Initiation à la recherche en mathématiques

Gaetan Bisson

https://gaati.org/bisson/

Introduction

Les mathématiques remontent aux premières civilisations et font l'objet d'études systématiques depuis plusieurs siècles. La manière concise par laquelle elles vous ont été enseignées en licence est trompeuse : afin de prendre cette forme aboutie, ce que nous appelons de nos jours les fondations des mathématiques ont connu bien des remaniements.

Ce cours a pour objectif de montrer la démarche de recherche par laquelle de nouvelles mathématiques voient le jour et, progressivement, prennent la forme établie sous laquelle elles sont ensuite enseignées. Discuter des thèmes de recherche actuels nous entraînerait bien trop loin, aussi nous contenterons nous de considérer quelques exemples concrets. Nous insisterons sur deux points :

— les démarches suivies par les chercheurs en mathématiques ;
— les outils permettant de supporter ces démarches.

Parmi ceux-ci, l'outil informatique occupe aujourd'hui une place importante ; la seconde partie de ce cours sera dédiée à leur usage avec pour objectif de servir tant le chercheur que l'enseignant. Rappelons qu'aux épreuves orales l'utilisation de logiciels est fortement appréciée par le jury.

Note. Le titre de ce module est un oxymore : on peut s'initier à des techniques connues et maîtrisées mais, par essence, pas à la recherche. Autrement dit, ce cours ne fera pas de vous des chercheurs ; il vise modestement à vous familiariser avec le monde de la recherche et certains des outils qui y sont mis en œuvre.

Table des matières

Chapitre 1

Contexte

Le monde mathématique des chercheurs est très différent de celui des étudiants : même si les objets étudiés sont les mêmes, la manière de les considérer est fondamentalement différente. Ce chapitre vise a donner une vague idée de la manière dont fonctionnent les chercheurs.

1.1 Perspectives

La recherche en mathématiques consiste à découvrir de nouvelles vérités. Les vérités connues sont des **théorèmes**, c'est-à-dire que leur véracité est assurée par une preuve. Lorsque l'on suppose une vérité mais ne parvient pas encore à la prouver, c'est une **conjecture**. Le but ultime est de pouvoir répondre à toute question par un théorème.

Exemple. *Pour $n \in \mathbb{N}^*$ soit la question : « Existent-ils des entiers positifs non nul x, y, z tels que $x^n + y^n = z^n$? »*

Pour $n = 1$ et $n = 2$, c'est évident que la réponse est oui.

En 1637, Fermat conjecture que pour tout $n > 2$ la réponse est négative. Il prouve cela dans le cas particulier $n = 4$.

En 1994, Wiles prouve la conjecture de Fermat pour tout entier $n > 2$; elle devient le théorème de Wiles.

Une fois qu'une question particulière a obtenue une réponse satisfaisante, on se penche sur d'autres questions, typiquement plus générales. Évidemment, tous les problèmes ne sont pas d'intérêts égaux ; savoir se poser des questions pertinentes (et écarter les autres) est l'une des qualités d'un bon chercheur.

Exemple. *Caractériser les polynômes $P \in \mathbb{Z}[x_1, \ldots, x_n]$ qui admettent des racines entières est un sujet de recherche important et très actif de nos jours dont le théorème de Fermat–Wiles n'est qu'un cas très particulier.*

Contrairement aux cours de licence qui sont figés, dans le sens où tous les problèmes qu'on y aborde ont été résolus de manière satisfaisante depuis bien longtemps, la recherche évolue constamment, chaque chercheur étant libre de la faire avancer dans la direction de son choix. Les mathématiques étant une science ancienne, cette évolution a actuellement lieu bien au delà du niveau licence.

1.2 Parcours

On vous enseigne des mathématiques depuis la maternelle mais c'est seulement en licence que cet enseignement est devenu rigoureux : on y a défini le vocabulaire utilisé et prouvé les énoncés affirmés. Les notions présentées en licence couvrent les bases du langage moderne et vous permettent ainsi de comprendre tout énoncé mathématique, au vocabulaire près. Considérons par exemple les deux résultats suivants.

Théorème (Helfgott, 2013). *Tout entier impair supérieur à cinq est la somme de trois nombres premiers.*

Théorème (Bhargava–Shankar, 2010). *Le rang des courbes elliptiques définies sur $\mathbb{Q}$ est de moyenne bornée lorsqu'elles sont ordonnées par leur hauteur.*

Le premier théorème est compréhensible par tous alors que le second utilise des notions plus avancées ; leur résolution à tous deux a cependant été de difficulté colossale. En particulier, la simplicité d'énoncé du premier théorème est trompeuse : il ne peut humainement pas être démontré avec les seuls outils que vous avez acquis en licence.

Tout parcours permettant d'atteindre un niveau recherche est donc relativement long ; typiquement :

licence	(3 ans)	On apprend les bases des grands domaines : algèbre, analyse, géométrie et probabilités. Parallèlement, on suit encore des cours non mathématiques.
master	(2 ans)	On apprend les résultats classiques d'un domaine particulier (toujours avec des cours et des livres) avant d'approfondir un sujet précis (sur articles).
doctorat	($\approx$ 4 ans)	On rattrape la recherche (soi-même, sur articles) puis on y contribue.
post-doctorat	($\approx$ 2 ans)	On fait encore ses preuves pour mieux prétendre à un poste permanent.
poste permanent	(∞ ans)	Enfin !

En France, il y a deux catégories de postes de chercheurs permanents :
- les enseignants-chercheurs (techniquement « maîtres de conférences » et « professeurs ») sont employés par les universités et dédient la moitié de leur temps à l'enseignement et l'autre moitié à la recherche ;
- les chercheurs (techniquement « chargés de recherches » et « directeurs de recherches ») sont employés par des instituts (CNRS, INRIA, IRD, etc.) et dédient la totalité de leur temps à la recherche.

Note. Dans des domaines plus jeunes que les mathématiques, notamment l'informatique, on peut faire de la recherche bien plus tôt, typiquement, dès le niveau L3, alors qu'en mathématiques c'est rarement avant la seconde moitié d'une thèse.

Attention. Comparé aux contributions individuelles qu'y fait chaque chercheur, l'édifice global des mathématiques est de taille absolument colossale, au point où il est désormais impensable qu'une personne puisse prétendre connaître l'entièreté des mathématiques. Comme illustration, voir notamment [2].

1.3 Contributions

Lorsqu'un chercheur estime avoir quelque chose de nouveau à contribuer à la science, il rédige un article. En mathématiques, cela arrive environ une fois par an et l'article fait une vingtaine de pages, même si ces chiffres varient énormément. Un article culmine généralement en l'énoncé d'un théorème majeur dont la preuve met bout à bout les différents éléments développés dans l'article mais, évidemment, ces éléments peuvent aussi avoir un intérêt intrinsèque indépendant de leur application phare.

Pour expliquer une telle contribution à un non spécialiste du domaine de recherche concerné, il faut préciser :

1. la motivation du problème ;
2. les enjeux de sa résolution ;
3. l'état de l'art sur la question ;
4. la difficulté et les obstacles ;
5. l'originalité de la résolution proposée ;
6. sa diffusion ;
7. son impact.

Exemple. *Illustrons ces éléments dans le cas concret de l'article [1] ; cela devrait vous permette d'apprécier les qualités de cette contribution malgré le vocabulaire qui vous fait défaut.*

1. *Les courbes elliptiques sont des objets centraux en théorie des nombres et en cryptographie. Ils sont munis d'une structure qui permet de les étudier bien plus efficacement : leurs anneaux d'endomorphismes ; malheureusement le calcul de ces anneaux est très coûteux actuellement.*
2. *Les applications exploitant ces anneaux sont actuellement bloquées par le coût de leur calcul. Le rabaisser permettrait de décupler la portée de ces applications, avec des retombées tant constructives que destructives en cryptographie.*
3. *Les méthodes de Kohel, Eisenträger–Lauter et Wagner sont les seules connues actuellement pour calculer ces anneaux mais elles sont toutes de complexité exponentielle, c'est-à-dire très coûteuses.*
4. *Les paramètres de la courbe elliptiques donnant directement des informations sur leurs anneaux d'endomorphismes sont intrinsèquement de taille exponentielle. Obtenir une méthode plus rapide nécessite donc une approche complètement nouvelle.*
5. *Notre approche exploite la théorie de la multiplication complexe afin de contourner cela. Essentiellement, cela permet de ramener ces grands paramètres à des produits de petits paramètres, plus faciles à calculer.*
6. *L'article rédigé a été accepté dans le* Journal of Number Theory*, une revue internationalement reconnue en théorie des nombres, et a fait l'objet d'exposés invités à des conférences internationales.*
7. *L'article en question a été cité plus de quarante fois, les méthodes qu'il introduit ont été reprises afin de résoudre de multiples autres problèmes, et sont actuellement en cours d'implantation dans le logiciel PARI.*

Rédiger de telles « explications » permet en outre de remettre les résultats concernés dans leur contexte et de prendre ainsi du recul par rapport à la contribution proprement dite. Nous allons maintenant détailler leurs différents éléments en prenant comme cas pratiques des résultats que vous (devriez) maîtriser.

Exercice. *Vous êtes le premier à démontrer que toute suite réelle croissante majorée admet une limite. Expliquez cette contribution à un non spécialiste.*

Exercice. *Vous êtes le premier à démontrer que, pour toute matrice réelle carrée M, les racines λ de $\det(M - \lambda \mathrm{id})$ sont exactement les valeurs propres de M. Expliquez cette contribution à un non spécialiste.*

Remarque. En tant qu'enseignants vous êtes aussi confrontés au problème de motiver les notions et résultats présentés en cours : une leçon ne doit pas se borner à être une liste de définitions et théorèmes. Entraînez vous, avant chaque définition, à expliquer pourquoi une nouvelle notion est introduite et, après chaque théorème, à expliquer ce à quoi il sert en pratique.

1.3.1 Motivation et enjeux

Motiver un problème consiste à expliquer pourquoi il est intéressant de l'étudier. Ses enjeux sont les bénéfices que l'on espère pouvoir tirer de sa résolution.

Exemple. *Soit le problème consistant à déterminer les facteurs premiers de l'entier dont l'expression en Base64 est :*

```
LHsoNUk1uuRUP+ciupo2jZcnUFVkKSUw5JqlP8GBauGGVN64e3gKzwtbZ
dfxCE9nUhxIeCAdmd6R5XNT7mZ6EChDUQQLWXVdkRzTqjD1iM+BuogzOH
QKHLh1Pz2NXr+gOPDd2G9PYDJYgsZX5G8V5uYfsn9AcfnW+1sW7vLSXBM
```

On peut le motiver en invoquant l'importance tant théorique que pratique du problème de la factorisation : savoir décomposer explicitement un entier en facteurs premiers signifie maîtriser la structure multiplicative de $\mathbb{Z}$; la taille de l'entier ci-dessus est à la frontière de ce que les techniques actuelles savent traiter et demande donc qu'on les améliorent.

Parmi ses nombreux enjeux, on peut citer une meilleure évaluation de la sécurité fournie par les cryptosystèmes de type RSA, ainsi que de nombreuses applications en théorie des nombres qui bénéficieront directement des techniques développées pour achever cette factorisation.

Exercice. *Motiver et décrire les enjeux du problème consistant à résoudre symboliquement les équations différentielles linéaires du premier ordre.*

1.3.2 État de l'art

L'état de l'art est la frontière des connaissances actuelles dans un domaine donné, c'est-à-dire l'ensemble des théorèmes les plus précis connus actuellement. Le présenter succinctement permet de montrer en quoi notre contribution fait avancer la science.

Exercice. *Soit comme problème l'énumération des groupes finis d'ordre n, pour un entier n donné.*
Donner, à votre propre niveau, l'état de l'art concernant ce problème.

1.3.3 Difficulté et originalité

Expliquer la difficulté d'un problème revient à justifier qu'aucune résolution n'ait encore vue le jour. Parallèlement, il convient de discuter de l'originalité des moyens que mets en œuvre la contribution pour le résoudre : s'agit il de bêtes calculs, ou y a-t-il quelque chose d'intrinsèquement intéressant à retenir de ces moyens ?

Exercice. *Soit le résultat et sa preuve suivante.*

Théorème. *Dans le cas $n = 2$, l'équation de Fermat $x^n + y^n = z^n$ admet une infinité de solution.*

Démonstration. Un simple calcul permet de vérifier que, pour tout couple d'entiers (n, m), le triplet $(x, y, z) = (m^2 - n^2, 2mn, m^2 + n^2)$ est solution. Cette équation admet donc une infinité de solution. □

Discuter de la difficulté qu'avait ce problème a priori ; que dire de l'originalité de sa résolution ?

1.3.4 Diffusion et impact

La diffusion d'une contribution est l'ensemble des moyens par lesquels ses auteurs en ont fait part tant aux autres spécialistes du domaine qu'à la communauté scientifique dans son ensemble, voire même au grand public ; typiquement, il s'agit de :

— un article de recherche, publié dans une revue renommée ;
— des exposés de recherche, donnés à l'occasion de séminaires ou conférences ;
— des travaux de vulgarisation (textes dans des magazines grands publics, présentations télévisées, etc.) ;
— du transfert industriel (dépôt de brevet, conception de logiciel, etc.).

L'impact d'une contribution est la réaction de ces communautés à sa diffusion. Les indicateurs classiques consistent en le nombre de citations de l'article ainsi qu'en les utilisations éventuelles que d'autres travaux en on fait.

Exercice. *Que pouvez-vous dire de la diffusion et de l'impact du résultat ci-dessous ?*

Théorème (Appel-Haken, 1976). *Quatre couleurs suffisent à colorier les sommets de tout graphe planaire de sorte qu'aucun couple de sommets adjacents n'aient la même couleur.*

Chapitre 2

Démarches

Le chapitre précédant avait pour but de vous donner une vague idée de la manière dont les chercheurs perçoivent les mathématiques et les communiquent. Bien évidemment, la vraie recherche reste l'obtention de résultats qui font avancer l'état de l'art. Ce chapitre va présenter plusieurs démarches générales que les chercheurs peuvent mettre en œuvre pour attaquer un problème donné.

2.1 Cadre expérimental

Aussi pompeusement appelée « démarche scientifique », c'est la manière canonique d'aborder essentiellement tout problème de sciences expérimentales. Elle est peu pertinente en sciences formelles, c'est-à-dire en mathématiques, informatique et physique théorique.

Face à un phénomène à étudier, cette démarche consiste en les étapes suivantes :

1. Identifier une problématique.
2. Formuler une hypothèse.
3. Élaborer un protocole expérimental.
4. Analyser les données recueillies.
5. Vérifier ou non l'hypothèse.

Les trois premières étapes demandent une certaine connaissance du domaine concerné, notamment afin d'identifier les variables du problème, leurs interactions, etc. Les deux dernières nécessitent quant à elles une bonne maîtrise des outils statistiques qui, mal utilisés comme ils le sont si souvent, mènent trop facilement à des erreurs d'interprétation.

Cette méthode est parfois employée dans certains domaines des mathématiques se prêtant à l'expérimentation. Naturellement, elle n'est pas rigoureuse : toute conclusions auxquelles elle mènerait devra idéalement être ensuite prouvée formellement.

Exercice. *Soit comme problème le calcul de la somme $\sum_{k=1}^{n} k^2$; on suit l'approche suivante :*

1. *Prenons ici comme problématique le calcul d'une expression close en n pour cette somme.*
2. *Quelle forme pensez vous que cette expression puisse prendre ?*
3. *Comment alors pourrait-on la calculer explicitement ?*
4. *Faisons le donc...*
5. *L'expression obtenue est-elle correcte ?*

2.2 Cadre mathématique

Par essence, la recherche en mathématiques ou tout autre discipline théorique ne peut être réduite à une démarche aussi simple que celle décrite ci-dessus. Cependant, une bonne première approche consiste à « épurer » chaque problème de recherche de la manière suivante :

1. Formuler le problème rigoureusement.
2. Le généraliser jusqu'à ce qu'il ne soit plus artificiel.
3. Le résoudre dans les cas particuliers les plus généraux possibles.
4. Identifier ce qui entrave une résolution complètement générale.

C'est alors sur cette obstruction que doivent porter les efforts du chercheur ; typiquement, elle est résolue en adaptant ou en combinant des techniques issues d'autres domaines des mathématiques.

Exercice. *Combien le polynôme $X^3 + 1$ a-t-il de racines dans le corps à 2^3 éléments ?*

Exercice. *Pour quels sous-ensembles $S \subset \{1, \dots, n\}$ la partie $\{M : \mathrm{rg}(M) \in S\} \subset \mathrm{Mat}_n(\mathbb{R})$ est-elle connexe par arc ?*

Exercice. *Étant donné n, comment calculer x tel que $2^x = 3 \bmod n$?*

Les exercices ci-dessus devraient vous rappeler de nombreuses notions et résultats vus en licence ; de la même façon, pour attaquer un problème efficacement, un chercheur doit d'abord bien connaître les résultats classiques des domaines connexes à ce problème, voire même idéalement bien au delà. C'est aussi pour cela qu'on fait rarement de la recherche en mathématiques avant la thèse.

Chapitre 3

Outils

3.1 Collaborations

Le plus important en recherche.
Interactif.
Les idées de chacun mises bout à bout résolvent le problème.

3.2 Exposés

Relatent des résultats à chaud pour spécialistes.
Interactif aussi.
Retour : peut susciter des collaborations.

3.3 Articles

Une fois proprement écrit, surtout pour les spécialistes.
Processus de relecture peut aussi susciter des collaborations dans une moindre mesure.

3.4 Cours

Organisé en un tout cohérent.
Devient accessible à un public plus large.

3.5 Livres

Rédigé de manière propre.
Le plus accessible qu'il soit.
Vous, enseignants, vous servirez surtout des deux derniers : les cours que vous avez suivis, et les ouvrages de référence.

Chapitre 4

L'outil informatique

L'outil informatique, c'est l'ordinateur ; chaque logiciel n'est qu'une manière différente de lui poser des questions. Pour bien savoir lui parler, il faut penser en termes effectifs. Pour cela, si votre objectif est de faire calculer x_n à un ordinateur, commencez par calculer vous-même à la main une quantité très simple x_0, puis un quantité simple x_1 et continuez ainsi jusqu'à ce que cela devienne machinal ; vous êtes alors prêt à expliquer le calcul de x_n à une machine.

Cette démarche s'applique à tous les logiciels ci-dessous. Nous commencerons par Maple (logiciel du même tenant que Sage), le plus général. Nous verrons ensuite deux autres logiciels plus particuliers, l'un permettant de bien illustrer les problèmes de géométrie, l'autre permettant d'extraire des statistiques.

Pour chacun, nous mettrons en avant leur application aux épreuves orales du concours.

4.1 Utilité

4.1.1 Calculs

Permet d'effectuer de longs calculs sans effort. Intérêt nul en enseignement.

Exercice. *Que vaut la quantité* $\int_0^\infty e^{-x^2}\,dx$ *?*

4.1.2 Expérimentation

petits calculs pour voir ce qui se passe, conjecturer un comportement, etc.
faire jouer les élèves avec un curseur pour mettre en évidence un comportement

Exercice. *Combien le polynôme* $X^p + 1$ *a-t-il de racines dans le corps à* 2^p *éléments ?*

Exercice. *Étant donné n, comment calculer* x *tel que* $2^x = 3 \bmod n$ *?*

Voir aussi `http://mathoverflow.net/questions/178139/examples-of-unexpected-mathematical-ima`

4.1.3 Records

gros calculs, pour : - montrer que votre conjecture/théorème est vérifié pour n très grand - prouver l'efficacité pratique de votre algorithme

4.1.4 Illustrations

dessins propres, animations, etc.

Exercice. *La fonction de Fabius* [1] *est* $\mathscr{C}^\infty(\mathbb{R},\mathbb{R})$ *mais nulle part analytique ; c'est la limite de la suite :*

$$f_0(x) = 1$$
$$f_{n+1}(x) = \int_0^{2x} f_n(t)dt$$

Dessiner cette fonction.

Voir aussi `http://math.stackexchange.com/questions/733754/visually-stunning-math-concepts-w`

4.2 Logiciels

— AlgoBox : programmation impérative pour les bébés
— ClassPad Manager : émulateur calculette
— Geogebra : algèbre et géométrie interactive
— Geoplan : géométrie planaire
— Geospace : géométrie spatiale
— Maxima : équivalent Maple
— OpenOffice.org : tableur
— Python : comme Sage sans Sage...
— Scilab : algèbre et analyse numériques.
— TI-NSpire CAS TE : émulateur calculette
— TI-SmartView 83 Plus.fr : émulateur calculette
— Xcas : Maple grenoblois

4.3 Algèbre avec ???

Développements informatiques :
— séries de Fourier : décomposition d'un signal en digital et reconstitution
— équations différentielles : implantation et comparaison de solveurs Euler/RK...
— nombre premiers : test de Miller-Rabin, méthodes de factorisation
— techniques de calcul d'intégrales : méthodes numériques

Leçons "exemples" :
— exemples d'algorithmes ;
— exemples d'utilisation d'un tableur ;
— exemples d'utilisation d'un logiciel de calcul formel.

Il ne faut pas que des exemples mais un fil conducteur ! Dans le cas des algorithmes, on peut présenter deux grandes familles d'agorithmes (notamment diviser-pour-reigner et gourmand) et différentes applications de chaque philosophie...

4.4 Géométrie avec GeoGebra

1. Voir `http://www.madore.org/~david/weblog/2014-09.html#d.2014-09-15.2223`.

Bibliographie

[1] Gaetan Bisson et Andrew V. Sutherland.
"Computing the endomorphism ring of an ordinary elliptic curve over a finite field".
In : *Journal of Number Theory* 131.5 (2011) : *Elliptic Curve Cryptography*. Sous la direction de Neal Koblitz et Victor S. Miller, pages 815-831.
doi : 10.1016/j.jnt.2009.11.003.

[2] Matt Might. *The Illustrated Guide to a Ph.D.* 2010.
url : http://matt.might.net/articles/phd-school-in-pictures/.