actualité puisqu'ils étudient un peu de cryptographie et en particulier le système R.S.A. ; or les idées à l'origine de certaines méthodes actuelles de factorisation viennent de Fermat, à une époque où la factorisation relevait plutôt du défi intellectuel que de l'utilité pratique. C'est aussi l'occasion de faire lire aux élèves un extrait d'une lettre de Fermat à Mersenne, et de leur parler du XVII^{e} siècle et de l'histoire des mathématiques.

En liaison avec ces idées les frères Carissan avaient construit vers 1920 une machine à congruences permettant de résoudre des équations diophantiennes, et en particulier de factoriser des grands nombres. Pour en savoir plus sur la machine de Carissan on pourra lire avec intérêt un article sur ce sujet, paru dans le bulletin nº 446, dans le dossier « Calcul » et dans le nº 17 de *Mnémosyme* (édité par l'IREM de Paris VII). On pourra aussi lire un article de François Morain paru dans le numéro de Janvier 1998 de *Pour la Science*.

Devoir à la maison

Cet énoncé pourrait paraître ambitieux si on le proposait tel quel. Mais ma pratique habituelle est de donner de tels devoirs quinze jours l'avance et de faire une petite séance de « Questions orales au gouvernement » (c'est le mercredi…) où nous faisons le point sur les questions qui se posent, sur les difficultés rencontrées dans une première approche. La seconde semaine étant alors consacrée à la rédaction structurée et raisonnée d'une solution individuelle.

(*) Lycée Flora Tristan 93 Noisy-Le-Grand. Groupe M. : A.T.H.(Mathématiques : Approche par des Textes Historiques), I.R.E.M. Paris VII.

Pour ce problème quels ont été les endroits « critiques » ? Dans la première partie certains n'ont pas eu l'idée de tirer a et b en fonction de p et q et, surtout, beaucoup n'ont pas su comment démarrer la démonstration de l'équivalence entre « a et b premiers entre eux » et « p et q premiers entre eux ». Dans la seconde partie les questions 1°,b) et 1°,c) ont nécessité des éclaircissements.

En 1643, Fermat répond à Mersenne qui lui a lancé le défi de factoriser 100 895 598 169. Il trouve cette factorisation (898 423 × 112 303), mais indique dans une lettre ultérieure une méthode générale. C'est cette lettre que nous allons lire ensemble.

I. DIFFÉRENCE DE DEUX CARRÉS ET FACTORISATION

Soit N un nombre entier naturel impair.

1°) On suppose que $N = a^2 - b^2$ avec a et b entiers naturels. Déterminer deux entiers naturels p et q tels que $N = pq$.

2°) On suppose que $N = pq$ avec p et q entiers naturels et $p > q$.

a) Quelle est la parité de p et q ?

b) Montrer qu'il existe deux entiers naturels a et b tels que $N = a^2 - b^2$.

c) Démontrer que :
« p et q sont premiers entre eux » équivaut à « a et b sont premiers entre eux ».

3°) Fermat utilise les définitions suivantes :
Les nombres compositeurs sont les facteurs d'un nombre composé.
Ex : 45 = 9 × 5 ; 9 et 5 sont les compositeurs du nombre composé 45.
Les parties d'un nombre sont ses diviseurs, c'est-à-dire les compositeurs.

a) Lire le texte lignes 1 à 14 (attention, à la ligne 2, traduire « ou » par « c'est-à-dire »).

b) Quelle est la phrase du texte de Fermat correspondant aux questions 1°) et 2°) b) ?

c) Quelle est la phrase du texte de Fermat correspondant à la question 2°) c) ?

d) Que se passe-t-il si N est un carré ?

e) Lire les lignes 15 et 16 et les traduire avec des notations algébriques.

II. FACTORISATION DE GRANDS NOMBRES

Le but de cette partie est la factorisation de N = 250 507. Cela revient à déterminer deux entiers naturels x et y tels que $x^2 - y^2 = N$ (équation notée (E) dans la suite). Une telle équation s'appelle « équation diophantienne ».

1°) Travail modulo 7.

a) Compléter le tableau suivant par le reste de X^2 modulo 7 suivant les valeurs de X.

X	0	1	2	3	4	5	6
X^2				2			

Le nombre $7 \times 113 + 3$ peut-il être un carré ? Pourquoi ? (Il est impératif d'utiliser le tableau précédent et son cerveau, mais surtout pas la calculatrice !)(1).

b) On cherche à résoudre $x^2 - y^2 = 250\,507$, c'est-à-dire $x^2 - 250\,507 = y^2$. Donc, si le nombre entier x est solution, alors le nombre $x^2 - 250\,507$ doit être un carré. À l'aide du tableau précédent, déterminer les valeurs possibles modulo 7 de $x^2 - 250\,507$. En déduire les valeurs possibles modulo 7 de x^2.

c) Mais x^2 doit être un carré, donc le même tableau permet de restreindre encore les valeurs possibles de x^2 modulo 7. Le faire, puis en déduire les valeurs possibles de x modulo 7. Le nombre 778 peut-il être solution de l'équation (E) ?

2°) Faire un travail analogue modulo 9.

3°) Faire un travail analogue modulo 15.

4°) Résolution de l'équation (E) : $x^2 - y^2 = 250\,507$.

a) Justifier : si x est solution de (E), alors $x \geq \sqrt{250\,507}$. Quelle est la plus petite valeur possible de x ?

b) Soit $x_0 = 501$. Calculer les restes de x_0 modulo 7, modulo 9 et modulo 15. Le nombre x_0 est-il solution de l'équation (E) ?

c) Remplir le tableau suivant jusqu'à trouver une valeur de x compatible avec les conditions trouvées dans les questions 1°), 2°), 3°).

x	501	502	503	504	…
mod 7					
mod 9					
mod 15					

Est-on sûr que la valeur ainsi trouvée est solution de l'équation (E) ?
Vérifier que cette valeur est bien une solution et en déduire une factorisation de 250 507.

(1) Les nombres 0, 1, 2, 4 s'appellent résidus quadratiques modulo 7.

Extrait de : Fermat *Œuvres* éd. Tannery et Henry, tome II, 1894, Lettre de 1643, p. 257-258.

LVII.

FRAGMENT D'UNE LETTRE DE FERMAT < 1613 >

Tout nombre impair non quarré est différent d'un quarré par un quarré, ou est la différence de deux quarrés, autant de fois qu'il est composé de deux nombres, et, si les quarrés sont premiers entre eux, les nombres compositeurs le sont aussi. Mais si les quarrés ont entre eux un commun diviseur, le nombre en question sera aussi divisible par le même commun diviseur, et les nombres compositeurs seront divisibles par le côté de ce commun diviseur.

Par exemple : 45 est composé de 5 et de 9, de 3 et de 15, de 1 et de 45. Partant, il sera trois fois la différence de deux quarrés : savoir de 4 et de 49, qui sont premiers entre eux, comme aussi sont les compositeurs correspondants 5 et 9 ; plus, de 36 et de 81, qui ont 9 pour commun diviseur, et les compositeurs correspondants, 3 et 15, ont le côté de 9, savoir 3, pour commun diviseur ; enfin 45 est la différence de 484 et 529, qui ont 1 et 45 pour compositeurs correspondants.

II est fort aisé de trouver les quarrés satisfaisants, quand on a le nombre et ses parties, et d'avoir les parties lorsqu'on a les quarrés.