*COLLÈGE DE FRANCE*

*CHAIRE DE THÉORIE DES NOMBRES*

# LEÇON INAUGURALE

*faite le jeudi 17 mai 2001*

PAR

M. DON ZAGIER

Professeur

161

Monsieur l'Administrateur,

Mes chers Collègues,

Mesdames, Messieurs,

Chers amis,

Si vous avez déjà assisté à d'autres « leçons » comme celle que je vais donner aujourd'hui, vous savez que le conférencier commence souvent par exprimer l'étonnement qu'il avait ressenti en apprenant qu'il pourrait être candidat à un tel honneur et le bonheur que lui a donné sa nomination. J'ai aussi éprouvé ces sentiments, mais j'ai été particulièrement étonné puisque, étant étranger, je n'en avais même jamais imaginé la possibilité. J'ai déjà partagé ma vie entre cinq pays — les États-Unis, l'Angleterre, la Suisse, l'Allemagne et les Pays-Bas — et je vais maintenant y rajouter un sixième, un pays que j'ai aimé depuis mon enfance. Mon bonheur aussi est donc sûrement aussi grand que celui éprouvé par mes collègues français.

Il est, je crois, d'usage, lors d'une leçon inaugurale au Collège de France, d'évoquer les liens entre la chaire nouvelle et celles qui l'ont précédée. Dans mon cas, deux des trois chaires de mathématiques récemment renouvelées me sont particulièrement proches, tant au

Mes chers Collègues,
Mesdames, Messieurs,

En préparant cette leçon mon intention première était de me présenter grâce à quelques considérations d'ordre personnel. Peut-être aurais-je aussi rajouté quelques réflexions générales sur le rôle et la nature des mathématiques. Mais j'ai préféré ne pas le faire et donner à cette conférence une orientation strictement mathématique. L'idéal serait qu'elle soit à la fois compréhensible pour les non-mathématiciens et « non-triviale » pour les mathématiciens. C'est évidemment un but inaccessible et je crains même d'arriver au résultat exactement opposé. Mais j'aimerais quand même au moins essayer de vous montrer la beauté de ma discipline et la fascination qu'elle peut exercer au point qu'on y consacre une vie. En fin de compte, c'est peut-être aussi la meilleure façon de me présenter.

Parmi les différentes branches des mathématiques dites « pures », la théorie des nombres est en un sens la « plus pure » de toutes. D'une part, c'est le domaine le plus éloigné des applications concrètes en technologie et en sciences — bien que celles-ci existent, notamment en cryptographie et en théorie des codes. D'autre part, les objets étudiés, à savoir les nombres entiers 1, 2, 3, ..., sont les plus basiques, les moins « construits » de tous les objets étudiés par les mathématiciens. Et dans cette théorie, l'étude des équations dites diophantiennes est peut-être la plus séduisante et la plus accessible au non-spécialiste. C'est de cette théorie et des théories, liées, des courbes elliptiques et des formes modulaires, que je

vais vous parler aujourd'hui ainsi que dans les cours que je donnerai dans les prochaines années.

La théorie des nombres est non seulement la plus pure, mais aussi l'une des branches les plus anciennes des mathématiques. Déjà dans l'antiquité on s'est demandé par exemple comment obtenir des solutions en nombres entiers, comme

$$9 + 16 = 25,$$

à l'équation

$$a^2 + b^2 = c^2.$$

Cette question, motivée initialement par le « théorème de Pythagore » et par la nécessité de construire des angles droits pour mesurer les parcelles rectangulaires, a été analysée ensuite bien au-delà de ces besoins pratiques par différents peuples anciens tels que les Babyloniens, les Chinois, les Grecs et les Indiens, qui ont découvert des algorithmes capables de produire autant de solutions qu'on voudra de cette équation. D'autres questions de la théorie des nombres, comme les propriétés des nombres premiers et la décomposition de tout entier en facteurs premiers, ont aussi été étudiées, notamment dans les *Éléments* d'EUCLIDE. Mais c'est surtout DIOPHANTE, un mathématicien alexandrin du III$^{e}$ siècle de notre ère environ qui, dans son chef-d'œuvre *Arithmetika*, a créé une notation algébrique systématique et les méthodes fondamentales pour étudier ce que l'on appelle aujourd'hui les *équations diophantiennes*. Ces équations ont continué à fasciner les mathématiciens professionnels et amateurs depuis lors. Dans cette conférence j'essaierai — sans suivre le chemin historique — de vous donner quelque idée des questions étudiées dans ce domaine, des résultats obtenus, et de

ses liens souvent inattendus avec d'autres branches des mathématiques.

Commençons par un exemple simple et classique. Voici une question qui a été posée par FERMAT au XVII$^{e}$ siècle, et avant lui peut-être déjà par Diophante : étant donné un nombre premier $p$ (c'est-à-dire un nombre qui ne se décompose pas en produit de facteurs strictement inférieurs), est-ce que $p$ peut s'écrire comme la somme de deux nombres carrés ? Par exemple, on a $5 = 4 + 1 = 2^2 + 1^2$ et $29 = 25 + 4 = 5^2 + 2^2$, tandis que 7 ou 23 ne se décomposent pas de cette manière. La réponse trouvée — et démontrée ! — par Fermat est aussi belle que simple : si on laisse de côté le nombre premier 2, qui a la décomposition évidente $2 = 1 + 1 = 1^2 + 1^2$, on peut écrire le nombre forcément impair $p$ comme $2n + 1$ ; alors $p$ sera la somme de deux nombres carrés si et seulement si $n$ est pair (Tab. 1). Par exemple $29 = 2 \times 14 + 1$ avec 14 pair, tandis que $23 = 2 \times 11 + 1$ avec 11 impair. Ce théorème est maintenant considéré comme facile et on en connaît une bonne centaine de démonstrations différentes (c'est d'ailleurs moi qui détiens actuellement le record mondial de la démonstration la plus courte !), mais c'est quand même un résultat profond qui a été le point de départ de nombreuses théories mathématiques importantes comme la théorie algébrique des nombres, la théorie des anneaux, la théorie des corps de classes, etc.

Aujourd'hui je voudrais considérer une classe de problèmes un peu différente, la recherche des *points rationnels sur les courbes planes.* Pour la motiver, reprenons l'équation de Pythagore $a^2 + b^2 = c^2$ et notons avec Diophante qu'au lieu d'en chercher les solutions en nombres entiers nous pouvons tout aussi bien chercher

| $p$ | $p = x^2 + y^2$ ? | $p = 2n + 1$ |
|---|---|---|
| 3 | – | $2 \times 1 + 1$ |
| 5 | $4 + 1$ | $2 \times \mathbf{2} + 1$ |
| 7 | – | $2 \times 3 + 1$ |
| 11 | – | $2 \times 5 + 1$ |
| 13 | $9 + 4$ | $2 \times \mathbf{6} + 1$ |
| 17 | $16 + 1$ | $2 \times \mathbf{8} + 1$ |
| 19 | – | $2 \times 9 + 1$ |
| 23 | – | $2 \times 11 + 1$ |
| 29 | $25 + 4$ | $2 \times \mathbf{14} + 1$ |

les solutions en nombres *rationnels* — c'est-à-dire en fractions — de l'équation plus simple

$$x^2 + y^2 = 1,$$

une solution entière $a, b, c$ de la première équation nous donnant en effet une solution fractionnaire $x = a/c$, $y = b/c$ de la deuxième et inversement. Par exemple, la solution mentionnée $3^2 + 4^2 = 9 + 16 = 25 = 5^2$ de l'équation $a^2 + b^2 = c^2$ correspond à la solution fractionnaire

$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = \frac{9}{25} + \frac{16}{25} = 1$$

de l'équation $x^2 + y^2 = 1$. Plus généralement, on peut demander de trouver les solutions en nombres rationnels $x, y$ de n'importe quelle équation $f(x, y) = 0$, où $f$ est un polynôme à coefficients entiers. Une telle équation décrit une relation entre les nombres $x$ et $y$ qu'on peut représenter d'un point de vue moderne — inconnu de Diophante mais développé plus tard par les mathémati-

ciens français Descartes et Fermat — par une *courbe* dans le plan, le cas spécial $x^2 + y^2 = 1$ déjà cité correspondant par exemple au cercle de rayon 1 (Fig. 1). Le problème de trouver des solutions rationnelles (c'est-à-dire fractionnaires) de l'équation $f(x, y) = 0$ se traduit alors par le problème équivalent, mais géométriquement plus intuitif, de chercher sur la courbe des points dont les coordonnées cartésiennes $(x, y)$ seront des nombres rationnels, ou, comme nous le disons aujourd'hui, de trouver des *points rationnels* sur cette courbe.

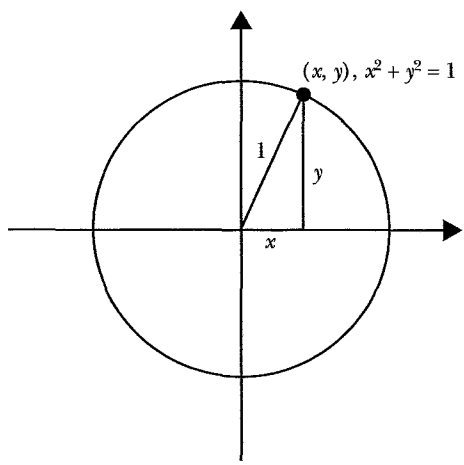


Figure 1.

Une propriété d'une importance capitale que l'on perçoit déjà de manière sous-jacente dans les *Arithmetika* de Diophante, mais dont toute la portée n'a été reconnue qu'au siècle dernier, est que les courbes peuvent être divisées en trois grandes classes ayant des propriétés

le point $(0, -1)$ est donnée par l'équation $y = -1 + tx$ et, en substituant cette expression dans l'équation du cercle, nous trouvons les formules

$$1 = x^2 + y^2$$
$$1 = x^2 + (-1 + tx)^2 = x^2 + 1 - 2tx + t^2x^2,$$
$$0 = (t^2 + 1)x^2 - 2tx,$$
$$0 = (t^2 + 1)x - 2t,$$
$$x = \frac{2t}{t^2+1}, \quad y = -1 + tx = -1 + \frac{2t^2}{t^2+1} = \frac{t^2-1}{t^2+1},$$

qui, pour des valeurs variables de $t$, donnent toutes les solutions de notre équation de départ (Fig. 4), les valeurs rationnelles de $t$ correspondant aux solutions rationnelles. Par exemple, la valeur numérique $t = 3$ donne

$$x = \frac{2\times 3}{3^2+1} = \frac{6}{10} = \frac{3}{5}, \quad y = \frac{3^2-1}{3^2+1} = \frac{8}{10} = \frac{4}{5},$$

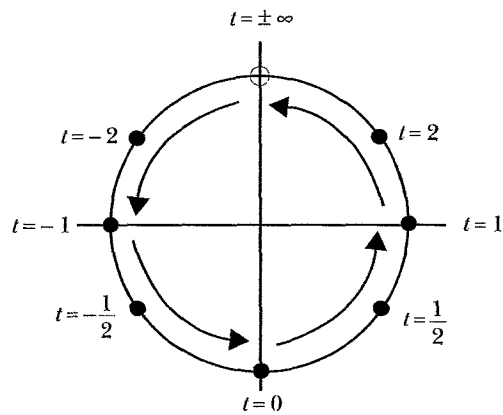


Figure 4.

la solution la plus simple et la plus ancienne, déjà mentionnée à plusieurs reprises, de l'équation $x^2 + y^2 = 1$. Ce calcul est essentiellement dû à Diophante lui-même, bien que, comme je l'ai déjà dit, il n'en connût pas l'interprétation géométrique.

Essentiellement la même méthode marche pour n'importe quelle courbe de degré 2 (pourvu qu'on en connaisse au moins un point rationnel), et on trouve que l'équation d'une telle courbe peut toujours être représentée ou, comme dit le mathématicien, *paramétrée*, par des fonctions $x = X(t)$, $y = Y(t)$ qui sont des quotients de fonctions polynomiales. (Dans notre exemple, $X(t)$ est la fonction $(2t)/(t^2 + 1)$ et $Y(t)$ la fonction $(t^2 - 1)/(t^2 + 1)$.) De telles fonctions s'appellent dans la terminologie moderne des *fonctions rationnelles*, d'où le nom « courbes rationnelles ». Mais il se trouve que ces mêmes courbes rationnelles possèdent une paramétrisation totalement différente, par des *fonctions trigonométriques*, ce qui nous donne un avant-goût de ce qui sera un élément clé de la théorie. Dans notre exemple, cette seconde paramétrisation est donnée par les deux fonctions $X(t) = \cos(t)$, $Y(t) = \sin(t)$. Parmi les propriétés de ces fonctions qu'on apprend à l'école figure l'équation $\cos^2(t) + \sin^2(t) = 1$ qui nous dit justement que nous avons affaire à une deuxième paramétrisation du cercle. La différence entre les deux paramétrisations est que, quand $t$ parcourt toutes les valeurs (réelles) possibles, le point correspondant sur le cercle avec les coordonnées $(X(t), Y(t))$ couvre le cercle une fois seulement dans le premier cas (en commençant au pôle nord pour $t = -\infty$ et en se déplaçant dans le sens inverse des aiguilles d'une montre pour rejoindre le pôle nord pour $t = +\infty$), cependant que dans le deuxième cas il contourne le cercle une infinité de fois, revenant au même point

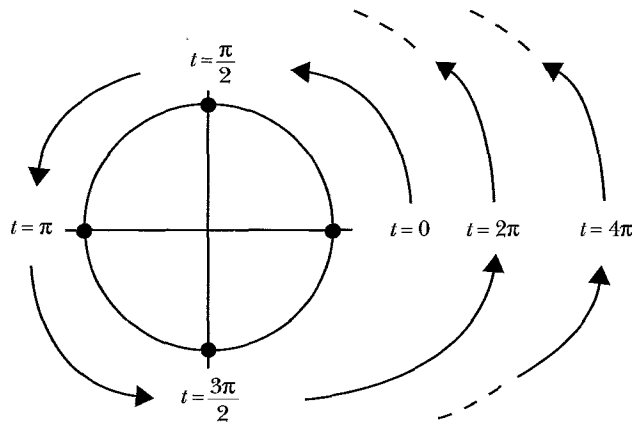


Figure 5.

chaque fois que t augmente de $2\pi$ (= 360°) (Fig. 5). En formules, ceci n'est rien d'autre que la *périodicité* fondamentale

$$\cos(t+2\pi)=\cos(t), \qquad \sin(t+2\pi)=\sin(t)$$

des fonctions trigonométriques cosinus et sinus que l'on peut aussi voir géométriquement dans les graphes de ces fonctions (Fig. 6). Cette périodicité peut être vue comme une *symétrie infinie* du graphe ou de la fonction qu'il représente, le mot « symétrie » dans ce contexte signifiant que ce graphe peut être déplacé d'une façon non-triviale sur lui-même (dans notre cas, de $2\pi$ unités vers la droite) et le mot « infinie », qu'il existe un nombre infini de tels déplacements (ici, les translations par tous les multiples de $2\pi$). La notion de symétrie (et sa représentation mathématique dans la théorie des groupes) compte parmi les idées les plus fondamentales en mathématiques, et jouera un rôle central dans ce qui va suivre.

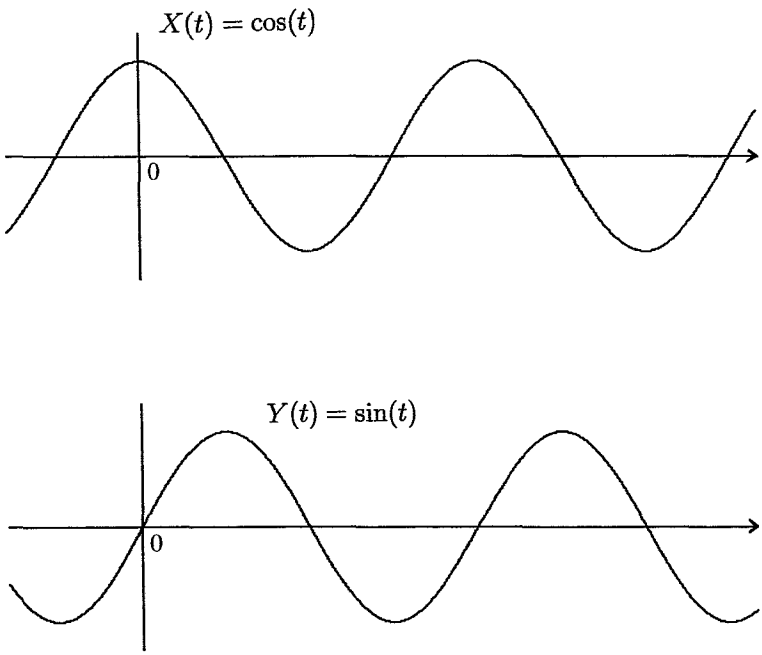


Figure 6.

**(ii) Courbes elliptiques**

La deuxième grande classe de courbes est, *grosso modo,* celle des courbes données par des équations de degré 3. (C'est une légère simplification de la vraie définition, qui est un peu plus technique.) Ici l'idée de Diophante ne marche plus dans sa forme originelle, puisqu'une droite générique coupe maintenant la courbe en trois points et non en deux comme avant (Fig. 7). Mais — comme l'a déjà découvert Diophante lui-même dans certains cas très spéciaux — une variante peut quelquefois produire des solutions intéressantes : si deux des trois points d'intersection de la droite et de la courbe

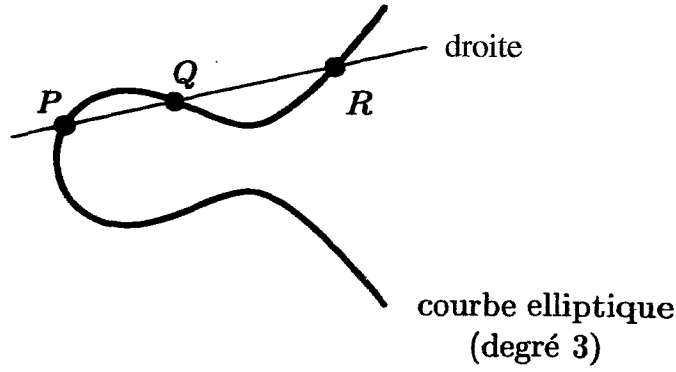


Figure 7.

ont des coordonnées rationnelles, alors il en sera automatiquement de même pour le troisième, ce qui nous donne une méthode pour produire des solutions nouvelles à partir des solutions déjà connues. Cette méthode a été utilisée par Diophante dans quelques cas où les deux premiers points coïncident, c'est-à-dire quand la droite est la tangente à la courbe en un point connu et la rencontre en un nouveau point (Fig. 8). (Cette méthode a été développée par Fermat au XVII$^{e}$ siècle et est à l'origine de sa célèbre méthode de « descente infinie ». L'interprétation géométrique que nous avons expliquée ici fut donnée par NEWTON au XVII$^{e}$ siècle, et le cas général avec trois points distincts par POINCARÉ à la fin du XIX$^{e}$ siècle.) C'est précisément cette possibilité de *composer,* ou *additionner,* des solutions connues de l'équation pour en obtenir de nouvelles qui rend la théorie des courbes elliptiques si riche.

A la différence du cas des courbes rationnelles, où la méthode de Diophante nous garantissait l'existence d'une infinité de solutions rationnelles (en supposant

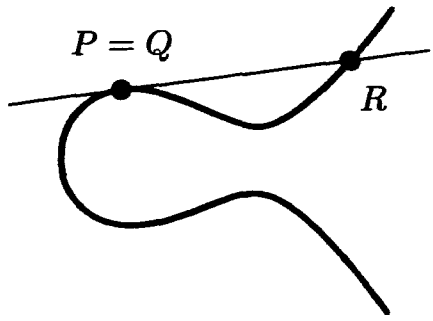


Figure 8.

toujours qu'il y en ait au moins une), ici le nombre de solutions peut être fini ou infini. Mais même dans le deuxième cas nous contrôlons bien la situation puisqu'un théorème démontré par le mathématicien britannique MORDELL en 1916 nous dit que toutes les solutions de l'équation d'une courbe elliptique s'obtiennent à partir d'un nombre fini d'entre elles en itérant la méthode de composition que j'ai déjà évoquée.

Enfin, exactement comme dans le cas des courbes rationnelles, les courbes elliptiques possèdent elles aussi une paramétrisation en termes de fonctions spéciales, mais cette fois les fonctions dont on a besoin sont *doublement périodiques,* c'est-à-dire qu'au lieu de n'avoir qu'une simple périodicité $X(t+A) = \mathrm{X}(t)$, $Y(t+A) = \mathrm{Y}(t)$ comme dans le cas du cercle (où la valeur de la constance $A$ était $2\pi$), elles ont *deux* périodicités indépendantes

$$X(t+A) = X(t+B) = X(t), \quad Y(t+A) = Y(t+B) = Y(t).$$

Ici la variable $t$ doit être interprétée comme un nombre *complexe* ou bi-dimensionnel, et le sens de l'équation est que les fonctions $X(t)$ et $Y(t)$ reprennent leurs valeurs si nous translatons $t$, non seulement dans une seule direc-

tion comme avant, mais dans l'une ou l'autre des deux directions définissant un réseau dans le plan (Fig. 9). Les fonctions doublement périodiques, étudiées depuis le XIX$^{e}$ siècle, s'appellent aussi *fonctions elliptiques,* d'où le nom « courbes elliptiques ».

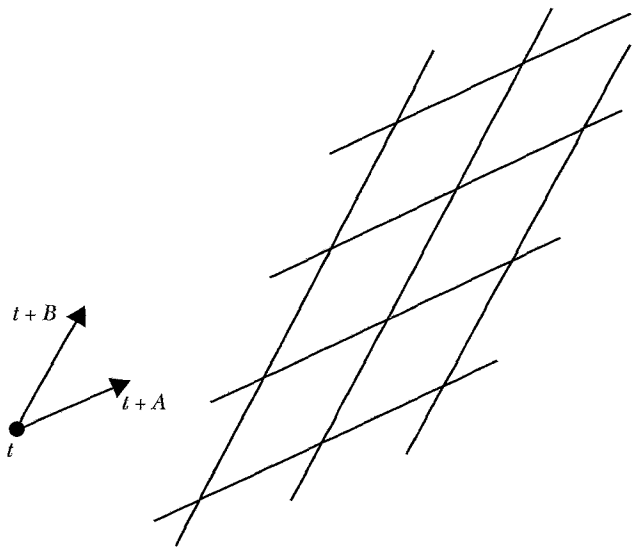


Figure 9.

**(iii) Courbes de type général**

Cette dernière classe contient toutes les courbes qui restent, c'est-à-dire toutes celles qui ne peuvent être représentées par aucune équation de degré 2 ou 3. Ici on ne connaît aucune paramétrisation, et même le problème de trouver des solutions rationnelles particulières — sans parler de décrire *toutes* les solutions rationnelles d'une équation donnée — est extrêmement difficile. Il a été conjecturé par Mordell en 1917, et démontré par FALTINGS en 1984, que le nombre des points ration-

nels sur les courbes de cette dernière classe est toujours fini — un théorème qui est à juste titre considéré comme l'un des joyaux des mathématiques contemporaines.

En résumé, les propriétés essentielles de nos trois classes de courbes sont :

(i) Les courbes rationnelles, ou courbes de degré 2, possèdent une paramétrisation par des fonctions rationnelles, et aussi des paramétrisations par des fonctions trigonométriques, qui sont périodiques. Les équations correspondantes ont une infinité de solutions rationnelles, qui s'obtiennent toutes par une procédure algorithmique simple.

(ii) les courbes elliptiques, ou courbes de degré 3, ont une paramétrisation par des fonctions elliptiques, qui sont doublement périodiques. L'équation correspondante peut avoir un nombre de solutions rationnelles fini ou infini, mais celles-ci s'obtiennent toujours à partir d'un nombre fini d'entre elles par une procédure algorithmique simple.

(iii) Les autres courbes ne possèdent aucune paramétrisation connue et il n'y a aucune procédure simple pour en trouver les points rationnels. Le nombre de tels points est toujours fini.

L'une des tâches les plus importantes et difficiles des mathématiques est de choisir les « bons » problèmes parmi l'infinité de questions possibles. Dans le cas présent, nous voyons que trouver les points rationnels est trop facile pour les courbes dans notre première classe et (du moins actuellement) trop difficile pour les courbes de la troisième classe pour mener à des mathématiques vraiment intéressantes. Mais, comme je l'ai

déjà indiqué, les courbes elliptiques ont une théorie profonde et d'une grande beauté. Dans le temps qui me reste, j'essaierai de vous en donner une idée.

Comme nous l'avons vu, il y a dans cette théorie une dichotomie essentielle : certaines courbes elliptiques n'ont qu'un nombre fini de points rationnels tandis que d'autres en ont une infinité. Une question fondamentale se pose donc : déterminer, dans chaque cas donné, laquelle de ces deux possibilités est réalisée. Cette question s'avère être un des « bons » problèmes mathématiques, dont la réponse dépend d'un lien totalement inattendu avec une autre branche de l'arithmétique. Ce lien a été découvert dans la forme d'une conjecture audacieuse qui s'est dégagée dans les années 50 et 60 et que l'on associe aux noms de TANIYAMA, SHIMURA, et WEIL. Exactement comme les courbes rationnelles avaient deux types de paramétrisation, par des fonctions *rationnelles* et par des fonctions *trigonométriques,* les courbes elliptiques en possèderaient elles aussi deux : la paramétrisation par des fonctions *elliptiques* connue depuis le XIX$^{e}$ siècle, à laquelle elles doivent leur nom, et aussi une deuxième paramétrisation par un autre type de fonctions transcendantes, les *fonctions modulaires.* Cette conjecture, qu'on avait vérifiée par des méthodes *ad hoc* dans un grand nombre de cas individuels, a été démontrée enfin par Andrew WILES et ses collègues (TAYLOR, BREUIL, CONRAD et DIAMOND) en 1994-2000. Ce résultat est non seulement considéré comme l'une des plus grandes réussites mathématiques du siècle, mais est sans doute aussi celle qui a reçu le plus de publicité — la raison en étant que, comme l'avait démontré K. RIBET en 1986 après des travaux préalables de G. FREY et J.-P. SERRE, il implique la solution du célébrissime « grand théorème de Fermat ». Vous

aurez peut-être lu à ce sujet certains des nombreux articles parus dans la presse il y a environ cinq ans, ou le livre de Singh qui est resté pendant des mois dans la liste des « meilleures ventes ». Le lien avec le théorème de Fermat est d'ailleurs indirect et fournit un bel exemple de la façon subtile dont un résultat mathématique peut en entraîner un autre : Le théorème de Fermat affirme qu'on ne peut pas trouver quatre entiers strictement positifs $a$, $b$, $c$ et $N$ avec $N \geq 3$ et $a^N + b^N = c^N$. Ce qu'ont prédit Frey et Serre et qu'a démontré Ribet est que, si l'on avait une telle solution, alors la courbe elliptique d'équation

$$y^2 = x^3 + 2(a^N + c^N)x^2 + b^{2N}x$$

ne serait *pas* paramétrée par des fonctions modulaires et contredirait donc le théorème que Wiles allait démontrer sept ans plus tard.

Que sont les fonctions modulaires ? Nous avons déjà vu les fonctions trigonométriques, qui ont une simple périodicité $X(t + A) = X(t)$, et les fonctions elliptiques, qui ont une double symétrie $X(t + A) = X(t)$ et $X(t + B) = X(t)$. Ceci est encore très simple puisque ces deux symétries « commutent » entre elles : nous avons $(t + A) + B = (t + B) + A$ (Fig. 10) et l'ordre dans lequel nous utilisons les deux équations d'invariance n'a donc pas d'importance. Cela peut être représenté graphique-

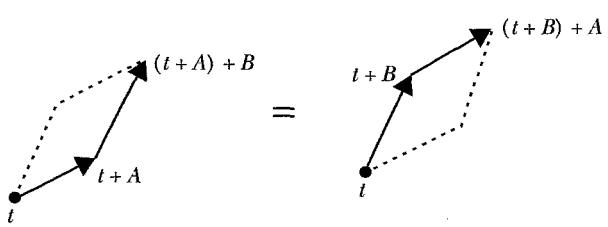


Figure 10.

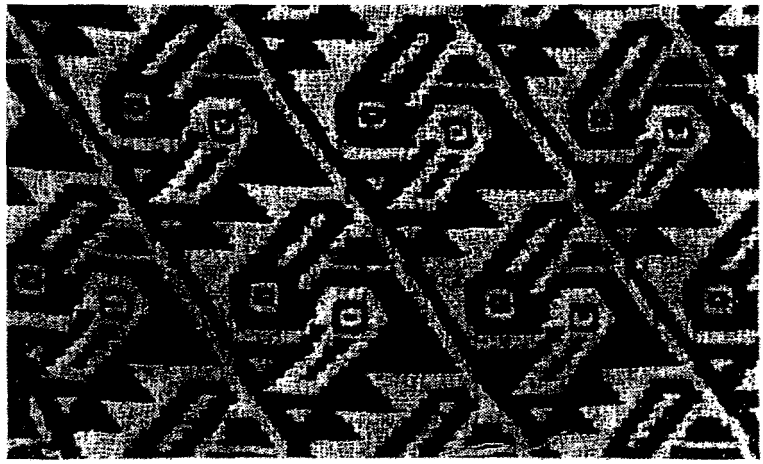

Figure 11.

ment par le dessin montré ici (Fig. 11), dans lesquels les répétitions d'un même motif indiquent les endroits où la fonction correspondante prend les mêmes valeurs. Les fonctions modulaires ont elles aussi une symétrie double ou multiple, mais cette fois les différents déplacements ne commutent pas entre eux, et à la différence des dessins réguliers que nous venons de voir, les dessins qu'il faut faire pour montrer comment les valeurs de ces fonctions se répètent sont ceux, beaucoup plus complexes, qu'on retrouve dans certaines gravures du célèbre artiste néerlandais ESCHER dont un exemple est montré ici (Fig. 12). La symétrie, je l'ai dit, est l'une des notions-clé de toutes les mathématiques, et c'est précisément la nature sophistiquée de la symétrie que possèdent les fonctions modulaires qui fait que leur théorie est si riche et donne lieu à des applications si profondes.

Comment les fonctions modulaires et le fait qu'elles paramètrent les courbes elliptiques nous aident-ils à

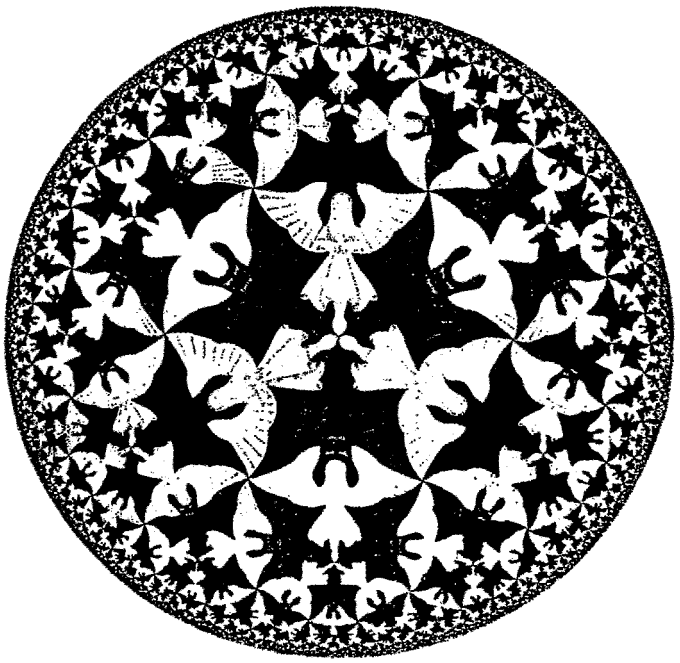

Figure 12.

résoudre des problèmes diophantiens ? Pour l'expliquer et pour fixer les idées, j'introduis un exemple qui me servira d'illustration dans toute la suite. J'avais commencé cette leçon par la question considérée par Fermat : quels nombres premiers sont sommes de deux carrés ? Regardons maintenant le problème suivant, d'apparence très analogue, posé par le mathématicien britannique du XIX$^{e}$ siècle SYLVESTER : quels nombres premiers sont sommes de deux *cubes* (nombres à la puissance trois) ? Par exemple, le nombre 7 peut s'exprimer comme la somme

$$7 = 8 + (-1) = 2 \times 2 \times 2 + (-1) \times (-1) \times (-1) = 2^3 + (-1)^3$$

(notez que, à la différence des carrés, les cubes peuvent être négatifs et que l'on peut donc indifféremment parler ici de sommes ou de différences), et le nombre 13, de façon un peu moins évidente, comme

$$13 = \frac{343+8}{27} = \frac{7\times7\times7+2\times2\times2}{3\times3\times3} = \left(\frac{7}{3}\right)^3+\left(\frac{2}{3}\right)^3,$$

tandis que les nombres 5 ou 11 ou 73 ne possèdent aucune décomposition de ce type. Notez aussi que nous admettons ici des nombres *rationnels* ou fractionnaires, et non seulement des entiers comme dans le cas du problème de Fermat. Voilà une nouvelle illustration de l'art de choisir de bons problèmes en mathématiques : il s'avère que le problème pour les cubes entiers n'est pas « bon », au sens où on ne discerne aucun motif, ni aucune possibilité de construire une théorie intéressante, tandis que le problème pour les cubes rationnels repose sur une structure belle et profonde. Mais même un mathématicien expérimenté ne pourrait savoir qu'il en est ainsi en regardant superficiellement les deux problèmes : on le découvre seulement après avoir pénétré loin dans leur théorie.

Une conséquence de la « composition » des solutions pour les courbes elliptiques que nous avons évoquée tout à l'heure est que, à l'exception du nombre premier 2 qui a la représentation unique $2 = 1^3 + 1^3$ comme somme de deux cubes rationnels, chaque nombre premier qui peut être exprimé ainsi, le peut d'une infinité de manières différentes. Par exemple, le nombre premier 19 n'a pas seulement la décomposition

$$19 = \frac{125+27}{8} = \left(\frac{5}{2}\right)^3+\left(\frac{3}{2}\right)^3,$$

mais aussi une infinité d'autres représentations

$$19 = (8/3)^3 + (1/3)^3 = (92/35)^3 + (33/35)^3 = \ldots$$

comme somme de deux cubes positifs et une infinité
$19 = 3^3 + (-2)^3 = (36/13)^3 + (-17/13)^3 = (109/31)^3 + (-90/31)^3 = ...$
où interviennent des cubes négatifs. La dichotomie « résoluble/non résoluble » est donc ici particulièrement tranchée : un nombre premier impair possède, soit un nombre infini de représentations du type voulu, soit aucune, et nous voulons savoir dans quel cas nous nous trouvons.

La première chose à souligner est qu'il s'agit ici d'un problème *difficile*. Comment pouvons-nous être sûrs que, parmi toute l'infinité des nombres rationnels, il ne se trouve aucune paire $x$ et $y$ satisfaisant à $x^3 + y^3 = 5$ ? Et même quand les solutions existent, comment pouvons-nous espérer les trouver, sachant que la solution rationnelle *la plus simple* de l'équation $x^3 + y^3 = p$ pour le « premier français » $p = 1789$ est donnée par

$$1789 = \left(\frac{381195380578202 21}{2828707454055574}\right)^3 - \left(\frac{24606633997841365}{2828707454055574}\right)^3$$

et que la solution la plus simple de l'équation $x^3 + y^3 = 382$ a pour dénominateur 812205439348579389316771950092906009315185401319457 4, ce qu'aucun ordinateur au monde ne pourrait jamais trouver par « force brute » ?

La réponse est tout à fait surprenante : la théorie des fonctions modulaires donne la solution aux deux questions ! Plus explicitement, on peut à l'aide de cette théorie associer à une courbe elliptique quelconque, et en particulier à chacun de nos problèmes $x^3 + y^3 = p$ avec $p$ premier, un « nombre magique » $S$ qui se calcule dans chaque cas par une procédure finie (bien que compliquée), et une conjecture profonde des mathématiciens

britanniques BIRCH et SWINNERTON-DYER, énoncée vers 1965, affirme que :

- si $S \neq 0$, alors l'équation n'a que des solutions évidentes ;
- si $S = 0$, alors l'équation a une infinité de solutions.

Cette conjecture est encore loin d'être complètement démontrée — c'est même l'un des sept problèmes, présentés dans cette même salle il y a presque exactement un an, pour les solutions desquels l'américain Landon Clay a offert un prix d'un million de dollars chacune. Cependant, nous en savons déjà beaucoup. L'une des deux directions est même entièrement démontrée : si le « nombre magique » $S$ est différent de 0, alors le nombre de solutions de l'équation en question est toujours fini (COATES, WILES, KOLYVAGIN). L'autre direction est partiellement démontrée. En fait, ce que j'ai appelé $S$ ci-dessus n'est pas seulement un nombre — c'est (essentiellement) la *valeur* en $s = 1$ d'une certaine fonction $L(s)$, appelée la « série $L$ » de la courbe, que l'on peut calculer explicitement. Par exemple, la série $L$ attachée à la courbe elliptique $x^3 + y^3 = 13$ que nous avons prise comme exemple tout à l'heure est la fonction suivante :

$$L(s) = 1 - \frac{2}{4^s} - \frac{1}{7^s} + \frac{4}{16^s} - \frac{1}{19^s} - \frac{5}{25^s} + \frac{2}{28^s} + \ldots$$

Ces séries $L$ jouent un rôle capital dans la théorie et nous les connaissons assez bien. Si $L(1)$ n'est pas égal à 0 (Fig. 13a), alors, comme je l'ai déjà dit, l'équation n'a pas de solution. Si $L(1)$ s'annule *simplement* (Fig. 13b), c'est-à-dire, si son graphe coupe l'axe $s$ avec un angle non nul (ou, dans un langage plus mathématique, si $L(1)$ s'annule mais que la dérivée $L'(1)$ n'est pas égale à 0), alors il y a une infinité de solutions, comme cela a

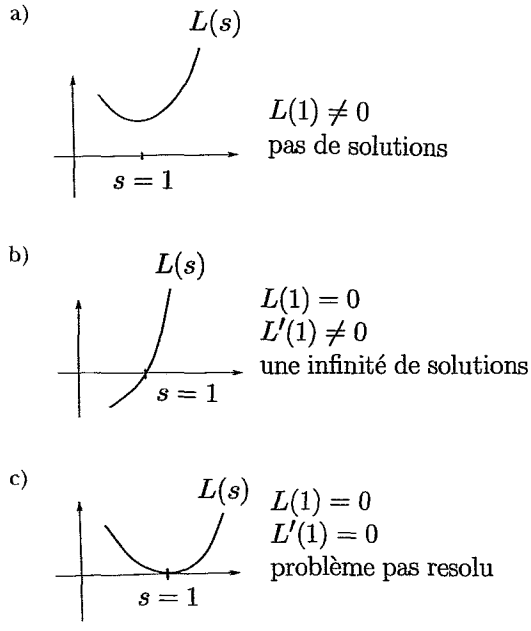


Figure 13.

été démontré par B. GROSS et moi-même il y a 15 ans. De plus, on peut même dans ce cas *utiliser* les fonctions modulaires qui paramètrent la courbe elliptique pour calculer un point rationnel non trivial sur la courbe, obtenant ainsi des solutions explicites comme les solutions gigantesques que je vous ai montrées tout à l'heure pour les deux équations $x^3 + y^3 = 1789$ et $x^3 + y^3 = 382$.

J'essaierai de dire en quelques mots d'où vient ce résultat. Supposons données une courbe elliptique et sa paramétrisation par des fonctions modulaires $x = X(t)$, $y = Y(t)$. Pour des valeurs spéciales $t_1$, ..., $t_m$ de $t$ convenablement choisies, on trouve alors certains points, appelés points de Heegner, sur la courbe. Ces points n'ont pas encore des coordonnées rationnelles, mais le

point que l'on obtient en en prenant la somme, de la manière que j'ai expliquée, sera rationnel. Malheureusement, il peut arriver qu'au cours de ce processus d'addition tout s'élimine et que l'on n'obtienne que la solution nulle de l'équation. Ce sera même toujours le cas si $L(1)$ n'est pas égal à 0. Mais un calcul long de presque 100 pages montre que si $L(1) = 0$, alors un certain nombre qui mesure la complexité du point de Heegner composé sera essentiellement égal à la valeur de la dérive $L'(1)$. Il s'ensuit que pour $L'(1)$ différent de 0 nous obtenons toujours une solution non triviale de notre équation diophantienne.

Ce théorème obtenu avec Gross était particulièrement intéressant parce que, grâce à un résultat préalablement démontré par le mathématicien américain D. GOLDFELD, on savait qu'il implique la solution du *problème des nombres de classes,* posé par Gauss en 1801 dans les *Disquisitiones Arithmeticae.* J'omets l'énoncé exact de ce problème, en soulignant cependant qu'ici — exactement comme dans le cas beaucoup plus spectaculaire de l'utilisation de la conjecture sur les paramétrisations modulaires pour démontrer le grand théorème de Fermat — un résultat difficile concernant les courbes elliptiques entraîne un théorème important dans un domaine de la théorie des nombres apparemment très éloigné.

Revenant maintenant à la conjecture de Birch et Swinnerton-Dyer et aux résultats connus à son sujet, nous pouvons résumer ce qui a été dit jusqu'ici comme suit :

- si $L(s)$ ne s'annule pas en $s = 1$, l'équation n'a que des solutions évidentes ;
- si $L(s)$ s'annule simplement en $s = 1$, l'équation a une infinité de solutions.

Ce n'est donc que dans le cas où $L(s)$ a un zéro multiple en $s = 1$, c'est-à-dire, où son graphe est tangent à l'axe $s$ en ce point (Fig. 13c), que le problème reste ouvert. En pratique ce n'est pas trop gênant puisque (a) ces cas sont conjecturalement (et expérimentalement) très rares, et (b) par une ironie du sort, précisément dans les cas où $L(s)$ a un zéro multiple, la conjecture de Birch et Swinnerton-Dyer prédit, et les expériences numériques confirment pleinement, qu'il y a *beaucoup* de solutions, y compris en général beaucoup de *petites* solutions, de sorte qu'une simple recherche par ordinateur suffit à résoudre le problème dans ces cas. Par exemple, pour $p = 19$, où la série $L$ associée à l'équation $x^3 + y^3 = p$ a un zéro double en $s = 1$, cette équation a de nombreuses solutions rationnelles simples, comme je vous l'ai montré tout à l'heure.

Enfin, pour vous donner quelque idée de la complexité cachée dans le problème apparemment simple que nous avons choisi, et pour satisfaire les appétits des mathématiciens professionnels parmi vous, j'aimerais finir notre excursion mathématique en vous montrant deux formules découvertes par le mathématicien argentin F. RODRIGUEZ VILLEGAS et moi-même il y a quelques années, qui permettent de calculer explicitement le « nombre magique » $S$ dans notre exemple $x^3 + y^3 = p$ avec $p$ premier et donc (conjecturalement) de déterminer dans tous les cas si cette équation a une solution. Ces formules ont l'air barbare pour le non-spécialiste, mais je promets aux non-mathématiciens que je ne les montrerai qu'assez brièvement et qu'il n'y aura pas d'examen. Je me restreins au cas où le nombre $p$ a la forme spéciale $9k + 1$, puisqu'il s'avère que c'est le cas le plus difficile et le plus intéressant. Le premier des deux résultats en question donne pour le nombre cherché $S$

une « formule close » qui a ceci d'intéressant que, bien que $S$ lui-même soit toujours un entier, la formule qui le donne contient des quantités transcendantes — ces quantités étant elles-mêmes, comme on pourrait peut-être s'en douter, des valeurs spéciales de fonctions modulaires. L'énoncé exact est le suivant. Nous associons à notre nombre premier $p$ le nombre réel $\alpha_p$ défini par la formule

$$\alpha_p = C\left(\frac{1}{6} + \frac{1}{A^p+1} - \frac{1}{A^{2p}-1} - \frac{1}{A^{4p}-1} + \frac{1}{A^{5p}+1} + \frac{1}{A^{7p}+1} - \ldots\right) \sqrt[3]{p},$$

où $A = e^{\pi/\sqrt{27}} = 1{,}830519\ldots$ et $C = 0{,}0380257\ldots$ est une deuxième constante définie par la condition $\alpha_1 = 1/54$. On démontre alors que $\alpha_p$ est en fait toujours un nombre algébrique, de degré exactement $2p-2$, et que, si l'on écrit l'équation qui le définit sous la forme

$$\alpha_p^{2p-2} + S_1\alpha_p^{2p-3} + S_2\alpha_p^{2p-4} + \ldots + S_{2p-3}\alpha_p + S_{2p-2} = 0,$$

alors le nombre $S$ que nous recherchons n'est rien d'autre que le premier coefficient $S_1$. Le deuxième résultat est de nature différente. Il existe une certaine suite d'entiers $B_0$, $B_1$, $B_2$, ... dont les premiers termes sont donnés comme suit :

$$\begin{aligned}
B_0 &= 1,\\
B_1 &= 2,\\
B_2 &= -152,\\
B_3 &= 6848,\\
B_4 &= -8103296,\\
B_5 &= -22483912960,\\
B_6 &= -8062284861440,\\
B_7 &= -196434444070666240,\\
B_8 &= 53265056425056944128 0,\\
&\vdots
\end{aligned}$$

Comme vous le voyez, ces nombres croissent très vite, mais ils se calculent à l'aide d'un algorithme élémentaire (bien qu'un peu compliqué) qui est décrit par le schéma montré ici (Table 2) : ce sont les nombres qui se trouvent à l'extrême droite du diagramme, dans lequel les petits nombres dans les cercles, les ovales et les carrés sont donnés par des formules très simples que ceux

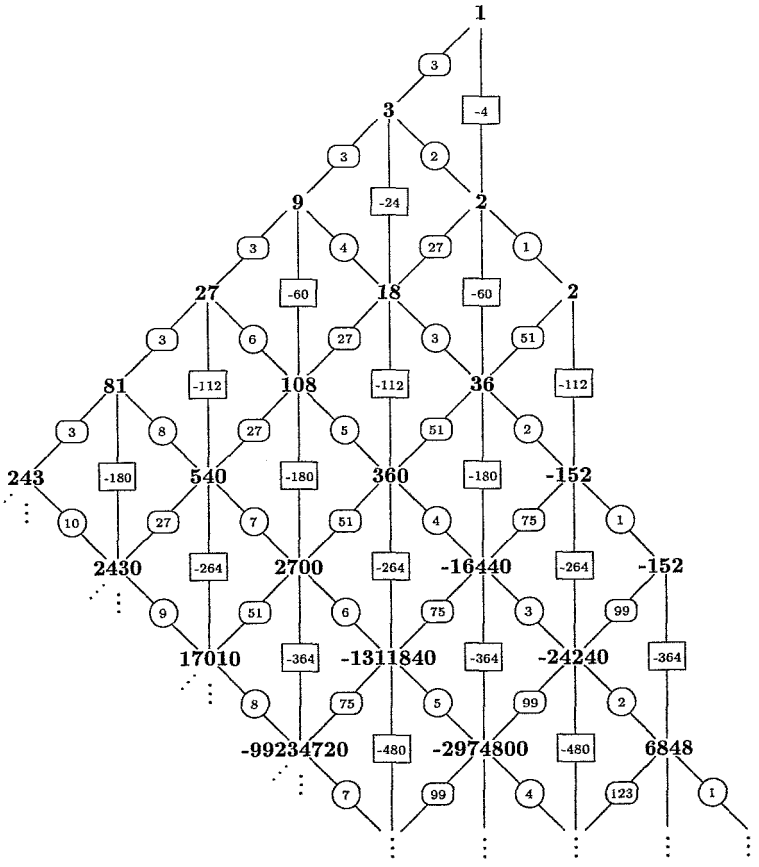


Table 2.

parmi vous qui aiment ce genre de devinette trouveront facilement, tandis que chaque nombre en caractères gras est la somme des trois nombres gras situés à son nord-ouest, nord, et nord-est, chacun multiplié par le nombre dans le cercle, carré ou ovale rencontré en chemin. Le théorème est maintenant le suivant : si le nombre premier $p = 9k + 1$ *divise* l'entier $B_k$, alors le nombre $S$ associé à l'équation $x^3 + y^3 = p$ est zéro et cette équation a (conjecturalement) une solution, tandis que si $B_k$ *n'est pas divisible* par $p$, alors $S$ est non nul et l'équation ne peut être résolue en nombres rationnels. (Il y a aussi une formule complète pour obtenir $S$, que j'omets.) Par exemple, les nombres premiers $19 = 9 \times 2 + 1$ et $37 = 9 \times 4 + 1$ divisent les nombres $B_2 = -152$ et $B_4 = -8103296$, respectivement, et devraient donc être tous les deux des sommes (ou des différences) de cubes rationnels, et en effet nous trouvons $19 = 27 - 8 = 3^3 - 2^3$ et $37 = 64 - 27 = 4^3 - 3^3$, tandis que le nombre premier $73 = 9 \times 8 + 1$ ne divise *pas* le nombre $B_8 = 532650564250569441280$ et ne peut donc pas être représenté comme la somme ou la différence de deux troisièmes puissances rationnelles.

Mesdames, Messieurs,

Mes chers Collègues,

Je suis arrivé à la fin de la partie mathématique de ma conférence, et presqu'à la fin du temps dont je dispose. J'espère que les deux derniers résultats que je vous ai montrés, même s'ils n'étaient pas compréhensibles en détail lors d'une présentation aussi rapide, ont pu vous donner une idée des subtilités auxquelles nous mène la recherche des solutions des problèmes apparemment

simples, voire enfantins, qui ont motivé la théorie. Dans les minutes qui me restent, je voudrais mentionner quelques-uns des sujets que j'espère discuter dans les cours que je donnerai cette année et dans les années suivantes. Il y a trois thèmes principaux, qui ont tous fait leur apparition dans ce que j'ai raconté aujourd'hui. Ces trois thèmes, étroitement liés entre eux et tous d'une grande importance dans la théorie des nombres aujourd'hui, sont : les équations diophantiennes et en particulier les courbes elliptiques, les séries $L$, et les fonctions modulaires. Je vous ai expliqué aujourd'hui comment les fonctions modulaires peuvent être utilisées pour obtenir des renseignements sur les équations diophantiennes et comment la série $L$ associée à une courbe elliptique détermine la solubilité de l'équation correspondante. En fait ceci n'est que l'une des raisons pour étudier ces objets : les fonctions modulaires (et les formes modulaires qui leur sont apparentées et qui seront centrales dans mon enseignement au Collège) possèdent une théorie très développée ayant des liens avec beaucoup de domaines mathématiques en dehors des équations diophantiennes, et les séries $L$, dont celles attachées aux courbes elliptiques et aux formes modulaires ne sont que des exemples très spéciaux, se sont avérées au cours des cinquante dernières années être l'un des outils les plus précieux dont nous disposons pour comprendre les problèmes de la géométrie et de l'arithmétique. Dans mes cours, cette année, j'étudierai la relation entre formes modulaires et équations différentielles. Ce lien, connu depuis plus de 100 ans, est très riche et a mené dans ces dernières années à de nombreuses applications dans différents domaines non seulement des mathématiques pures, mais aussi de la physique théorique, tels que la théorie de la percolation, la

théorie conforme des champs, la théorie des cordes, la symétrie miroir et la cohomologie quantique. J'espère aussi discuter les liens avec la combinatoire, la théorie des séries théta et des « mock theta functions » inventées par le génie indien RAMANUJAN juste avant sa mort prématurée en 1919, et les propriétés et applications des *formes de Jacobi,* une sorte d'hybride entre les fonctions elliptiques et les fonctions modulaires dont j'ai pu présenter la théorie, alors toute nouvelle, lors d'un cours au Collège de France en 1982 — cours dont mes souvenirs sont aujourd'hui d'autant plus vagues qu'avant chaque conférence j'avais partagé une bonne bouteille avec J.-P. Serre. Les sujets prévus pour les années ultérieures comprennent l'étude des valeurs spéciales des séries $L$ et, comme thème générique et récurrent, l'utilisation des fonctions transcendantes dans l'étude des questions arithmétiques — non seulement les formes modulaires et les séries $L$, mais aussi d'autres fonctions comme les fonctions de Green, les polylogarithmes, et leurs généralisations. Le premier cours commence lundi à 16 heures. J'espère vous y voir !