

MATHEMATIQUES SUR ORDINATEUR

par

D. Lazard

(Université Paris VI et GRECO de Calcul Formel)

Il est universellement connu que les ordinateurs ont ouvert des possibilités immenses au calcul scientifique. Pendant longtemps, ces possibilités se sont limitées au maniement des nombres (réels approchés), et cela a provoqué un développement rapide de l'analyse numérique, qui est la théorie de ces calculs approchés.

Il est beaucoup moins connu que les ordinateurs peuvent également manipuler les concepts abstraits des diverses branches mathématiques. Ceci fournit un outil inestimable à la recherche en permettant une expérimentation impossible à la main.

Mais là ne se limite pas l'influence des ordinateurs sur les mathématiques ; il est facile de donner des exemples de théorèmes dont une partie de la démonstration est constituée de calculs sur ordinateurs (théorème des quatre couleurs, classification des groupes finis, problème de Waring, ...). L'objet de cette table ronde est d'illustrer un autre aspect de l'interaction entre les mathématiques et l'informatique, qui a déjà une grande influence sur la recherche en mathématique et semble devoir modifier profondément les questions étudiées, même dans les domaines les plus classiques.

La puissance des ordinateurs ne permet pas d'assurer la faisabilité des calculs souhaités en un temps acceptable. Il faut élaborer des méthodes puissantes dont la mise au point passe par la démonstration de théorèmes nouveaux, souvent intéressants indépendamment de leurs applications au calcul.

Ainsi apparaît une interaction extrêmement riche entre la théorie mathématique, l'expérimentation et la programmation. Pour l'illustrer, nous avons choisi quatre domaines particulièrement représentatifs :

La géométrie algébrique (M. Demazure)
 La topologie algébrique (F. Sergeraert)
 Les équations différentielles (J.P. Ramis)
 La théorie des nombres (J.L. Nicolas).

I. MATHEMATIQUES SUR ORDINATEUR par M. Demazure (Ecole Polytechnique).

Constatation : Les mathématiciens "classiques" sont très mal à l'aise lorsqu'il s'agit de parler d'algorithmes. Certaines démonstrations, qui consistent en fin de compte à exhiber un algorithme, vérifier sa correction et démontrer sa convergence, sont rédigées de façon incompréhensible et inutilement compliquée, faute des concepts et du langage nécessaires. En particulier, sont très mal compris des mathématiciens : la différence entre syntaxe et sémantique (sauf pour les logiciens) et le contrôle "implicite" des algorithmes (récursivité, etc...). Classiquement, un mathématicien a beaucoup de peine à programmer récursivement, ou fonctionnellement, ou en style objet ; beaucoup ne dépassent pas le stade du BASIC, car ils sont mal à l'aise dès que la convergence des algorithmes n'est pas explicite dans les algorithmes eux-mêmes. Corrélativement, les cours de maths ne comprennent pas les énoncés basiques et universellement utiles qui permettent de maîtriser ces situations (théorème de König, théorème du point fixe dans les treillis, etc...), ni les rudiments sur les structures de données de base (arbres,...).

Une nouvelle espèce de mathématiciens : "Classiquement" encore, les mathématiciens se divisent en "purs" et "appliqués", les uns ayant plutôt des rapports avec la physique, les autres avec les sciences de l'ingénieur. En fait, on constate que l'univers mathématique est en train de se diviser en trois, trois cultures, trois langages, trois communautés : ceux qui respectivement se sentent bien avec

- . les physiciens théoriciens : analyse, géométrie, ... ex "mathématiciens purs"
- . les mécaniciens : analyse numérique, ... ex "mathématiciens appliqués"
- . les informaticiens : logique, arithmétique, ... nouvelle *race*.

Un test : la différence entre syntaxe et sémantique, suffit à départager cette nouvelle catégorie des autres.

Il me semble que, dorénavant, la frontière ne passe plus entre les mathématiques et le reste des sciences, mais à l'intérieur des mathématiques elles-mêmes.

11. MATHEMATIQUES, INFORMATIQUE, ANALYSE NON STANDARD ET AXIOMATIQUES par Francis Sergeraert (Institut Fourier, Université de Grenoble)

Je voudrais rapprocher la situation du mathématicien utilisant l'informatique comme outil de travail par rapport à ses confrères "ordinaires", de celle du mathématicien ordinaire par rapport aux utilisateurs de "l'Analyse Non Standard". Pour abrégé la rédaction, j'utiliserai, de façon tout à fait impropre mais ce sera commode, les dénominations respectives de "informaticien", "mathématicien", et "non-standardiste".

Il s'agit donc d'expliquer ici une sorte d'égalité :

$$\frac{\text{informaticien}}{\text{mathématicien}} = \frac{\text{mathématicien}}{\text{non-standardiste}}$$

1. Analyse du rapport mathématicien/non-standardiste

Le champ d'étude du non-standardiste, est légèrement élargi par rapport à celui du mathématicien, par extension de l'axiomatique utilisable. Le travail d'extension du système de Zermelo-Fraenkel, l'axiomatique usuelle du mathématicien, fut d'abord entrepris par le logicien Robinson [RBN], puis mis sous une forme à l'esthétique fort réussie par Nelson [NLS] ; son efficacité pratique n'est plus à démontrer.

La situation respective des mathématiciens et des non-standardistes est idéale ; il est en effet démontré (voir [NLS]) que les deux axiomatiques sont essentiellement équivalentes, au sens suivant : Tout résultat démontré par le mathématicien peut aussi, trivialement, être démontré par le non-standardiste ; inversement, par un procédé entièrement "automatique", tout énoncé et toute démonstration du non-standardiste peuvent être transformés en un énoncé et une démonstration acceptables par le mathématicien. Noter au passage que le fait que le "procédé" soit "automatique" relève de la compétence de l'informaticien ...

Cette situation est très saine : mathématiciens et non-standardistes croient au même Dieu ; les rites de leurs religions respectives sont seulement un peu différents, mais qu'importe, la nature n'en est que plus riche ; on espère seulement que cette situation est suffisamment bien comprise par les fanatiques des deux religions pour éviter la seule ombre au tableau : qui dit religion dit souvent guerre de religion.

2. Analyse du **rapport informaticien/mathématicien**

Je voudrais expliquer que la situation est, ou plutôt devrait être, analogue entre informaticiens et mathématiciens.

L'informaticien travaille dans une axiomatique sensiblement plus stricte que celle du mathématicien. La description de ce qu'il faut enlever au système de Zermelo-Fraenkel est fort difficile, et la situation à ce sujet ne semble pas assez mûre pour qu'il soit possible de donner des références aussi commodes et communément admises pour l'axiomatique de l'informaticien, que la référence Bourbaki pour le mathématicien, ou Nelson pour le non-standardiste.

Bien sûr, on peut citer tous les textes sur la calculabilité, la définition des fonctions récursives, etc. Voir par exemple [CHR], [AHU] et [TRL]. Mais ce qui est décrit dans ces textes n'est autre qu'un nouveau "terme" de la théorie des ensembles, le terme "machine" ou "ensemble des fonctions récursives", ainsi que l'axiomatique à adopter pour y travailler commodément. C'est déjà très agréable de pouvoir disposer de telles constructions, mais je veux dire pourquoi la situation n'est pas encore idéale, c'est-à-dire comparable à celle des mathématiciens par rapport aux non-standardistes.

Il n'est pas si facile d'isoler la difficulté à laquelle je fais allusion, et pour ce faire, je vais utiliser un exemple cité dans le remarquable article sur Kronecker dû à H. Edwards [EDW].

3. Les décimales d'un **nombre réel**

Edwards décrit les relations épineuses entre Kronecker et Weierstrass à l'université de Berlin pendant le siècle dernier. Weierstrass utilisait allègrement une axiomatique à la Cantor, qui révélsait Kronecker. Ce dernier ne voulait pas entendre parler du développement décimal d'un nombre réel, puisque ce développement nécessite une infinité de décimales, mais seulement d'un algorithme (en utilisant le langage maintenant usuel) capable de donner la n -ième décimale de ce réel.

Autrement dit Kronecker ne voulait considérer que les réels récursifs. Ces "réels" posent des problèmes fort intéressants qui, à ma connaissance, n'ont pas encore été examinés. Considérons par exemple la démonstration par Cantor de l'existence de nombres transcendants, par simple examen des cardinaux de l'ensemble des nombres

algébriques et de l'ensemble des nombres réels. Pour un disciple de Kronecker, cette argumentation est une hérésie, et il verra le problème d'une autre façon. Soit \mathbf{R}_{rec} l'ensemble des réels récurrents ; c'est un ensemble dénombrable et l'argument de Cantor ne fonctionne donc plus.

Le problème pourrait être présenté de la façon suivante : existe-t-il une mesure sur \mathbf{R}_{rec} , "naturelle", donc entre autres invariante par translation, telle que l'ensemble des réels algébriques soit de mesure nulle ? Mais la question est encore mal posée : notre ensemble est dénombrable, et si notre mesure est invariante par translation, ce ne peut être que la mesure nulle !

Il faut donc dire : quelle est la "bonne" notion de "mesure" sur \mathbf{R}_{rec} donnant la traduction à un disciple de Kronecker du phénomène de Cantor ? On voit que décidément il y a un travail tout à fait non négligeable à faire.

4. Existe-t-il une axiomatique **pour** l'informaticien ?

Dès lors, on aimerait bien pouvoir disposer d'une axiomatique de l'informaticien (baptisons-la AXINFO), sous-ensemble de Zermelo-Fraenkel, essentiellement équivalente au système de Zermelo-Fraenkel au même sens que plus haut : tout résultat obtenu dans Zermelo-Fraenkel devrait pouvoir être "automatiquement" transformé en un résultat dans AXINFO. Par exemple le résultat de Cantor sur les nombres transcendants pourrait peut-être, pourquoi ne pas rêver, être ainsi transformé en un résultat de complexité sur la calculabilité des réels récurrents, énoncé du genre : "presque tout" réel récurrent a un indice de complexité $\leq C$, mais l'indice de complexité des réels algébriques est $\leq C$.

On voit qu'on est fort loin d'un tel état de la science ; il est pourtant tout à fait raisonnable de demander une telle axiomatique, plus proche de la réalité que celle de Zermelo-Fraenkel. Les résultats des mathématiciens utilisant sans complexes les axiomes du choix, de l'infini, ... ne seraient dès lors que des raccourcis fulgurants et élégants de phénomènes très concrets de la réalité des informaticiens, qu'on pourrait d'ailleurs au besoin retrouver par un processus de réduction automatique. Le résultat de cette traduction serait souvent beaucoup moins élégant que la version originale chez Zermelo-Fraenkel ; de même que, par exemple, la traduction en

Zermelo-Fraenkel des magnifiques résultats sur les canards obtenus par l'Ecole Strasbourgeoise est certainement si indigeste qu'elle n'a jamais été faite !

Il y a pourtant ici une différence entre ce qui se passe entre mathématiciens et informaticiens, d'une part, et entre mathématiciens et non-standardistes, d'autre part. Les mathématiciens et les non-standardistes travaillent dans des mondes également abstraits, alors que l'informaticien travaille dans un monde sensiblement plus concret, si bien que les traductions indigestes de Zermelo-Fraenkel vers AXINFO pourraient peut-être avoir des retombées pratiques à ne pas négliger.

5. Vous avez dit indigeste ?

Mais après tout, peut-on être si certain que les traductions des textes de mathématiciens en textes d'informaticiens ne produiront que des énoncés indigestes ?

La citation suivante de Hensel [EDW] au sujet de la philosophie de Kronecker est un peu longue, mais convient tellement à notre sujet :

"Je dois aussi souligner une règle que Kronecker s'est consciencieusement imposée au sujet des définitions et démonstrations d'arithmétique générale ; son strict respect distingue son traitement de la théorie des nombres et de l'algèbre de presque tous les autres. Il croyait qu'on pouvait, et qu'on devait, dans ces parties des mathématiques, organiser chaque définition de telle façon qu'on puisse tester en un nombre fini d'étapes si elle s'applique à n'importe quel objet donné. Dans le même esprit, une démonstration d'existence ne peut être considérée comme rigoureuse que si elle contient une méthode permettant de construire l'objet dont l'existence est démontrée. Kronecker était loin d'écarter définitivement définitions et démonstrations qui ne répondaient pas à ces critères, mais il pensait que dans de telles situations, quelque chose manquait, que combler cette lacune était important, et que de la sorte des nouveautés essentielles pouvaient être découvertes. De plus, il croyait qu'une formulation rigoureuse de ce point de vue prendrait en général une forme plus simple qu'une autre ne satisfaisant pas ces exigences ; dans ses cours, il en a donné de nombreux exemples, très probants."

Bref, Kronecker croyait très fermement que faire des mathématiques effectives, pour employer un mot à la mode, pouvait

non seulement nous rapprocher d'une réalité concrète et utile, mais que le résultat net de cette ambition pourrait se révéler plus simple et plus élégant. L'exemple que j'ai décrit ailleurs de la version "homologie effective" de la suite spectrale de Serre [SRG], beaucoup plus simple à décrire que la version originale, bien que satisfaisant parfaitement l'exigence de Kronecker, est caractéristique d'une telle situation. Il est tout à fait clair que si l'on pouvait ressusciter aujourd'hui Kronecker et Weierstrass et réarbitrer leur débat dans l'environnement d'aujourd'hui, le résultat ne serait sans doute pas le même.

6. En guise de conclusion

Il s'agit dans le cadre de ce Colloque d'organiser au mieux la suite de nos aventures de mathématiciens (au sens large) ; dans le domaine que je connais bien, celui qui consiste à réfléchir à la topologie algébrique "effective", je ne peux qu'être très frappé par la géniale profondeur de vue de Kronecker ; autrement dit, pour penser utilement à l'an 2000, il ne faut peut-être pas négliger ce qui nous a été conseillé dès 1860 !

L'unification résultant du travail de Nelson me paraît par ailleurs exemplaire : les relations mathématiques entre Kronecker et Weierstrass furent si tendues qu'elles finirent par détruire une belle amitié ; quel dommage ! Or, on constate très (trop) souvent aujourd'hui des phénomènes analogues entre "informaticiens" et "mathématiciens" (au sens de l'introduction). Nelson, par la définition de son axiomatique, a merveilleusement réussi à réconcilier les croyants en Zermelo- Fraenkel et les adeptes de la religion Robinson, au moins ceux qui ne sont pas définitivement pathologiques. Qui saura de la même façon réconcilier informaticiens et mathématiciens ?

REFERENCES

- [AHU] Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman : The design and analysis of computer algorithms, Addison-Wesley, 1974.
- [CHR] Alonzo Church : The calculi of lambda-conversion, Princeton University Press, 1941.
- [EDW] Harold M. Edwards : An appreciation of Kronecker, The mathematical Intelligencer, 9 (1987), 28-35.

- [NLS] Edward Nelson : Internal set theory : a new approach to nonstandard analysis, Bull. A.M.S., 83 (1977), 1165-1198.
- [RBN] Abraham Robinson : Non-standard analysis, 2nd ed., American Elsevier, New York, 1974.
- [SRG] Francis Sergeraert : Homologie effective, C.R. Acad. Sci. Sér. I Math, 304 (1987), 279-282 et 319-321.
- [TRL] George J. Tourlakis : Computability, Reston, 1984.

m. UN LOGICIEL POUR LA RESOLUTION DES EQUATIONS DIFFERENTIELLES ORDINAIRES DANS LE CHAMP COMPLEXE - "LE CODE DESIR"

Les auteurs : DESIR est le résultat des efforts de deux équipes :

A Grenoble l'équipe de J. Delladora : E. Tournier, C. Dicrecenzo, D. Duval, A. Hillali.

A Strasbourg l'équipe de J.P. Ramis : A. Duval, J. Thomann, F. Richard.

Les équations différentielles dans le champ complexe ont été très étudiées au XIX^{ème} siècle : travaux de Gauss, Riemann, Poincaré, Picard, Klein, Fuchs, Schlessinger, ... et au début du XX^{ème} : Birkhoff, Dulac, etc. Le sujet est ensuite entré en sommeil jusque vers 1970. Il a été récemment repris avec succès par divers auteurs : Deligne, Sibuta, Malgrange, Gérard, Levelt, Ramis. Parmi les nouveaux progrès les plus notables figure la "*Théorie des invariants*" : il s'agit de *classifier* les équations différentielles modulo divers *changements de variables* "naturels" (algébriques, analytiques : i.e. séries convergentes ou fonctions holomorphes). La première étape d'une telle classification est la "*classification formelle*" : on ne se préoccupe pas de la convergence des objets obtenus.

Le nouvel éclairage ainsi jeté sur la théorie (et dû en grande partie à des outils modernes et sophistiqués forgés dans d'autres domaines : Géométrie Algébrique et Analytique, Topologie, Arithmétique, Théorie des Groupes) a permis aussi de *renouveler et approfondir les divers algorithmes de calcul* dont on disposait. D'où l'idée que quelques uns d'entre nous ont eue vers 1980 d'utiliser ces progrès pour créer un "*Solver d'équations différentielles ordinaires*".

L'enjeu était *double* :

1°/ Fournir un *outil puissant au "mathématicien pur"* : calcul des invariants, allure des solutions d'équation éventuellement assez compliquées,... lui permettant un "travail expérimental" sur le sujet.

2°/ Créer un *logiciel utilisable par un "public" assez varié* : scientifiques (physiciens, chimistes), ingénieurs, etc.

Le problème

On veut "*résoudre*" des *équations différentielles linéaires* :

$$a_n(x) y^{(n)} + a_{n-1}(x) y^{(n-1)} + \dots + a_0(x) = 0,$$

où x est une variable complexe, y une fonction inconnue et les a_n, \dots, a_0 , des polynômes (ou plus généralement des fonctions holomorphes).

On s'est (d'abord) limité au cas linéaire qui présente déjà des difficultés considérables. Mais que peut bien "en pratique" signifier ici "résoudre" ?

Les équations résolubles par "formules", même en utilisant un attirail considérable de "fonctions spéciales" sont rares (et même rarissimes : on peut préciser cela pour des théorèmes rigoureux !).

La réponse est donc autre, et d'ailleurs *plus "pragmatique"* : obtenir à partir de la *donnée (finie) des polynômes a_n, \dots, a_0* , des *informations* aussi précises que possible, *qualitatives ou quantitatives, graphiques ou numériques, sur les solutions.*

On peut d'abord chercher à comprendre (ou calculer) ce qui se passe dans les "environs" (le "voisinage") d'une valeur fixée a de la variable x .

Soit $a=0$, pour fixer les idées.

Deux cas se présentent :

1. $A_n(0) \neq 0$ où 0 est un *point régulier*.

La situation est "triviale" : on se ramène en "déformant un peu" à $y^{(n)} = 0$. Analytiquement on "*développe en série*" la solution cherchée et la série obtenue "*converge*" et se prête à des calculs *aussi précis que voulu* (si on a le temps et l'argent).

2. $a_n(0) = 0$ où 0 est un point irrégulier. Les choses peuvent alors se gâter sérieusement et les solutions devenir très compliquées. C'est ici que le logiciel va entrer en oeuvre.

On va quand même "développer en série" les solutions (à l'origine). Regardons un peu ce qui se passe sur quelques exemples :

$$x^2 y' + y = x \quad (\text{équation d'Euler})$$

Solution particulière :

$$y = \sum_{n \geq 0} (-1)^n n! x^{n+1}$$

C'est une série "divergente" (et qui diverge même pas mal), mais qui permet si on est malin (comme Euler, vers le milieu du XVIIIème siècle) d'obtenir des informations numériques très précises (plus vite qu'une série convergente !) sur la vraie solution.

Solution générale :

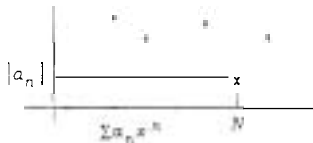
$$y = \sum_{n \geq 0} (-1)^n n! x^{n+1} + c e^{1/x}$$

(c constante complexe).

Il faut utiliser d'autres "fonctions" que les séries. Notre "arsenal" va se composer de :

1. séries (peut-être divergentes)
2. exponentielles : e^p avec $p(\frac{1}{x})$ polynôme
3. logarithmes
4. x^d (d nombre complexe et $x^d = e^{d \log x}$)

La remarque d'Euler a été systématisée par Poincaré, vers la fin du XIXème siècle, qui a étudié la "sommation au sens des astronomes".



On arrête la *sommation au "plus petit terme"* : le résultat est "pratiquement" très bon.

Cette méthode a été parfaitement étayée théoriquement et donne lieu à *divers algorithmes de resommation*. Ceci est mis en pratique dans le module

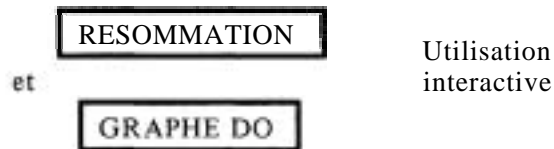
RESOMMATION

qui ne marche pour le moment que pour des cas "génériques". Pour les cas les plus difficiles on ne dispose d'un algorithme de resommation théorique que depuis quelques mois. Cet algorithme n'est pas étudié numériquement (et encore moins implanté). Tel quel, le module résout toutefois énormément de cas.

La dernière étude est l'étude graphique des solutions. C'est le rôle du module

GRAPHE DO

En pratique, il y a un jeu *interactif* entre



On utilise divers procédés de calcul : Resommation, Range-Kutta, séries convergentes.

Il y a des difficultés considérables dues à l'*instabilité*



Un autre exemple :

Les fonctions *hypergéométriques confluentes* (de Kummer) : fonctions spéciales bien connues et utiles (niveau d'énergie de l'atome d'hydrogène, diffusion...).

$$z y'' + (c-z) y' - a y = 0 \quad (a, c \text{ complexes})$$

Notons : $(b)_n = b(b+1) \dots (b+n-1)$.

Près de 0 on a une base de solution :

$$F(a,c;z) = \sum_{n \geq 0} \frac{(a)_n}{(c)_n n!} z^n$$

$$z^{1-c} F(a-c+1, z-c; z)$$

Les séries écrites sont convergentes (partout !) : pas de problème.

Près de ∞ on a une base de solutions (on pose $x = \frac{1}{z}$ et x est près de zéro) :

$$z^{-a} (-1)^n \frac{(a)_n (1+a-c)_n}{n!} z^{-n}$$

$$z^{a-c} e^z \frac{(c-a)_n (1-a)_n}{n!} z^{-n}$$

Ici les séries écrites divergent : que faire ?

Le logiciel que nous décrivons va d'abord calculer les solutions formelles (on ne se préoccupe pas de la convergence). On utilise pour cela les modules :

FROBENIUS

NEWTON

(s'il n'y a pas d'exponentielle)

(cas général)

La première difficulté est qu'il faut calculer formellement, et en temps raisonnable, avec des nombres algébriques : on a en effet à résoudre une succession d'équations algébriques :

Ex. : $x^2+1 = 0$, il faut "ajouter i "
 $x^3-2 = 0$, il faut ajouter $\sqrt[3]{2}$ et j .

On utilise pour cela le module

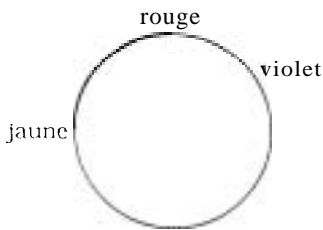
NOMBRES ALGEBRIQUES D5

Une fois qu'on a les solutions formelles le "Mathématicien Pur" est déjà très content : calcul des "invariants formels", comportement arithmétique des coefficients. Mais le résultat pourrait sembler *sans intérêt "pratique"*.

Ce n'est pas le cas et Physiciens et Ingénieurs savent bien que *les séries divergentes peuvent fournir des résultats numériques très fiables*. (Et que les situations les plus "intéressantes" donnent souvent lieu à des divergences !).

La *représentation graphique* pose des problèmes bien connus : le graphe d'une fonction complexe de variable complexe et un objet *dessiné en dimension 4*.

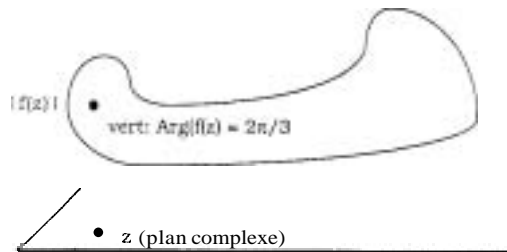
On emploie les *deux méthodes* suivantes basées sur *l'utilisation de la couleur*



1. On *colore un cercle* de centre 0 et de rayon p (240 couleurs) ce qui permet de *repérer l'Argument*.

On dessine l'image plane du cercle coloré par la fonction à étudier. On dispose d'un *système puissant de "zooms"* (de la taille de l'atome à celle d'une Galaxie : déjà nécessaire pour la fonction de Bessel !!).

2. On dessine dans \mathbb{R}^3 (en perspective) le *relief du module de la fonction à étudier* (comme les modèles en plâtre du XIXème siècle). On le *colore suivant l'argument* du point image.



IV. THEORIE DES NOMBRES par J.L. Nicolas (Université de Limoges)

A partir de quelques exemples, je voudrais montrer l'influence des ordinateurs sur les développements récents de l'arithmétique.

La fonction ζ de Riemann

Une des réalisations les plus impressionnantes est certainement le calcul de un milliard et demi de zéros de la fonction ζ de Riemann par H. te Riele, J. Van de Lune et D. Winter. Ils sont tous de partie réelle $1/2$, et le plus haut d'entre eux a une ordonnée de quelque 545 millions. Il a fallu deux mois d'un très gros ordinateur (CYBER 205) pour mener à bien ce travail. Ce type de calcul oblige à faire des mathématiques effectives : il ne suffit pas d'un reste qui tend vers 0, il en faut une majoration. Par ailleurs une hiérarchie s'établit entre les différentes formules : la meilleure est celle qui se calcule le plus vite.

Le système de cryptographie R.S.A.

Il y a une dizaine d'années, Rivest, Shamir et Adleman ont proposé un nouveau système de transmission secrète des messages basé sur le fait qu'il est relativement facile de construire des nombres premiers de 50 chiffres. Mais si l'on multiplie deux tels nombres entre eux, il est impossible à l'heure actuelle de retrouver les deux nombres premiers initiaux à partir de leur produit.

L'intérêt de ce système a développé considérablement les tests de primalité (certifiant qu'un nombre est premier) et les méthodes de factorisation, et l'on a fait appel pour cela à des outils mathématiques qui semblaient *a priori* assez éloignés des nombres premiers.

Les courbes elliptiques

L'un de ces outils est la théorie des courbes elliptiques, c'est-à-dire des fonctions $y = \pm \sqrt{x^3 + ax + b}$. Ces courbes avaient été introduites pour étudier le mouvement du pendule simple, elles font l'objet de très nombreux travaux depuis deux siècles.

Les formes quadratiques

Un autre outil est la théorie des formes quadratiques, c'est-à-dire des fonctions des deux inconnues x et y de la forme $ax^2 + bxy + cy^2$, proches parentes du bon vieux trinôme du second degré $ax^2 + bx + c$. Gauss avait introduit une opération sur ces formes, et en avait donné une méthode de calcul relativement

compliquée à effectuer à la main. Beaucoup plus tard cette opération était interprétée comme un produit d'idéaux dans l'anneau des entiers d'un corps de nombres, et cette interprétation algébrique éclipsait le premier point de vue. Mais il se trouve que pour effectuer cette opération avec un ordinateur, la méthode de Gauss est efficace, et se trouve ainsi réhabilitée.

Les algorithmes probabilistes

L'utilisation des ordinateurs a conduit à développer fortement des méthodes de calcul, c'est-à-dire des algorithmes, et c'est une compétition intéressante de trouver pour des opérations mathématiques diverses (calcul du plus grand commun diviseur, test de primalité, etc...) l'algorithme le plus rapide. Une nouvelle famille d'algorithmes a été ainsi trouvée, ce sont les algorithmes probabilistes. Par exemple, pour trouver un diviseur de n , on choisit un nombre d au hasard entre 2 et \sqrt{n} , on regarde si n est multiple de d . Si oui on a gagné, si non, on recommence avec un autre nombre d' au hasard. Cet algorithme de factorisation n'est pas très bon, mais il en existe d'autres très efficaces. On ne peut pas démontrer qu'ils marchent mais en pratique ils marchent, de la même façon que vous ne pouvez pas garantir, en lançant 100 fois un dé, que le 6 sortira au moins une fois, bien que cela ait lieu en pratique.

Le calcul formel

Certains ordinateurs réalisent maintenant des opérations algébriques, des calculs de primitives et de dérivées, le calcul matriciel, etc... . Cela constitue évidemment un outil très important pour les ingénieurs, et pour les scientifiques incluant bien sûr les mathématiciens. Les algorithmes pour cela sont loin d'être évidents. De la même façon que l'on comprend la difficulté d'enseigner à l'école primaire la division avec deux chiffres au diviseur en essayant de la faire à l'ordinateur, on voit que le calcul des intégrales que l'on enseigne en taupe ou en Deug n'est pas facile à décortiquer. Il y a là un vaste champ d'études pour les mathématiciens.