DANS NOS CLASSES

Thèmes abordés : arithmétique
Niveau : Terminale S
Outils nécessaires : nombres premiers puis, pour un prolongement en classe, congruences
Texte étudié : une lettre de Fermat à Mersenne (1643)

Martine Bühler

Le problème des pages suivantes est l'aboutissement d'un travail effectué en 2000 avec des participants à un stage d'histoire des mathématiques à l'I.R.E.M. Paris VII ; il a été donné en devoir à la maison à des élèves de terminale scientifique, spécialité mathématiques. Il permet d'aborder le thème de la factorisation des grands nombres[1] à partir d'une lettre de Fermat à Mersenne de 1643.

La première partie du problème est assez aisée ; cependant, la deuxième partie, qui s'attaque à un algorithme de factorisation indiqué par Fermat, a semblé difficile aux élèves et a nécessité une correction soignée en classe. La troisième partie traite de longueur d'algorithme et introduit un début de réflexion sur les nombres carrés, qui s'appuie sur une remarque de Fermat. Lors de la correction en classe, nous avons travaillé sur les congruences pour reconnaître si un nombre peut être un carré ou non, puis nous avons visionné un film sur la machine à congruences des frères Carissan[1].

[1] Voir l'étude *Factorisation de grands nombres* dans ce mêmes numéro, page 17

Devoir à la maison donné en Terminale S (spécialité maths)

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

I.DIFFERENCE DE DEUX CARRES 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 = 9x5 ; 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.ALGORITHME DE FACTORISATION

1°) Quelles sont les questions que pose Fermat dans les lignes 20-21-22 ?

Dans la suite on pose N = 2 027 651 281.

2°) Pour résoudre son problème, Fermat cherche deux nombres a et b tel que a^2-N est un carré.

a) Pourquoi ?

b) Quelle est la valeur minimale de a pour que a^2-N soit un carré ?

c) Si vous savez utiliser un tableur, rechercher à l'aide du tableur le plus petit entier a solution du problème ; vous joindrez à la copie la feuille de calcul du tableur et un tableau indiquant comment vous avez rempli les cellules.

d) Ecrire un algorithme permettant de programmer votre calculatrice pour obtenir la plus petite solution a. Donner a.

3°) Fermat, ne disposant pas d'un ordinateur, faisait ses calculs à la main et a préféré, avant de calculer, améliorer l'algorithme ; il emploie donc une procédure de calcul équivalente à la vôtre, mais évitant les élévations au carré. Le but de cette question est de comprendre son algorithme.

Dans la suite $X_0=E(\sqrt{N})$ (partie entière de $\sqrt{N}$)= 45 029, R=40 440 et $A_0=X_0+1$.

a) Lire les lignes 23-24(jusqu'à « de reste ») et écrire une égalité liant N, X_0 et R.

b) Pourquoi s'intéresse-t-on à A_0 ?

c) On pose : $U_0=2X_0+1$ et $B_0=U_0-R$. Sans utiliser les valeurs numériques, montrer que $B_0 = A_0^2 - N$.

La question est donc de savoir si B_0 est un carré. Calculer les valeurs numériques de U_0 et B_0 répondre à la question ; lire les lignes 23 à26 jusqu'à « ne finit par 19 ».

4°) On pose, pour p entier naturel, $A_{p+1} = A_p + 1$; $U_{p+1} = U_p + 2$; $B_{p+1} = B_p + U_{p+1}$.

a) Vérifier, sans utiliser les valeurs numériques, que $A_1^2 - N = B_1$.

Quelle question se pose-t-on sur B_1 ? Calculer B_1 et répondre à la question.

b) Montrer : pour p entier naturel, $U_{p+1} = 2 A_p + 1$ et $A_p^2 - N = B_p$.

Lire les lignes 26 à 36.

5°) a) A quel moment Fermat arrête-t-il ses calculs ?

b) Pour p entier naturel, exprimer A_p à l'aide de X_0 et p, et exprimer p à l'aide de U_p et U_1.

c) Quelle est la valeur numérique B_{p_0} à laquelle Fermat arrête ses calculs ? Quelle est la valeur numérique U_{p_0} correspondante (voir les lignes 37 à 39) ? Calculer p_0, puis A_{p_0}.

d) Exprimer N comme différence de deux carrés, puis comme un produit de facteurs.

e) Lire la fin du texte.

III. COMPLEMENTS

1°) Utiliser un tableur pour programmer l'algorithme de Fermat.

2°) Ecrire un algorithme permettant de programmer votre calculatrice pour effectuer les calculs de Fermat.

3°) Expliquer les phrases suivantes du texte :

« reste 49 619, lequel n'est pas quarré, parce que aucun quarré ne finit par 19 ».

« car les carrés ne peuvent souffrir les finales qu'elles ont ».

4°) Lorsque $N = a^2 - b^2$,quel est le nombre d'étapes nécessaires dans l'algorithme de Fermat pour trouver a ?

Quel est le nombre d'étapes nécessaires pour factoriser 100 895 598 169 ? Qu'en pensez-vous ?

5°) Si N est premier, la seule factorisation possible de N est N = N x 1. Quelle est alors la valeur correspondante de a ? Quel est le nombre d'étapes nécessaires dans l'algorithme de Fermat pour aboutir ? L'algorithme de Fermat peut ainsi servir de test de primalité ; je l'appellerai « test historique » bien que ni Fermat, ni ses successeurs ne l'aient utilisé comme test de primalité. Ce « test historique » est-il plus efficace que votre « test habituel » ?

Extrait des *Œuvres*, éd. Tannery et Henry, tome II, 1894, Lettre de 1643, pp. 257-258.

LVII.

FRAGMENT D'UNE LETTRE DE FERMAT (²).

< 1643 >

(A, f° 74.)

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.

Il 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.

Cette proposition se trouve quasi tout par tout. On en pourrait quasi autant dire des pairements pairs, excepté 4, avec quelque petite modification.

Cela posé, qu'un nombre me soit donné, par exemple 2 027 651 281, on demande s'il est premier ou composé, et de quels nombres il est composé, au cas qu'il le soit.

J'extrais la racine, pour connoître le moindre des dits nombres, et trouve 45 029 avec 40 440 de reste, lequel j'ôte du double plus 1 de la racine trouvée, savoir de 90 059 : reste 49 619, lequel n'est pas quarré, parce que aucun quarré ne finit par 19, et partant je lui ajoute 90 061, savoir 2 plus que 90 059 qui est le double plus 1 de la racine 45 029. Et parce que la somme 139 680 n'est pas encore quarrée, comme on le voit par les finales, je lui ajoute encore le même nombre augmenté de 2, savoir 90 063, et je continue ainsi d'ajouter tant que la somme soit un quarré, comme on peut voir ici (¹). Ce qui n'arrive qu'à 1 040 400, qui est quarré de 1020, et partant le nombre donné est composé; car il est aisé, par l'inspection des dites sommes, de voir qu'il n'y a aucune qui soit nombre quarré que la dernière, car les quarrés ne peuvent souffrir les finales qu'elles ont, si ce n'est 499 944 qui néanmoins n'est pas quarré.

Pour savoir maintenant les nombres qui composent 2 027 651 281, j'ôte le nombre que j'ai premièrement ajouté, savoir 90 061, du dernier ajouté 90 081. Il reste 20, à la moitié duquel plus 2, savoir à 12, j'ajoute la racine premièrement trouvée 45 029. La somme est 45 041, auquel nombre ajoutant et ôtant 1020, racine de la dernière somme 1 040 400, on aura 46 061 et 44 021, qui sont les deux nombres plus prochains qui composent 2 027 651 281. Ce sont aussi les seuls, pource que l'un et l'autre sont premiers.

Si l'on alloit par la voie ordinaire, pour trouver la composition d'un tel nombre, au lieu de onze additions, il eût fallu diviser par tous les nombres depuis 7 jusqu'à 44 021.

Plusieurs abrégés se peuvent trouver, comme lorsqu'on ne fait qu'une addition au lieu de dix, aux endroits où les sommes ont leurs finales quarrées, quand les compositeurs sont beaucoup éloignés l'un de l'autre.

LVI.

FERMAT A MERSENNE (1).

MARDI 7 AVRIL 1643.

(A, f^os 19-20; B, f° 22 v°.)

4. Vous me demandiez donc quelle proportion a le nombre, qui se produit des nombres suivants, avec ses parties aliquotes :

214 748 364 800 000, 11, 19, 43, 61, 83, 169, 223, 331, 379, 601, 757, 961, 1201, 7019, 823 543, 616 318 177, 6561, 100 895 598 169.

Vous me demandiez ensuite si ce dernier nombre est premier ou non, et une méthode pour découvrir dans l'espace d'un jour s'il est premier ou composé.

A la première question, je vous réponds que le nombre qui se fait de tous les nombres précédents multipliés entre eux, est sous-quintuple de ses parties.

A la seconde question, je vous réponds que le dernier de ces nombres est composé et se fait du produit de ces deux :

$$898\,423 \quad \text{et} \quad 112\,303^3,$$

qui sont premiers (1).

Je suis toujours, mon Révérend Père,

Votre très humble et très affectionné serviteur,

FERMAT.

A Toulouse, ce 7 avril 1643.

Paris chez Petit rue S. Jacques pres les Mathurins