Chercheur en maths : quel métier bizarre !

Chimène Sivak et Stéphane Fischler
Université Paris-Sud
Janvier 2005

Plan de l'exposé

1. Formations et débouchés
2. La recherche
3. Quelques idées reçues
4. Un peu de mathématiques…

1. Formation et débouchés

- Les études de maths
- Les métiers des maths
  - L'enseignement
  - La recherche

Les études de maths

Etudes

Premier cycle

- Université :

  DEUG (filière non sélective)
- Classes préparatoires.

Etudes

Deuxième cycle

- Université :

  Licence et Maîtrise.
- Grandes écoles :
  - E.N.S. : pour recherche et enseignement.
  - Ecole Polytechnique : généraliste.
  - Mines, Ponts, Centrale, … : ingénieur.
- CAPES, Agrégation (concours).

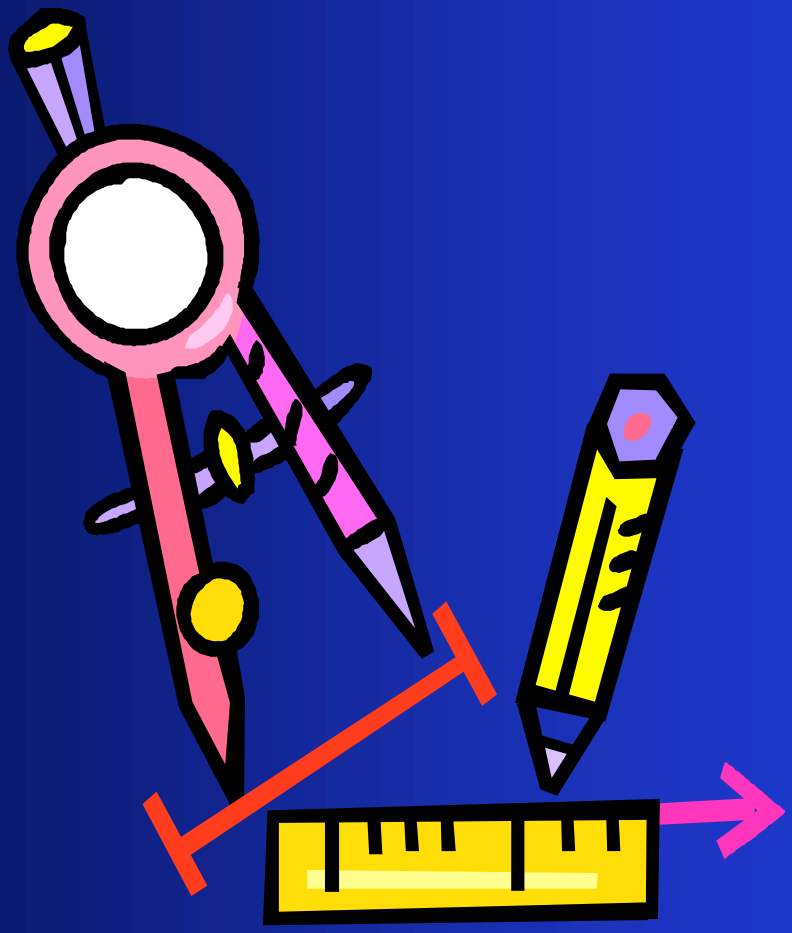
Etudes

Troisième cycle

- D.E.A.

  Université et/ou Grandes écoles.
- Thèse (3 ans) :
  - Université (peut être couplé à de l'enseignement en premier cycle).
  - Grandes écoles.
  - Entreprise.

Les métiers des maths



Métiers

L'enseignement

- Collège, Lycée.
- Classes préparatoires.
- Grandes écoles.
- Université :
  - Cours en amphithéâtre : 100 étudiants.
  - Séances d'exercices (T.D.) : 25 étudiants.

Métiers

La recherche

- Organismes publics de recherche :
  CNRS, INRIA, INSERM …
- Universités :
  Enseignants-chercheurs.
- Entreprises privées :
  Recherche appliquée.

2. La recherche

- Qu'est-ce que la recherche ?
- Résoudre un problème
- La place de l'ordinateur
- « Il n'y a plus rien à trouver… »
- Les difficultés
- En France…
- Notre quotidien

La recherche

Qu’est-ce que la recherche ?

- Se poser des questions.
- Résoudre le problème posé.
- Trouver des relations avec d’autres problèmes…

Ce qui revient à se poser d’autres questions!

- Rédiger, publier et communiquer ses résultats.

Résoudre un problème

- D'abord résoudre un cas particulier :
  - Faire des essais dans un cas simple.
  - En tirer une méthode pour un cas plus général.
- Puis généraliser.
- Savoir rebrousser chemin si on est dans une impasse !

La place de l'ordinateur

- Outil indispensable :
  - Rédaction des articles.
  - Communication : email, internet.
  - Calcul numérique ou formel.
- Mais ne remplace pas l'homme :
  - Incapable de réfléchir, d'avoir des idées…
  - Un calcul n'est pas une démonstration !

La recherche

« Il n'y a plus rien à trouver… »

- Plus de théorèmes depuis 1945 qu'avant.
- Il reste des questions anciennes non résolues.
- Et les avancées posent beaucoup de nouvelles questions !

Les difficultés

- Peu de femmes.
- Compétitif.
- Nécessite vraie motivation ; métier-passion.
- Problème de communication avec le grand public :
  - Contenu inaccessible.
  - Intérêt difficile à partager.

En France…

- Emploi permanent, mais pas bien payé.
  - 9 années d'études.
  - Salaire à l'embauche : 1800 EUR environ.
  - Avantage : beaucoup d'autonomie.
- Recherche de très haut niveau :
  - 8 Médaillés Fields.
  - Nombreuses revues françaises.
  - Nombreux articles en français.

Notre quotidien

- Enseignement :
  - 6 h/semaine de T.D.
  - Préparation des exercices et des devoirs.
  - Correction des copies.
- Recherche :
  - 1 ou 2 exposé(s) par semaine (1 heure).
  - Congrès (quelques semaines par an).
  - Travail de recherche proprement dit.
- Autres :
  - Vulgarisation, Math en Jeans, …
  - Organisation de conférences, …

3. Quelques idées reçues

- Solitaire
- Coupé du monde
- Peu de moyens

Solitaire ?

Solitaire ?

Oui :

- La recherche en mathématiques, c'est avant tout un travail personnel.

Exemples:

- Réfléchir par soi-même.
- Trouver de nouvelles idées.
- Apprendre de nouvelles choses.
- Se tenir au courant des avancées.

Solitaire ?

Non :

- Mise en commun des résultats.

Exemples:

- Séminaires hebdomadaires.
- Congrès, colloques (nationaux ou internationaux).

- Travail en équipe.

Exemples:

- Collaborations : chacun apporte ses idées et son savoir.
- Groupes de travail (on étudie en groupe).

Coupé du monde ?

Coupé du monde ?

Oui :

- Peu de gens comprennent !

Pour un article moyen, dans le monde :

- 10 personnes comprennent vraiment tous les détails.
- 100 personnes comprennent les idées principales.
- 1000 personnes comprennent l'intérêt des résultats.

- Pas beaucoup d'applications :

Intérêt théorique avant tout.

Coupé du monde ?

Non :

- Applications à d'autres sciences.

Exemples:

- Physique théorique : relativité, atomistique.
- Informatique : compression d'images (JPEG).

- Applications industrielles.

Exemples:

- Codes correcteurs d'erreurs ; cryptographie.
- Recherche de puits de pétrole.
- Lutte contre les avalanches.

Peu de moyens ?

Peu de moyens ?

Oui :

- Peu de moyens pour la recherche fondamentale.

Exemples :

- Peu de postes.
- Peu d'argent pour les missions, le matériel et la bibliothèque.
- Pas assez de personnel d'encadrement.

Peu de moyens ?

Non :

- Moins grave en maths que dans les autres disciplines.

Exemples:

- Biologie, Chimie, Physique : besoin de matériel très coûteux.
- Mathématiques fondamentales : « il nous suffit d'un papier et d'un crayon ! »

4. Un peu de mathématiques…

- Le théorème de Fermat
- Le code R.S.A.
- Le problème de Syracuse

Le théorème de Fermat (1636)

Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere.

Fermat

Le théorème de Fermat (1636 - 1994)

Il n'existe pas d'entiers positifs non nuls x,y,z tels que

$$x^n + y^n = z^n$$

avec $n \geq 3$.

Fermat

Pour n=2…

L'équation

$$x^2 + y^2 = z^2$$

a une infinité de solutions entières :

$$3^2 + 4^2 = 5^2$$

$$12^2 + 5^2 = 13^2$$

…

Fermat

Stratégie de preuve (1)

Si $x^n + y^n = z^n$, on considère l'équation

$$A^2 = B\,(B - x^n)\,(B + y^n)$$

qui est celle d'une

« courbe elliptique »

avec des propriétés bien particulières…

Stratégie de preuve (2)

…tellement particulières qu'elle ne peut pas être *modulaire*.

Or Wiles a démontré (sous certaines hypothèses) que *toute courbe elliptique est modulaire* : c'est la conjecture de **Taniyama-Weil**.

Le code R.S.A.

Inventé par **Rivest, Shamir et Adleman en 1977.**

Utilisé pour transmettre des données confidentielles sans que personne ne puisse les déchiffrer.

R.S.A.

Codage

Message à envoyer : bonjour

Message codé : 02 15 14 10 15 21 18

Le problème est maintenant de crypter cette suite de chiffres…

R.S.A.

Clef publique / Clef privée

Une clef *publique* : permet à n'importe qui de pouvoir crypter un message.

Une clef *privée* : permet seulement à **une** personne de décrypter les messages.

R.S.A.

Problème

Personne ne doit pouvoir deviner quelle est la clef privée !

R.S.A.

Solution

Nombres *privés* : deux grands nombres premiers **p** et **q**.

Nombre *public* : le produit **pq**.

Justification : factoriser, c'est très long !

R.S.A.

Congruences

On note

$$\mathbf{a \equiv b \pmod{N}}$$

si a-b est multiple de N.

Exemple : $26 \equiv 5 \pmod{7}$

R.S.A.

Choix des clefs

p = 11, **q** = 23 *privés*

N = **pq** = 11*23 = 253 *public*

N' = (**p**-1)(**q**-1) = 10*22 = 220 *privé*

Clef *privée* : D = 27 choisie

Clef *publique* : E = 163 calculée pour que D*E ≡ 1 (mod N')

R.S.A.

Cryptage de 02

Cryptage : $2^{163} \equiv 52 \pmod{253}$

Le message crypté est 52.

Décryptage : $52^{27} \equiv 2 \pmod{253}$

Le message décrypté est 2.

Publics : 163, 253. *Privé* : 27.

R.S.A.

Exemple

Message *initial* : bonjour

Message *codé* : 02/15/14/10/15/21/18

Message *crypté* :

52/152/159/43/152/109/35

Problème de Syracuse

Partons d'un entier n :

- Si n est pair, on le divise par 2.
- Si n est impair, on le multiplie par 3 et on ajoute 1.

On recommence ce procédé…

Syracuse

Conjecture

En recommençant suffisamment de fois,
on finit toujours par arriver à 1.

Syracuse

Exemples

- 7 → 22 → 11 → 34 → 17 → 52 → 26
  → 13 → 40 → 20 → 10 → 5 → 16
  → 8 → 4 → 2 → 1
- 3 → 10 → 5 → 16 → 8 → 4 → 2 → 1

Légende :

→ on multiplie par 3 et on ajoute 1

→ on divise par 2

Maintenant, c'est à vous de chercher…