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 expliquer comment ils font. Je vous laisserai d'ailleurs une petite collection de problèmes-défis pour vous exercer.

1 Les mathématiques c'est utile

1.1 Les mathématiques sont utiles actuellement

Comme tous les lycéens de ce pays, vous apprenez des mathématiques, mais peut-être vous demandez-vous : à quoi ça sert[1] ? 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.

En vérité, des mathématiques très élaborées sont présentes, de manière cachée, dans la vie de tous les jours, qu'il s'agisse des prévisions météo, qui utilisent de façon essentielle de l'analyse (dérivées, équations différentielles, équations aux dérivées partielles, en un mot, les fonctions), des tests ADN, qui utilisent fondamentalement des statistiques, etc. 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 arithmétique, et cela permet de détecter si la caissière se trompe. C'est aussi le cas pour les numéros de sécurité sociale ou ceux des cartes bancaires.

[1] Je n'aborde ici que l'aspect utilitaire, mais un autre élément de réponse important concerne l'apprentissage de la rationalité, du raisonnement, de la logique.

1.2 Les mathématiques seront utiles demain : l'exemple des coniques

Certains domaines des mathématiques semblent à première vue ne pas avoir d'applications, mais il faut se garder de croire qu'ils n'en auront jamais.

Voici deux exemples en ce sens. Le premier concerne les coniques (ellipses, paraboles, hyperboles). Les anciens Grecs étudiaient ces courbes pour leurs propriétés géométriques. À l'époque, elles n'avaient pas d'applications. Ce n'est qu'au XVII-ième siècle que Kepler s'est aperçu que les trajectoires des planètes étaient justement des ellipses. De nos jours, ces courbes sont utiles dès qu'on envoie un satellite (et vous savez combien c'est important pour le téléphone, la télévision, le GPS, etc.).

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

L'autre exemple concerne l'arithmétique. 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.

1.3.1 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[2]. On retraduit alors le message en lettres et on a YNYQVU. Le

[2]Une méthode très simple de codage consiste à transformer l'entier z variant entre 1 et

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 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.

1.3.2 Le code RSA

La méthode RSA dont nous allons parler a été inventée en 1978 par Rivest, Shamir et Adleman et repose sur les nombres premiers. La problématique de cette méthode est la suivante.

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. Cette clé doit lui être transmise par son chef. Le problème, de nos jours, avec Internet et tous les satellites qui nous tournent autour, c'est qu'on n'est pas sûr du tout que les ennemis n'écoutent pas les messages transmis. Avec la plupart des systèmes de codage, si l'on connaît la clé de codage, on sait aussi décoder les messages. Par exemple, imaginons que la clé soit l'opération qui à une lettre, représentée par un nombre x modulo 26, associe $11x - 7$ (toujours modulo 26), ce qui associe par exemple à la lettre E la lettre V. On calcule alors facilement l'opération inverse[3], ce qui permet de décoder les messages.

L'intérêt du code RSA c'est qu'il est à sens unique : la clé de codage n'est pas une clé de décodage ! Voici le principe de cette méthode.

Le chef C calcule deux grands nombres premiers p et q (disons d'une centaine de chiffres au moins), il calcule ensuite le produit pq (cela ne représente qu'une fraction de seconde pour une machine). Il choisit aussi un nombre e premier avec $p - 1$ et $q - 1$ (il y en a beaucoup, par exemple un nombre

26 en $az + b$ avec a, b entiers, avec a premier à 26, et à réduire ce nombre modulo 26, voir ci-dessous.

[3]C'est $x \mapsto -7x + 3$.

premier qui ne divise ni $p-1$ ni $q-1$). Il transmet à E la clé de codage, qui est constituée du nombre pq et du nombre e (mais il garde secrets les deux nombres p et q). La clé est **publique** : peu importe si l'ennemi l'intercepte. Pour coder le message, E n'a besoin que pq et de e, 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.

Voici précisément la méthode de codage. Le message est un nombre $a < pq$. Pour le coder, E calcule a^e modulo pq (le reste r de a^e dans la division par pq). Là encore, une machine fait cela instantanément. C'est ce nombre r qu'il envoie à son chef.

Comment faire pour retrouver a à partir de r ? En principe c'est simple. Comme e est premier avec pq, le théorème de Bézout montre qu'il existe un nombre d tel que $de \equiv 1 \pmod{(p-1)(q-1)}$. Avec ce d on calcule a en faisant l'opération à l'envers[4] : $a = r^d \pmod{pq}$. Il suffit donc de calculer d. Quand on connaît $(p-1)(q-1)$, trouver d est facile (c'est l'algorithme d'Euclide). Mais voilà : on a $(p-1)(q-1) = pq-p-q+1$ et pour connaître ce nombre il nous faut $p+q$, donc p et q et ça, on ne sait pas faire !

1.3.3 Un exemple

Je prends un exemple avec des nombres pas trop grands : $pq = 11639$ et $e = 3361$. Si le message a est égal à 2511, on calcule a^e modulo pq. Il faut tout de même écrire un programme, sinon la machine répond ∞. Avec la fonction *powerv* on trouve 9404.

Pour inverser le processus, il y a besoin de connaître $(p-1)(q-1)$, donc p et q. Ici, ce n'est pas trop compliqué : on a $p = 103$ et $q = 113$, d'où $(p-1)(q-1) = 11424 = 2^5 \times 3 \times 7 \times 17$. Comme e est premier, il est bien premier avec ce nombre. Pour trouver d tel que $de \equiv 1 \pmod{11424}$ on utilise l'algorithme d'Euclide pour trouver les coefficients de Bézout. On a :

$$673 \times 3361 - 198 \times 11424 = 1.$$

On doit donc choisir $d = 673$. On vérifie qu'on a bien $9404^{673} \equiv 2511 \pmod{11639}$.

[4]Le principe est dans le petit théorème de Fermat : pour tout a premier avec p on a $a^{p-1} \equiv 1 \pmod{p}$ et de même avec q.

1.3.4 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[5] $F_n = 2^{2^n} + 1$ 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[6].

(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). Même pour* $2^{512}+1$ *elle donne une réponse négative en une minute environ. En revanche, pour le suivant, elle ne donne rien en un quart d'heure*[7]*, 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[8] (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[9], mais je peux tout de même dire qu'il commence par 437075 et finit par 193791. Je vous laisse montrer cela à titre d'exercice (pas si facile).

---

[5] Seuls les $2^r + 1$ où r est une puissance de 2 ont une chance d'être premiers à cause de la formule $a^m + 1 = (a + 1)(a^{m-1} - a^{m-2} + a^{m-3} - \cdots - a + 1)$ lorsque m est impair.

[6] On montre que 641 divise $2^{32}+1$. Cela repose sur les égalités $641 = 625+16 = 5^4+2^4$ et $641 = 640 + 1 = 2^7 \times 5 + 1$. Modulo 641 on a donc $2^{28} \times 5^4 = 1$ et comme $5^4 = -2^4$, on a bien $2^{32} = -1$.

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

[8] 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).

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

1.3.5 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[10] 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 qui représente environ 35 années de temps de calcul pour une machine seule.

Voilà ces nombres :
109417386415705274218097073220403576120037329 45
449205990913842131476349984288934784717997257891 26
733249762575289978183379707653724402714674353159335433389 7 =
102639592829741105772054196573991675900 7
165678080380668033419335217907113077 79×
106603488380168454820927220360012878679 2
079585759892915222706082371930628086 43.

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[11] !

[10] Fermat avait répondu au défi, et semble-t-il très rapidement. On ignore comment il a fait. On trouvera en annexe une hypothèse que je soumets au lecteur, sans la moindre garantie.

[11] N'ayez pas trop d'espoir tout de même. On pense qu'il a vraiment une raison profonde

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 lycée, sauf en arithmétique et c'est donc là que je vais prendre mes exemples.

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.

qui fait que la factorisation est beaucoup plus difficile que la primalité.

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[12].

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 :

On choisit un nombre entier. On le décompose en somme de plusieurs entiers et on fait le produit de ces nombres. Pour quelle décomposition obtient-on le plus grand produit ?

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".

[12]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.

L'idée est donc de décrire la vision partielle qu'on a de la situation : la conjecture est une tentative pour éclairer le paysage. Bien entendu, cette vision partielle peut être erronée, cela dépend beaucoup de la profondeur de notre connaissance du sujet.

Dans notre problème, on regarde l'exemple du nombre 14. On essaie d'abord les décompositions les plus simples : en deux morceaux. Ainsi, $14 = 12 + 2$ donne 24, $14 = 10 + 4$ donne 40, $14 = 8 + 6$ donne 48, etc. Une idée géométrique peut nous aider : le nombre donné peut se voir comme le demi-périmètre d'un rectangle écrit comme $longueur + largeur$. Le produit est alors $longueur \times largeur$, c'est-à-dire l'aire du rectangle. Intuitivement, on se doute bien que, parmi les rectangles de périmètres donnés, celui qui a la plus grande aire est le carré. On peut donc hasarder une conjecture :

Le plus grand produit est atteint quand on coupe le nombre en deux parties égales.

3.2 À l'assaut des conjectures

La phase suivante est de décider si les conjectures sont vraies ou non. Cette phase est dialectique, entre la recherche d'arguments probants[13] en faveur de la conjecture (ou la recherche d'une démonstration dans le cas du mathématicien, l'objectif étant avant d'emporter la conviction) et la recherche de contre-exemples. Dans cette partie, l'erreur joue un rôle fondamental.

Voilà 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.*

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.

Dans notre situation on se rend vite compte que la décomposition en deux n'est pas optimale. Par exemple, la décomposition $14 = 7 + 7$ donne 49, mais on peut faire mieux avec $5 + 5 + 4$ qui donne 100.

[13] On ne peut se contenter d'une vérification expérimentale, comme on l'a vu ci-dessus avec le problème cité par Jean-Paul Delahaye.

Il faut donc remettre en cause notre vision des choses, et renoncer à l'idée trop simple du découpage en deux. D'ailleurs cette remise en cause en induit d'autres. Ainsi, on voit très vite qu'on peut faire encore mieux que $5+5+4$ en changeant le 5 en $2+3$ car $2\times 3 = 6 > 5$. On voit ici apparaître des 2 et des 3. L'exemple de $6 = 3+3 = 2+2+2$ montre que les 3 sont meilleurs. Une nouvelle conjecture émerge donc assez naturellement, centrée sur le nombre 3 :

Il faut mettre le plus possible de 3 dans la décomposition.

Voilà une nouvelle conjecture qui semble bien solide car si on prend $14 = 3+3+3+3+2$, on obtient le produit $3^4\times 2 = 162$ et l'examen des divers cas montre qu'on ne peut faire mieux. Un autre essai avec 15 conforte cette vision. Tout va bien ? Si on examine l'exemple suivant, 16 écrit $3+3+3+3+3+1$ selon notre principe, le produit est 243, tandis qu'avec $16 = 3+3+3+5+2$ c'est 270, la conjecture est encore fausse !

On est ici en présence de ce que j'ai envie d'appeler une erreur "partielle" : dans la situation, il y a un détail qui nous a échappé. En général, ce type d'erreur est réparable (parfois au prix d'un rude labeur) et ne remet pas en cause l'ensemble du travail.

Dans le cas de notre problème, nul doute que le lecteur a déjà trouvé comment réparer la faute !

Il reste ensuite à écrire une preuve sous une forme mathématique, afin d'être sûr d'avoir traité tous les cas et d'avoir bien compris toutes les subtilités de la situation. L'intérêt principal d'une démonstration est d'emporter la conviction, d'être inattaquable en quelque sorte. Quoique ...

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[14] 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,

[14]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).

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, même en me récitant l'évangile selon Grothendieck !

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 Les sommes de nombres consécutifs

Quels sont les nombres qui sont sommes d'un nombre $n \geq 2$ fixé d'entiers positifs consécutifs ? Quels sont ceux qui sont sommes d'au moins deux entiers positifs consécutifs ?

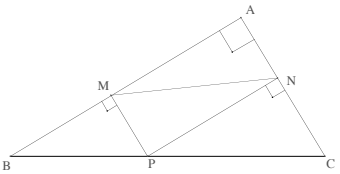
4.3 Les développements décimaux

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[15]. 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 Annexe, la factorisation de Fermat

5.1 Le problème

Rappelons la question de Mersenne :

Le nombre 100895598169 *est-il premier ?*

Voici la réponse de Fermat :

À cette question je réponds que ce nombre est composé et se fait du produit des deux : 898423 *et* 112303 *qui sont premiers. Je suis toujours, mon révérend Père, votre très humble et très affectionné serviteur.*

La question est : comment a-t-il fait ?

5.2 Une procédure bien connue de Fermat

5.2.1 Une citation

Je recopie ici un extrait d'une lettre du même Fermat au même Mersenne en 1664 :

Cela posé, qu'un nombre me soit donné, par exemple 2027651281*, on demande s'il est premier ou composé, et de quels nombres il est composé,*

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

au cas qu'il le soit. J'extrais la racine, pour connaître le moindre des dits nombres, et trouve 45029 *avec* 40440 *de reste, lequel j'ôte du double plus* 1 *de la racine trouvée, savoir de* 90059 *: reste* 49619*, lequel n'est pas carré, parce qu'aucun carré ne finit par* 19*, et partant je lui ajoute* 90061*, savoir* 2 *plus* 90059 *qui est le double plus* 1 *de la racine* 45029*. Et parce que la somme* 139680 *n'est pas encore carrée, comme on le voit par les finales, je lui ajoute encore le même nombre augmenté de* 2*, savoir* 90063 *et je continue ainsi d'ajouter tant que la somme soit un carré, comme on peut voir ici. Ce qui n'arrive qu'à* 1040400 *; qui est carré 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 carré que la dernière, car les carrés ne peuvent souffrir les finales qu'elles ont, si ce n'est* 499944 *qui néanmoins n'est pas carré. Pour savoir maintenant les nombres qui composent* 2027651281*, j'ôte le nombre que j'ai premièrement ajouté, savoir* 90061*, du dernier ajouté* 90081*. Il reste* 20*, à la moitié duquel plus* 2*, savoir à* 12*, j'ajoute la racine premièrement trouvée* 45029*. La somme est* 45041*, auquel nombre ajoutant et ôtant* 1020*, racine de la dernière somme* 1040000*, on aura* 46061 *et* 44021*, qui sont les deux nombres plus prochains qui composent* 2027651281*. Ce sont les seuls, parce que l'un et l'autre sont premiers.*

5.2.2 Traduction

La procédure, dite avec des symboles[16], est donc la suivante. On a à décomposer un nombre N. On en calcule la racine carrée et sa partie entière q, ici $q = 45029$. On a donc $q^2 \leq N < (q+1)^2$. Si on a $N = q^2$ on a fini. Ici, ce n'est pas le cas car on a $N = q^2 + 40440$. On pose $r = N - q^2$.

L'idée, ensuite, est d'écrire N sous la forme $N = (q+k)^2 - s^2 = (q + k - s)(q + k + s)$. On essaie successivement avec $k = 1, 2, ...$ et on s'arrête si $(q+k)^2 - N$ est un carré. Par exemple pour $k = 1$, on regarde $(q^2 + 2q + 1) - N = (2q + 1) - r$. On retranche donc $r = 40440$ de $2q + 1 = 90059$ comme le dit Fermat. Il reste 49619 qui n'est toujours pas un carré. Comme on a $2kq + k^2 = 2(k-1)q + (k-1)^2 + (2q + 2k - 1)$, on continue en ajoutant $2q + 3$, $2q + 5$, ..., $2q + 2k - 1$, jusqu'à ce qu'on trouve un carré. Ici, il faut aller jusqu'à $k = 12$:

$$2q + 1 - r + (2q + 3) + (2q + 5) + \cdots + (2q + 23) = 1040400 = (1020)^2 = s^2.$$

On a donc $N = (q+k)^2 - s^2 = (45029 + 12)^2 - 1020^2 = 44021 \times 46061$.

[16]Et l'on voit ici quelle économie de pensée ils procurent !

5.2.3 La méthode de Fermat dite à ma manière

Il s'agit de décomposer le nombre N en produit de facteurs premiers. On suppose N impair. On pose $q = [\sqrt{N}]$ et on suppose que N n'est pas un carré. On a donc $q^2 < N < q^2 + 2q + 1$. On cherche une décomposition de N sous la forme $N = (q + a)(q + b)$ avec $a, b \in \mathbf{Z}$.

5.1 Lemme. *Si on a une décomposition comme ci-dessus :*

- *a et b sont de même parité,*
- *a et b sont non nuls et de signes contraires, sauf si l'on a $N = q(q+2)$,*
- *on a $ab \leq 0$ et $a + b > 0$.*

Démonstration. Comme N est impair il en est de même de $q + a$ et $q + b$ et on a donc $a \equiv q + 1$ et $b \equiv q + 1$ modulo 2.

Si a, b sont tous deux ≤ 0 on a $(q + a)(q + b) \leq q^2 < N$, s'ils sont tous deux > 0 on a $(q+a)(q+b) \geq q^2+2q+1 > N$. Ces cas sont donc impossibles. Il reste à examiner le cas où l'un des deux, disons a, est nul et l'autre > 0. Comme on a $q(q+b) \leq q^2 + 2q$ on a $b \leq 2$ et donc $b = 2$ à cause de la parité.

Pour le dernier point, il est clair que ab est ≤ 0. On a donc $q^2 < N = q^2 + (a + b)q + ab \leq q^2 + (a + b)q$, ce qui montre que $a + b$ est > 0.

On cherche donc a, b tels que $N - q^2 = (a + b)q + ab$ et on sait que $a + b$ est pair et $ab \geq 0$. Pour cela, on effectue une pseudo-division euclidienne en écrivant $N - q^2 = 2nq - r_n$, avec $n \in \mathbf{N}^*$ et $r_n < 0$, mais sans imposer la condition $|r_n| < q$.

On aura la factorisation cherchée si l'on peut résoudre en $a, b \in \mathbf{Z}$ les équations $a+b = 2n$ et $ab = -r_n$. Les nombres a, b sont racines de l'équation $X^2 - 2nX - r_n = 0$ et cette équation admet des solutions entières si et seulement si son discriminant (réduit) $\Delta_n = n^2 + r_n$ est un carré.

Pour faire ce calcul de proche en proche, on peut, comme Fermat, utiliser une formule de récurrence : $\Delta_{n+1} = \Delta_n + 2q + 2n + 1$ (qui résulte de $r_{n+1} = r_n + 2q$).

La validité de la méthode est donnée par le lemme suivant :

5.2 Lemme. *On suppose que N est produit de deux nombres premiers $p_1 p_2$. Soit A la "patience" de l'utilisateur (c'est-à-dire le nombre d'essais qu'il est prêt à faire pour mettre en œuvre la méthode). La méthode de Fermat donne un résultat pourvu que la moyenne $m = \dfrac{p_1 + p_2}{2}$ diffère de $q = [\sqrt{N}]$ de moins de A.*

Démonstration. Si on a $N = (q + a)(q + b)$, la moyenne est $m = q + \dfrac{a + b}{2}$. Un succès de la tentative correspond à l'écriture $N - q^2 = 2nq - r_n$, avec

$n = \dfrac{a+b}{2} = m - q$ et il doit être obtenu avec $n \leq A$, d'où le résultat.

5.3 *Remarques.* 1) Si $N = q(q+2)$, on a $N - q^2 = 2q$ et la factorisation est obtenue dès la première opération.

2) Le cas le plus favorable après celui-ci est celui où le succès est obtenu avec $n = 1$. Dans ce cas, l'écriture $N - q^2 = 2q - r$ est la division euclidienne de $N - q^2$ par $2q$ (avec reste r négatif mais tel que $|r| < 2q$).

Attention, l'exemple de $N = q^2 + q - s$ avec $0 < s < q$ et $q + s + 1$ carré comme $N = 65$, $q = 8$, $r = 7$ montre que $N - q^2 = 2q - (q + s)$ n'est pas nécessairement la division euclidienne de $N - q^2$ par q.

5.3 Une hypothèse sur la décomposition de 100895598169 ?

5.3.1 Le principe

L'idée est très voisine de celle de la méthode précédente. On part d'un entier N et on suppose qu'il est impair et que ce n'est pas un carré. Au lieu de regarder seulement $q = [\sqrt{N}]$, on regarde tous les nombres $q = [\sqrt{N/k}]$ pour $k = 1, 2, \ldots$, jusqu'à la patience de l'utilisateur. On cherche ensuite, avec le nombre q en question, une décomposition de la forme $N = (kq + a)(q + b) = kq^2 + (kb + a)q + ab$. Précisément :

5.4 Proposition. *On suppose que N est produit de deux nombres premiers $p_1 p_2$. Soit A la "patience" de l'utilisateur (c'est-à-dire le nombre d'essais qu'il est prêt à faire pour mettre en œuvre la méthode). On suppose qu'il existe $k \leq A$ tel que, si $q = [\sqrt{N/k}]$, on ait $p_1 = kq + a$ et $p_2 = q + b$ avec $|a| < \sqrt{q}$ et $|b| < \sqrt{q}$. On trouve alors la décomposition en effectuant les divisions euclidiennes de $N - kq^2$ par q pour $k \leq A$.*

Démonstration. Si on a $N = (kq + a)(q + b)$, on a $N - kq^2 = (kb + a)q + ab$. Comme on a supposé $|ab| < q$, la division euclidienne de $N - kq^2$ par q donne $kb + a$ comme quotient et ab comme reste (éventuellement négatif) et, comme k est connu, on en déduit a, b donc p_1 et p_2.

5.5 *Remarque.* Si l'on est dans cette situation, on a $N - q^2 = q(kb + a) + ab$ avec $|ab| < q$ et le quotient approché de $N - q^2$ par q est proche de l'entier $kb + a$. C'est ainsi qu'on peut repérer les cas propices à un essai.

5.3.2 Application à Fermat et Mersenne

Pour $k = 1, 2, \ldots$ on calcule $q = [\sqrt{N/k}]$, puis le quotient approché de $N - kq^2$ par q et on regarde si ce quotient est proche d'un entier. On obtient

successivement, pour $k = 1, \ldots, 7$ les quotients suivants : $1,34$; $3,5$; $5,57$; $2,69$; $2,28$; $3,14$; $12,46$, tous assez éloignés des entiers.

En revanche, pour $k = 8$, on a $q = 112302$, et $\dfrac{N - kq^2}{q} \simeq 15,0000623$. On écrit donc :

$$100895598169 - 8 \times 112302^2 = 15 \times 112302 + 7.$$

Il reste à résoudre les équations : $8b + a = 15$ et $ab = 7$, ce qui donne évidemment $a = 7$ et $b = 1$. On obtient la décomposition $N = p_1 p_2$ avec $p_1 = kq + a = 898423$ et $p_2 = q + b = 112303$.