En mathématiques :

que cherche-t-on ? comment cherche-t-on ?

Daniel PERRIN

Présentation

Bonjour, je suis professeur de mathématiques à l'université Paris-Sud à Orsay et, comme presque tous les enseignants de l'université, je suis aussi chercheur. Mon objectif, aujourd'hui, est d'essayer de montrer, d'abord, que les mathématiques sont utiles dans presque toutes les activités humaines, ensuite, qu'il y a beaucoup de problèmes de mathématiques dont on ne connaît pas la solution. C'est à ces problèmes que s'attaquent les chercheurs et j'essaierai de vous montrer comment ils font, en vous faisant jouer le rôle de l'apprenti chercheur. Je vous laisserai d'ailleurs une petite collection de problèmes-défis pour vous exercer. Je répondrai enfin à vos questions.

1 Les mathématiques c'est utile

1.1 Les mathématiques sont utiles actuellement

Comme tous les collégiens de ce pays, vous apprenez des mathématiques, mais beaucoup d'entre vous se demandent : à quoi ça sert ? La réponse est à la fois facile : les maths ça sert partout, et difficile, car il n'est pas évident de donner des exemples qui se situent à votre niveau. Bien sûr vous savez que la maîtrise des opérations est utile pour faire ses courses et qu'il faut savoir calculer des longueurs ou des aires lorsqu'on bricole.

Certes, et tout cela utilise des mathématiques, mais assez peu. En fait, des mathématiques beaucoup plus élaborées sont présentes, de manière cachée, dans la vie de tous les jours, qu'il s'agisse des prévisions météo, des tests ADN, ou des satellites. Dans le moindre des objets de la vie courante, il y a des mathématiques. Lorsque, dans un magasin, le lecteur optique n'arrive pas à lire un code-barre et que la caissière doit le taper, les derniers chiffres sont ce qu'on appelle une clé, la machine les trouve à partir des autres par un petit calcul, et cela permet de détecter si la caissière se trompe. C'est aussi le cas pour les numéros de sécurité sociale.

1.2 Les mathématiques seront utiles demain : l'exemple des nombres premiers

Certains domaines des mathématiques semblent ne pas avoir d'applications. Ainsi, si l'on m'avait demandé, dans les années 1970, à quoi servaient les nombres premiers dans la vie courante, j'aurais répondu sans hésiter, à rien, et j'aurais peut-être ajouté comme un de mes collègues, qu'en tout cas ils ne servaient pas à faire la bombe atomique. En fait, j'aurais dit une bêtise, puisque les nombres premiers, avec le code RSA, jouent maintenant un rôle de premier plan dans tous les secteurs de la communication, de la finance, etc. et que parmi leurs utilisateurs se trouvent justement ... les militaires.

1.2.1 La cryptographie

La cryptographie (du grec crypto, caché et graphie, écrire) est la science des messages secrets. Elle remonte à l'antiquité et Jules César l'a employée pour coder ses messages. Il utilisait le système le plus simple, celui des alphabets décalés d'un ou plusieurs crans (où l'on remplace, par exemple, A par B, B par C, etc). Ainsi peut-on penser qu'il envoya au sénat, après sa victoire sur Pharnace, le message suivant : TCLG TGBG TGAG.

Bien entendu des méthodes beaucoup plus sophistiquées ont été inventées depuis. Le plus souvent ces méthodes utilisent le principe suivant. On code les lettres de l'alphabet de A à Z par les nombres de 1 à 26. On traduit le message en chiffres. Par exemple si le message est A L'AIDE il devient 1 12 1 9 4 5. Ensuite on permute les nombres de 1 à 26 selon une certaine règle. On obtient par exemple ici 25 14 25 17 22 21 avec une règle très simple que je vous laisse deviner. On retraduit alors le message en lettres et on a YNYQVU. Le défaut de ce genre de méthodes c'est qu'elles ne résistent pas au décryptage par analyse de fréquences qui consiste à identifier quelles sont les lettres qui interviennent le plus (voir la nouvelle "le scarabée d'or" d'Edgar Poe). C'est d'ailleurs ainsi, dit-on, que la reine d'Écosse Marie Stuart a péri. En effet, elle était prisonnière de la reine d'Angleterre Elisabeth et elle communiquait avec ses partisans en envoyant des messages codés. Mais ceux-ci ont été interceptés par les anglais et décodés par cette méthode et la pauvre Marie, convaincue de complot contre la reine, a été décapitée (1587).

Par cette méthode, vous devez réussir à déchiffrer le message ci-dessous :

SALCFCFVHLCNEANVHHPLGNZIPUUANAKNRNHHLBNCFVH
NYOANEGLYHKNZKVSOANHUNARNGNHZLHHNVAHGNZFGNH
HNZANOHUALYZLPHKNHNHMPFYHYFYOMKVHTVLSPNYHN

ONYPAUNKPZPOLOPFYH
en sachant qu'en français les lettres statistiquement les plus fréquentes sont, dans l'ordre, E, puis S et A, puis R, I, N et T, puis U, puis O et L, etc.

1.2.2 Le code RSA

La méthode RSA dont nous allons parler a été inventée en 1978 par Rivest, Shamir et Adleman. Je ne peux pas vous en expliquer exactement le principe, mais, si vous allez en terminale S et que vous faites la spécialité maths, vous saurez exactement de quoi il retourne. Cette méthode repose sur les nombres premiers. Vous savez sans doute qu'un nombre premier est un nombre qui n'a pas d'autres diviseurs que lui-même et 1. Dans l'ordre, on trouve successivement $2, 3, 5, 7, 11, 13, 17, 19$, etc. Leur intérêt, c'est que tous les autres entiers s'écrivent comme produits de nombres premiers (c'est presque évident : si n n'est pas premier, il est produit de deux nombres $n = pq$. S'ils sont premiers on a gagné, sinon, on recommence).

Comment fonctionne alors le code RSA ?

Imaginons un espion E (Ernesto), loin de son pays et de son chef C (Carlos). Il doit transmettre des messages secrets à C. Pour cela, il a besoin d'une clé pour coder ses messages. Le chef C calcule deux grands nombres premiers p et q, il calcule ensuite le produit pq et c'est ce nombre qui est la clé de codage et qu'il transmet à E (mais il garde secrets les deux nombres p et q). Attention, de nos jours, avec Internet et tous les satellites qui nous tournent autour, on n'est pas sûr du tout que les ennemis n'écoutent pas les messages transmis. Peu importe, car la clé pq est **publique**. Pour coder le message, E n'a besoin que de la clé pq, en revanche, pour le décoder, le chef C a besoin des deux nombres p et q. Le principe qui fonde le code RSA c'est qu'il est beaucoup plus facile de fabriquer de grands nombres premiers p et q (et de calculer pq) que de faire l'opération inverse qui consiste à décomposer le nombre pq en le produit de ses facteurs premiers.

1.2.3 Trouver de grands nombres premiers

On sait depuis Euclide qu'il y a une infinité de nombres premiers mais il n'est pas si facile d'en donner explicitement de très grands. Pierre de Fermat (1601-1665) avait cru trouver une formule donnant à coup sûr des nombres premiers. Il prétendait que, pour tout entier n, le nombre $F_n = 2^{2^n} + 1$ était premier. C'est effectivement le cas pour $n = 0, 1, 2, 3, 4$ qui correspondent respectivement aux nombres premiers $3, 5, 17, 257, 65537$, mais ce n'est pas vrai pour F_5 comme l'a montré Euler.

(On peut faire le calcul à la main jusqu'à 257*. Pour voir que* 65537 *est*

premier, mais que $2^{32}+1$, $2^{64}+1$ *et* $2^{128}+1$ *ne le sont pas on peut utiliser la fonction EstPrem de la calculatrice TI Voyage 200 qui répond presque instantanément. La calculatrice factorise facilement* $2^{32}+1$ *et* $2^{64}+1$ *(mais cela prend plus de temps). En revanche, pour le suivant, elle ne donne rien en un quart d'heure*[1]*, mais le logiciel Pari le donne sans peine :*

$$2^{128}+1 = 59649589127497217 \times 5704689200685129054721.)$$

On notera qu'à l'heure actuelle on ne sait pas exactement lesquels parmi les F_n sont premiers ou non. La réponse est seulement connue pour un nombre fini de n et, sauf pour les 5 premiers, tous les F_n en question sont composés. Cet exemple montre déjà deux choses, d'abord qu'un grand mathématicien peut dire des bêtises, et ensuite qu'il y a des questions, somme toute assez simples, pour lesquelles on n'a pas de réponse. J'y reviens plus loin.

Il y a donc des records du plus grand nombre premier connu qui sont détenus par d'énormes ordinateurs[2] (en général il s'agit de certains nombres de Mersenne (1588-1648) : $M_n = 2^n - 1$). Le plus ancien record est celui de Cataldi en 1588 avec $M_{19} = 524287$. Il y eut ensuite Lucas (1876) avec M_{127} qui a 39 chiffres. Le record, en 1999, était le nombre de Mersenne $M_{6972593}$ qui a tout de même plus de 2 millions de chiffres ! Je ne vais pas l'écrire[3], mais je peux tout de même dire qu'il commence par 437075 et finit par 193791.

1.2.4 Factoriser des grands nombres ?

Ce qu'il faut comprendre, c'est que les ordres de grandeur des nombres premiers que l'on sait exhiber, d'une part, et des nombres que l'on sait factoriser, d'autre part, ne sont pas du tout les mêmes, comme on l'a déjà senti à propos des nombres de Fermat. Pendant longtemps, factoriser un nombre de l'ordre d'un milliard était considéré comme à peu près impossible. Ainsi Mersenne, en 1643, avait donné à Fermat, comme un défi, de factoriser le nombre 100895598169 et le même défi avait été présenté comme impossible par Stanley Jevons en 1874 avec le nombre 8616460799. Pourtant, aujourd'hui, une calculatrice un peu perfectionnée factorise ces deux nombres sans difficulté.

Cependant, le record absolu de factorisation (en 1999 là encore) est bien loin de celui de primalité, c'est un nombre n de 155 chiffres, produit de deux nombres p et q de 78 chiffres, et encore a-t-il fallu pour cela faire travailler 300 ordinateurs en parallèle pendant 7 mois sur un algorithme très complexe, ce

[1] On constate sur cet exemple que la primalité est plus facile que la factorisation !

[2] Ce n'est pas seulement la puissance des ordinateurs qui est en jeu, mais surtout la qualité des algorithmes qu'ils utilisent (donc des mathématiques qui sont derrière).

[3] Il y faudrait un livre de 500 pages !

qui représente environ 35 années de temps de calcul pour une machine seule.

Voilà ces nombres :
$$10941738641570527421809707322040357612003732945$$
$$44920599091384213147634998428893478471799725789126$$
$$73324976257528997818337970765372440271467435315933543338 97 =$$
$$10263959282974110577205419657399167590 07$$
$$16567808038066803341933521790711307779\times$$
$$10660348838016845482092722036001287867 92$$
$$07958575989291522270608237193062808643.$$

On notera tout de même qu'il y a seulement 30 ans, on estimait qu'il faudrait 50 milliards d'années pour factoriser un nombre de 150 chiffres. Les progrès accomplis par les mathématiciens et les ordinateurs sont donc considérables. Bien entendu, cela ne remet pas en cause la fiabilité du code RSA : si on sait factoriser un nombre $n = pq$ de 150 chiffres il suffit de choisir des nombres p et q plus grands. On a vu qu'il y a de la marge puisqu'on sait expliciter des nombres premiers avec des millions de chiffres. Les banques travaillent déjà avec des clés n de l'ordre de 300 chiffres et les militaires avec des clés de 600 chiffres.

Et si un mathématicien améliorait fondamentalement les algorithmes de factorisation et leur permettait de rattraper les tests de primalité ? Alors, pour un temps au moins, il ne serait pas loin d'être le maître du monde[4] !

2 Il y a beaucoup de questions sans réponse en mathématiques

2.1 Introduction

Sans doute serez-vous étonnés de savoir qu'il y a beaucoup de questions sans réponses en mathématiques. Peut-être vous imaginez-vous que vos professeurs connaissent tout en mathématiques ? Au risque de ternir leur image, je dirai que ni eux, ni moi, ni aucun des mathématiciens, même les plus illustres, ni même tous les mathématiciens de la terre mis ensemble ne connaissent toutes les mathématiques. Je dirais même qu'il y a bien plus de choses inconnues que de choses connues. Mais, encore une fois, il n'est pas facile de donner des exemples au niveau du collège, sauf en arithmétique et c'est donc là que je vais mes exemples.

[4] N'ayez pas trop d'espoir tout de même. On pense qu'il a vraiment une raison profonde qui fait que la factorisation est beaucoup plus difficile que la primalité.

On a déjà vu un tel exemple avec les nombres de Fermat : personne, à l'heure actuelle, ne sait s'il y a d'autres nombres de Fermat que les 5 premiers qui sont des nombres premiers (on pense plutôt qu'il n'y en a pas, mais ce n'est qu'une **conjecture**, voilà un mot important).

2.2 Quelques problèmes d'arithmétique

2.2.1 Combien de nombres premiers dans une dizaine ?

Si on regarde combien il y a de nombres premiers dans une dizaine, on peut éliminer les multiples de 2 et ceux de 5. Il reste donc à regarder les nombres se terminant par $1, 3, 7, 9$. Il se peut qu'ils soient tous premiers, c'est le cas de $11, 13, 17, 19$, mais c'est rare. Si l'on cherche ensuite, cela n'arrive plus jusqu'à 100 (sont non premiers : 21, 33, 49, 51, 63, 77, 81, 91). En revanche, $101, 103, 107$ et 109 sont tous premiers (il suffit de voir qu'ils ne sont pas multiples de 3 ni de 7). La question est donc : peut-on trouver une infinité de dizaines riches contenant 4 nombres premiers ? La calculatrice (et l'ordinateur) permettent d'explorer le problème, mais pas de le résoudre et, à l'heure actuelle, on ne sait pas s'il y a une infinité de telles dizaines. Pire, on ne sait même pas s'il y a une infinité de nombres premiers jumeaux (c'est-à-dire avec 2 d'écart comme 11 et 13, ou 59 et 61).

Ce dernier problème date des Grecs, il est très facile à exprimer, mais très difficile, puisque personne n'a su le résoudre encore. Bien entendu, ce problème a été exploré avec l'ordinateur (jusqu'à 10^{15} on a trouvé environ 1177 milliards de paires de jumeaux), mais cela ne permet pas de répondre à la question : les capacités des ordinateurs, même immenses, sont limitées.

Puisqu'on parle de la question de la répartition des nombres premiers, si vous regardez le début des tables vous aurez peut-être l'impression qu'il y a des nombres premiers dans toutes les dizaines. Eh bien, ce n'est pas vrai et il n'y a pas besoin d'aller chercher très loin (il n'y en a pas entre 200 et 210). En fait, même si on prend un nombre même très grand (disons par exemple 1000), on peut toujours trouver 1000 nombres de suite sans aucun nombre premier. Cette affirmation vous paraît ambitieuse ? Elle est pourtant facile à prouver et vous devez pouvoir y arriver. Sur ces deux exemples, on voit combien il peut être délicat de prévoir, face à un problème de mathématiques inconnu, quelle va être sa difficulté.

2.2.2 La suite de Collatz ou de Syracuse

Il s'agit de la suite de nombres fabriqués comme suit. On part d'un entier n, s'il est pair on le divise par 2, s'il est impair on le multiplie par 3 et

on ajoute 1, il devient pair et on recommence. L'expérience semble montrer qu'on finit toujours par aboutir à 1. Par exemple, partant de 7, on trouve successivement 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1. Il est très facile de programmer cette suite sur une calculatrice et on vérifiera que cela semble bien marcher à partir de n'importe quel nombre. Mais, parfois, on peut monter assez haut, par exemple à partir de 27 on va jusqu'à 9232 avant de redescendre. Là encore, personne ne sait prouver que la suite revient toujours à 1.

Attention, puisqu'on parle de calculatrice et d'ordinateur, il faut bien comprendre que si l'informatique est un puissant outil, notamment d'exploration, elle ne permet pas, en général, de prouver les théorèmes, au moins lorsque ceux-ci font appel à des ensembles infinis. Il arriver d'ailleurs, que l'ordinateur déclare forfait alors qu'il y a des solutions, mais hors de sa portée. Voici un exemple que j'emprunte au livre de Jean-Pierre Delahaye (*Merveilleux nombres premiers*, Belin). Il s'agit de nombres "premiers entre eux". On dit que deux nombres p et q sont premiers entre eux s'ils n'ont pas de diviseur commun autre que 1. Par exemple 25 et 12 sont premiers entre eux, mais pas 25 et 15 qui ont en commun le facteur 5. Si, pour un entier n pas trop grand, disons jusqu'à $n = 10$, on regarde les nombres $n^{17} + 9$ et $(n+1)^{17} + 9$ et si on calcule leur plus grand commun diviseur (avec la calculatrice), on trouve toujours 1, ce qui signifie que ces nombres sont premiers entre eux. Si on continue, en écrivant un programme, jusqu'à 1000 ou 10000, ça marche encore. On peut continuer ainsi jusqu'à 8 millions de milliards de milliards de milliards de milliards de milliards et ça marche toujours. Pourtant, ce n'est pas toujours vrai, on montre que c'est faux pour

$$n = 8\,424\,432\,925\,592\,889\,329\,288\,197\,322\,308\,900\,672\,459\,420\,460\,792\,433.$$

3 Le chercheur : comment fait-il ?

Nous venons de voir qu'il y avait encore beaucoup de problèmes ouverts en mathématiques (et encore, vous n'en avez vu qu'une infime partie) et il y a, de par le monde, un grand nombre de chercheurs (plus de 100 000 sans doute ?) qui travaillent sur ces problèmes et on dit couramment qu'il s'est produit plus de mathématiques depuis la dernière guerre mondiale que depuis l'origine des temps jusqu'à la dernière guerre[5].

[5]Pour donner une idée, il y a, à la bibliothèque d'Orsay, plus de 400 revues de mathématiques qui publient chacune plus de 1000 pages de mathématiques nouvelles par an.

Ce que je voudrais aborder maintenant c'est une description de l'activité d'un chercheur. Pour que vous compreniez cette démarche, je vais l'illustrer en regardant avec vous un petit problème sur lequel vous allez exercer vos talents de chercheurs en herbe :

Tous les entiers ne sont pas des carrés parfaits, mais tout entier naturel peut-il s'écrire comme différence de deux carrés ?

3.1 Exploration et conjectures

La première phase de la recherche est une phase d'exploration et d'expérience qui consiste à étudier des exemples, des cas particuliers et, sur ces exemples, de **formuler** ce qu'on voit. C'est l'un des moments les plus amusants de la recherche, l'un de ceux où l'on peut donner libre cours à son imagination et il ne faut pas craindre de dire des bêtises, voyez ce qu'en dit Alexandre Grothendieck, l'un des plus grands mathématiciens du XX-ème siècle :

Quand je suis curieux d'une chose, mathématique ou autre, je l'interroge. Je l'interroge, sans me soucier si ma question est peut-être stupide ou si elle va paraître telle ... Souvent la question prend la forme d'une affirmation – une affirmation qui, en vérité est un coup de sonde. ... Souvent, surtout au début d'une recherche, l'affirmation est carrément fausse – encore fallait-il l'écrire pour que ça saute aux yeux que c'est faux, alors qu'avant de l'écrire il y avait un flou, comme un malaise, au lieu de cette évidence. Ça permet maintenant de revenir à la charge avec cette ignorance en moins, avec une question-affirmation peut-être un peu moins "à côté de la plaque".

Pour notre petit problème de carrés, la première chose à faire pour pouvoir regarder des exemples est de disposer d'une liste des carrés. Voici les premiers :

$$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, ...$$

On veut se faire une idée des entiers qui sont différences de deux carrés. On va faire l'expérience, en utilisant la liste ci-dessus. Bien entendu, il vaut mieux faire cela de manière ordonnée et rationnelle. On peut donc faire une première liste en retranchant deux carrés consécutifs, puis deux carrés pris de deux en deux, etc. Voilà ce qu'on obtient :

$$1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23$$

$$4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44$$

$$9, 15, 21, 27, 33, 39, 45, 51, 57, 63$$

$$16, 24, 32, 40, 48, 56, 64, 72, 80...$$

Que voit-on apparaître dans cette énumération :

• il semble qu'on atteint tous les nombres impairs,

• il semble qu'on atteint aussi tous les multiples de 4,

• en revanche il semble bien que l'on n'atteint pas les multiples de 2 qui ne sont pas multiples de 4.

La conjecture est donc la suivante :

3.1 Conjecture. *Les entiers n qui sont différences de deux carrés d'entiers sont les nombres impairs et les nombres multiples de* 4.

3.2 À l'assaut des conjectures

Une fois repérée une conjecture un peu solide, il faut la prouver, car, en mathématiques, on ne peut se contenter d'une vérification expérimentale, comme on l'a vu ci-dessus avec le problème cité par Jean-Paul Delahaye.

C'est le plus difficile. Parfois, et nous le verrons ci-dessous, l'expérience porte en germe une preuve, mais, le plus souvent, la phase de démonstration est longue, difficile et souvent elle échoue.

Heureusement, dans le cas des différences de carrés, la preuve n'est pas trop difficile et l'expérience qui a fourni la conjecture 3.1, permet aussi de la démontrer, au moins dès qu'on dispose de l'écriture et du calcul algébrique. En effet, si on compulse la liste, on voit qu'on atteint, par exemple, le nombre 7 comme différence de 16 et de 9 c'est-à-dire $4^2 - 3^2$, puis 9 comme différence de 25 et de 16, soit $5^2 - 4^2$, puis 11 comme différence de $36 = 6^2$ moins $25 = 5^2$. On répète l'expérience autant qu'il faut, jusqu'à ce qu'on soit capable de **formuler** ce qu'on voit, à savoir que les carrés qu'il faut utiliser sont, en quelque sorte, ceux des deux "moitiés" (celle du dessous et celle du dessus) du nombre impair. Vérifions que c'est bien ça en traitant le cas d'un nombre plus grand, par exemple 123, dont la moitié est $61,5$ et qui, si l'on a bien compris, doit être la différence $62^2 - 61^2 = 3844 - 3721$. On vérifie : c'est bien ça !

Pour prouver le théorème en toute généralité, il faut le faire avec des lettres : un nombre impair c'est un nombre de la forme $2p + 1$. Ses moitiés ? Ce sont $p + 1$ et p. La différence des carrés est alors $(p + 1)^2 - p^2$ que l'on peut calculer soit en utilisant la formule $(p + 1)^2 = p^2 + 2p + 1$ soit en la factorisant : $(p + 1 - p)(p + 1 + p)$. Dans les deux cas on trouve bien $2p + 1$. Au passage, vous noterez que pour faire des mathématiques il faut aussi de la technique (ici, connaître les identités remarquables).

Je vous laisse le plaisir de trouver le cas des nombres multiples de 4, puis de comprendre pourquoi ça ne marche pas pour les nombres pairs qui ne sont pas multiples de 4 et de vous poser de nouvelles questions (par exemple, quand il y a des solutions, y en a-t-il une seule ? plusieurs ? comment les trouver toutes ?).

3.3 Errare humanum est

Lorsqu'enfin on a écrit une preuve, les choses ne sont peut-être pas encore terminées. En effet, mon expérience, c'est qu'il peut arriver qu'une preuve soit fausse, même si on l'a faite soigneusement, et même parfois si elle a été acceptée par les experts. C'est quelque chose qui m'est arrivé il y a quelques années.

À l'époque, nous travaillions, ma collègue Mireille Martin-Deschamps[6] et moi-même, sur un objet nommé schéma de Hilbert (peu importe ce que cela signifie) qui dépend de deux entiers d et g et qu'on note $H_{d,g}$ et nous avions cru prouver que $H_{d,g}$ n'était **"presque" jamais connexe** (là encore, peu importe ce mot). La démonstration était écrite, contrôlée par un rapporteur, mais heureusement pas encore parue ! Pourtant, en étudiant plus à fond un exemple précis, correspondant à de toutes petites valeurs de d et g, $H_{4,0}$, nous avons montré qu'il était connexe, contrairement à ce que nous pensions. Il nous a fallu quelques jours pour admettre notre erreur et quelque temps encore pour comprendre où était la faute dans la démonstration. L'intérêt de cette erreur c'est qu'elle était révélatrice d'une conception très fausse sur l'objet en question. La preuve en est que, passant d'un extrême à l'autre, nous pensons maintenant que le schéma de Hilbert est **toujours** connexe.

Déceler une erreur dans une démonstration est un des moments les plus difficiles dans la vie d'un chercheur et je n'ai toujours pas acquis le détachement qui serait nécessaire pour vivre ce genre de moment avec sérénité, mais je relis ce que dit à ce sujet A. Grothendieck :

Mais il arrive aussi que cette image [de la situation] *est entachée d'une erreur de taille, de nature à la fausser profondément. ... Le travail, parfois laborieux, qui conduit au dépistage d'une telle idée fausse est souvent marqué par une tension croissante au fur et à mesure qu'on approche du nœud de la contradiction, d'abord vague, puis de plus en plus criante jusqu'au moment où elle éclate avec la découverte de l'erreur et l'écroulement d'une certaine vision des choses, survenant comme un soulagement immense.*

[6] Bien sûr, il y a aussi des femmes mathématiciennes. J'ai eu beaucoup de très bons élèves (deux d'entre eux ont eu la médaille Fields), mais je dirais que le meilleur de tous était une fille (Claire Voisin, actuellement directrice de recherche au CNRS).

Et il ajoute plus loin :

La découverte de l'erreur est un des moments cruciaux, un moment créateur entre tous, dans tout travail de découverte.

Tout cela pour dire qu'on ne peut pas faire de la recherche si l'on n'accepte pas de se tromper.

4 Des problèmes pour réfléchir

Les problèmes sur lesquels je vous propose de réfléchir sont des problèmes qui seront souvent pour vous de véritables problèmes de recherche. Cela signifie qu'il ne faut pas espérer les résoudre en un instant, mais au contraire y revenir encore et encore. On demandait un jour à Isaac Newton comment il avait trouvé la gravitation universelle. Il répondit : *En y pensant toujours.* La première qualité d'un chercheur c'est l'obstination.

Ce que je vous suggère c'est d'aborder ces problèmes avec la méthode que j'ai proposée ci-dessus : exploration, formulation de conjectures, contrôle des conjectures, puis, éventuellement (mais cela ne sera sans doute pas toujours possible), preuve des conjectures.

Je répète qu'il est normal que vous ne sachiez pas d'avance faire ces problèmes, qu'il est normal aussi que vous fassiez des erreurs. Être un chercheur c'est aussi sécher (parfois très longtemps) et se tromper. Une chose importante : la recherche est souvent une affaire d'équipe. Vous aurez donc intérêt à mettre en commun vos trouvailles. Enfin, vous avez aussi le droit de faire appel à vos professeurs.

4.1 Des trous dans les nombres premiers

Il s'agit du problème évoqué plus haut : comment trouver 1000 nombres de suite (ou un million, ou plus ...), sans aucun nombre premier ? (On pourra utiliser les factorielles c'est-à-dire les nombres de la forme $1\times2\times3\times4\times\cdots\times n$.)

4.2 Le plus grand produit

On choisit un nombre entier (par exemple 14, ou 25, etc.). On le décompose en somme de plusieurs entiers, par exemple $14 = 5+9$ ou $14 = 3+7+4$ (et bien d'autres) et on fait le produit de ces nombres, ici $5 \times 9 = 45$, $3 \times 7 \times 4 = 84$, etc. Pour quelle décomposition obtient-on le plus grand produit ? (On cherchera une réponse dans chaque cas, mais on essaiera aussi de donner une règle générale.)

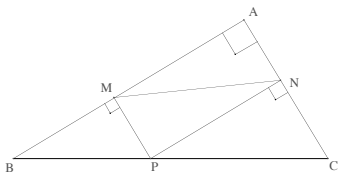
4.3 Les développements décimaux

On considère une fraction $\frac{p}{q}$ et on effectue la division de p par q, en écrivant aussi les chiffres derrière la virgule. On obtient une écriture décimale, en général illimitée. Que peut-on dire de cette écriture et pourquoi ?

Il y a beaucoup d'expériences à faire sur ce problème, à la main et à la calculatrice. On conseille de regarder les cas suivants, avec plusieurs p à chaque fois : $q = 7$, $q = 11$, $q = 13$, $q = 17$, $q = 28$, $q = 37$, etc. On n'oubliera pas qu'il y a une seule chose qu'on sait bien faire avec les écritures décimales, c'est de les multiplier par 10.

4.4 La longueur du segment mobile

On considère un triangle rectangle ABC, un point P de l'hypoténuse et ses projections M, N sur les côtés de l'angle droit. Pour quelle position de P la longueur MN est-elle minimale ? Plus difficile : et si le triangle n'est pas rectangle ?



4.5 La classe

La maîtresse du cours moyen de l'école des Aiguilles à Saint-Tricotin-sur-Pelote (Marne et Garonne) a donné un exercice sur les fractions à ses élèves. Le pourcentage de réussite a été de $47,82\%$ (valeur arrondie par défaut). Sachant que les classes de Saint-Tricotin ont moins de 30 élèves, dire combien la classe comporte d'élèves et combien ont réussi l'exercice.

4.6 Les fractions égyptiennes

Les anciens égyptiens utilisaient des fractions, mais seulement de numérateur 1, c'est-à-dire de la forme $\frac{1}{n}$. Bien sûr, toute fraction s'écrit comme somme de fractions égyptiennes : il suffit de répéter la même fraction :

$$\frac{p}{q} = \frac{1}{q} + \frac{1}{q} + \cdots + \frac{1}{q}, \qquad (p \text{ fois})$$

mais comment faire pour écrire n'importe quelle fraction (par exemple $\frac{4}{17}$ ou $\frac{4}{25}$) comme somme de fractions égyptiennes de dénominateurs *tous différents* ?

4.7 Les polyèdres

On appelle f le nombre de faces d'un polyèdre, a son nombre d'arêtes, s son nombre de sommets. En observant plusieurs polyèdres (un cube, une pyramide, un prisme, etc.) vous constaterez qu'il y a une relation entre ces nombres (qu'on appelle la formule d'Euler), laquelle ?

Un polyèdre archimédien est un polyèdre dont les faces sont des polygones réguliers (mais pas nécessairement tous de même type) et qui est tel qu'en chaque sommet aboutissent le même nombre de faces de chaque type, en respectant de plus le même ordre. Le ballon de football, lorsqu'il est fabriqué avec des pentagones et des hexagones, en est un bon exemple[7]. Comment savoir d'avance de combien de faces de chaque sorte on a besoin pour réaliser un polyèdre en sachant seulement ce qui se passe en un sommet, par exemple qu'il y a une alternance triangle, carré, pentagone, triangle ? (Il y a beaucoup d'inconnues, mais il faut essayer de les calculer les unes à partir des autres, et ne pas oublier la formule d'Euler.)

4.8 La voiture et les chèvres

Il s'agit d'un jeu télévisé américain. Dans ce jeu le candidat a devant lui trois portes. Derrière l'une de ces portes il y a une voiture et derrière chacune des autres, une chèvre. Si le candidat désigne la porte derrière laquelle se trouve la voiture, il la gagne. Le jeu se passe ainsi. Le candidat désigne une porte. Le présentateur (qui sait où se trouve la voiture) n'ouvre pas cette porte, mais en ouvre une autre, derrière laquelle se trouve une chèvre. Le candidat a droit à un autre essai dans lequel il peut maintenir son choix initial ou en changer. À votre avis, doit-il le maintenir, en changer, ou est-ce indifférent ?

5 Réponse aux questions des collégiens

Les questions des collégiens apparaissent en caractères romains, mes réponses sont en italiques.

5.1 Questions sur le métier de mathématicien

[7] Si on veut vraiment un polyèdre, avec des faces planes, il ne faut pas trop le gonfler !

Dans quel domaine des maths travaillez-vous ? géométrie, numériques ?

En fait, les deux ! Mon domaine s'appelle la géométrie algébrique. On y étudie des courbes définies par des équations. Il y a donc à la fois de la géométrie (les courbes) et du calcul (les équations). Depuis quelque temps je travaille plutôt sur la géométrie projective et les géométries non euclidiennes, de drôles de géométries dans lesquelles les droites sont courbes.

Comment choisissez vous ce que vous allez chercher ? Est-ce que quelqu'un vous dit ce que vous devez chercher ?

Déjà, au départ, on décide de s'intéresser à un domaine particulier des mathématiques (car personne ne connaît tout). Ce choix est dicté par deux choses : les préférences de chacun (on peut être plus géomètre ou plus calculateur, par exemple), et les perspectives qu'offre le domaine, à la fois sur le plan scientifique et sur celui des débouchés. Ensuite, il faut choisir un sujet, un point précis sur lequel on travaille. Pour un jeune chercheur, c'est le plus souvent son directeur de recherche qui lui propose un sujet. Pour un chercheur confirmé, ce choix provient de ses lectures, de discussions avec des collègues, de séminaires, de ses réflexions personnelles, etc.

Est-ce passionnant ?

Oui, c'est difficile, mais c'est passionnant, parce qu'on a l'impression de comprendre des choses nouvelles, d'explorer des domaines inconnus, de faire progresser la connaissance.

En quoi cela consiste-t-il ?

J'ai essayé d'expliquer cela plus haut : on se pose des questions, on imagine des réponses (des conjectures), on les teste, on essaye de prouver ce qu'on affirme, on se trompe, on propose autre chose, etc.

Comment savez vous que vous avez trouvé ?

C'est simple : au départ on se pose des questions et on a trouvé quand on est capable de leur donner une réponse, par exemple, telle chose est-elle vraie ? comment calculer telle quantité ? etc. Attention, comme on l'a vu, même quand on pense avoir trouvé, il peut subsister des erreurs ...

Ce que vous faites, ça sert à qui, à quoi ?

Dans mon cas, je ne connais pas d'applications directes de mon travail, mais comme on l'a vu plus haut, les applications des mathématiques n'arrivent souvent que longtemps après.

Est-ce la même fac que pour "l'espace" ?

Je ne sais pas. À mon avis, il n'y a pas une Fac pour l'espace, mais plusieurs.

5.2 La formation

Combien y a -t-il d'années d'études ?

Pour être chercheur en mathématiques, il faut un bac scientifique, puis licence, master et doctorat, soit en tout 8 ans après le Bac[8]*. Deux grandes voies : on peut entre à l'université dès le Bac, ou choisir les classes préparatoires aux grandes écoles. Là, l'idéal est de rentrer dans les Écoles Normales Supérieures ou à l'École Polytechnique (ou dans d'autres écoles, mais les écoles d'ingénieurs ne mènent pas directement à la recherche en maths), mais on peut aussi, et ça marche assez bien, revenir à la Fac en 3ème année.*

5.3 Les questions concrètes

Combien gagnez-vous ?

On ne peut pas dire que le métier soit très bien payé. Un enseignant chercheur ou un chercheur débutant gagne environ 1400 euros par mois. Avec un niveau d'études comparable, voire inférieur, un ingénieur débutant gagne plus de 2000 euros par mois. Un professeur d'université en fin de carrière (c'est mon cas) gagne plus de 4000 euros. La question (pour moi en tous cas) c'est l'intérêt qu'on a pour ce métier : ça me semble plus important de faire un métier qui m'intéresse plutôt que de gagner beaucoup d'argent, ne serait-ce que parce que je passe beaucoup de temps à mon travail.

Est-ce que vous faites 35h par semaine ?

Oh non, je travaille beaucoup plus que ça. Il ne faut pas oublier que je suis aussi enseignant. J'ai un peu diminué mon rythme depuis quelque temps, mais je travaille encore 50 heures par semaine au moins et souvent plus. Mais, encore une fois, si je travaille beaucoup c'est parce que je le veux bien, que j'aime ça et que ça m'intéresse plus que beaucoup d'autres choses.

5.4 La recherche en France et dans les autres pays

On dit que c'est difficile la recherche en france, êtes-vous parti aux USA ? pourquoi oui ou pourquoi non ?

La recherche c'est difficile partout. Le problème est plus aigu pour les disciplines comme la physique ou la biologie où il y a besoin de beaucoup de matériel dans les laboratoires, donc de beaucoup d'argent. C'est là qu'on dit parfois qu'il peut être intéressant de partir aux Etats-Unis. En mathématiques c'est moins essentiel, car on n'a pas besoin de grand-chose pour travailler.

[8]Mais il y a beaucoup de métiers qui utilisent des maths et où il n'est pas nécessaire d'avoir un doctorat. Souvent un master suffit (5 ans après le Bac), voire moins.

Cela peut toutefois présenter un intérêt pour rencontrer d'autres chercheurs. Pour ma part je ne suis jamais allé travailler aux USA, d'abord parce que j'aime bien la France, que je ne suis pas un grand voyageur et enfin parce que mon anglais est vraiment trop nul !

Les français sont-ils forts ?

En mathématiques, la réponse est oui de manière incontestable. Il suffit par exemple de regarder les médailles Fields et la proportion de français : sur 47 médailles, 12 pour les USA, 9 pour la France, 7 pour la Russie, 6 pour la Grande-Bretagne, etc. Il y a une très bonne école mathématique française.

Connaissez vous l'homme du grenier ? (Andrew Wiles)

Pas personnellement.

5.5 Questions personnelles

Aimiez vous les maths quand vous étiez petit ? Est-ce que vous étiez fort ? très fort ? Pourquoi êtes vous devenu chercheur ? et pourquoi en maths et pas en autre chose ?

J'essaie de répondre à toutes ces questions. Au départ je n'avais pas vraiment la vocation. Au collège et au lycée j'étais bon en maths, mais aussi dans les matières littéraires : français, histoire, notamment. Comme je suis issu d'un milieu très modeste (mes parents étaient ouvriers), j'ai suivi un cursus qui n'était pas fait pour mener aux études longues et, en particulier, je n'ai pas fait les études classiques (latin, grec) indispensables à l'époque pour faire des études littéraires supérieures. J'ai donc choisi les sciences par défaut. En terminale, le conseil de mes profs a été de faire une classe préparatoire aux grandes écoles. Comme, ni moi, ni mes parents, ne connaissions rien au système, j'ai suivi le conseil. J'ai été reçu à l'Ecole Normale Supérieure de la rue d'Ulm et à l'Ecole Polytechnique et j'ai choisi un peu par hasard d'entrer à la rue d'Ulm (paradoxalement, c'est plutôt à cause du prestige de l'école littéraire et de tous les grands écrivains qui y étaient passés, mais aussi à cause de la qualité du concours). A Ulm j'ai encore choisi un peu par hasard de faire des maths plutôt que de la physique. Cela étant, en dépit de tous ces hasards, je n'ai jamais regretté aucun de ces choix. Je fais un métier passionnant : j'aime bien les maths et surtout j'aime les enseigner. Ce que j'aime le plus, dans les maths elles-mêmes, c'est le sentiment de **comprendre** *les choses.*

Avez-vous été prof de primaire ? collège ? lycée ?

Non, j'ai tout de suite été professeur (au début on est seulement "assistant") dans l'enseignement supérieur.

Donnez-vous des cours particuliers ?

Non.

Enseignez vous à des gens qui veulent devenir chercheur ?

Oui, je l'ai fait beaucoup pendant toute une période (mais plus directement maintenant).

5.6 La question subsidiaire

Êtes vous plutôt OM ou PSG ?

En vérité, ni l'un ni l'autre. Je suis très amateur de foot, j'y ai joué moi-même pendant très longtemps (à un petit niveau), mais je n'ai pas une grande affection pour les supporters des grandes équipes et leur attitude souvent chauvine et parfois raciste. Je suis plutôt supporter des équipes de ma région : Nancy, Sochaux ou de celles de ma femme : Lille, Lens. J'ai longtemps soutenu l'OM quand il était en coupe d'Europe (et avant l'OM, Saint-Etienne, à la grande époque des verts), mais l'affaire OM-VA m'a refroidi.

En tous cas, je suis toujours supporter de l'équipe de France et mon pire souvenir c'est en 1982 (vous n'étiez pas nés) la demi-finale de coupe du monde perdue contre l'Allemagne à Séville.