Sommes infinies, équations diophantiennes et le dernier théorème de Fermat[1]

Henri DARMON (U. McGill et CICMA)
Claude LEVESQUE (U. Laval et CICMA)

§1. Introduction

Le Dernier Théorème de Fermat vient de faire la une du New York Times, suite à la démonstration d'Andrew Wiles, complétée avec l'aide de son ancien élève Richard Taylor. Ainsi s'achève une épopée qui commence vers 1630, lorsque, dans la marge de sa version latine du volume ARITHMETICA de Diophante, Pierre de Fermat inscrit ces lignes énigmatiques, loin de se douter des passions qu'elles vont déchaîner:

> *Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum, potestatem in duos ejusdem nominis fas est dividere. Cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*

Ou encore, pour ceux qui ne sont pas latinistes:

> *On ne peut exprimer un cube comme une somme de deux cubes, un bicarré comme une somme de deux bicarrés, et plus généralement une puissance parfaite comme une somme de deux mêmes puissances. J'en ai découvert une démonstration tout à fait remarquable. Mais ma marge est trop étroite pour la contenir.*

On connaît la suite: Fermat ne communiqua jamais sa démonstration, à supposer qu'il en eût une. A la grande frustration des milliers de mathématiciens – des piètres amateurs aux savants les plus illustres – qui pendant plus de trois siècles allaient s'acharner à la retrouver!

[1]Conférence prononcée par Henri Darmon le 14 octobre 1995 au CEGEP de Lévis–Lauzon à l'occasion du Colloque des Sciences Mathématiques du Québec.

Dernier théorème de Fermat. *L'équation*

$$\boxed{x^n + y^n = z^n} \quad (n \geq 3) \tag{1}$$

ne possède pas de solution entière non triviale (i.e. où $xyz \neq 0$).

Le cas où $n = 4$ fut démontré par Fermat lui-même au moyen de sa méthode de *descente infinie*. On attribue à Euler la preuve (quoiqu'incomplète) du cas où $n = 3$. La liste des mathématiciens qui se sont attaqués au problème de Fermat est un véritable panthéon de la théorie des nombres: Dirichlet, Legendre, Cauchy, Lamé, Sophie Germain, Lebesgue, Kummer et Wieferich, pour ne citer que les noms les plus connus. Leurs travaux fournirent une démonstration du théorème de Fermat pour tous les exposants $n \leq 100$. Bien qu'il semble avoir une importance largement symbolique, le problème de Fermat n'en fut pas moins extraordinairement fécond pour les mathématiques modernes. Des théories entières – théorie algébrique des nombres, corps cyclotomiques – naquirent des efforts de Kummer pour le résoudre. En 1985, la théorie des courbes elliptiques et des formes modulaires jeta sur le problème une lumière inattendue, entrevue tout d'abord par le mathématicien allemand Gerhard Frey. Point de vue qui devait mener, dix ans plus tard, à la démonstration de Wiles.

Voici donc – enfin! – la démonstration du théorème de Fermat, si âprement recherchée. En gros!

Démonstration du dernier théorème de Fermat.
D'après K. Ribet [**R**], *la conjecture de Shimura–Taniyama (pour les courbes elliptiques semi-stables) implique le dernier théorème de Fermat.*
Or on sait grâce aux travaux de Wiles [**W**] *et Taylor–Wiles* [**T–W**] *que la conjecture de Shimura–Taniyama est vraie pour les courbes elliptiques semi-stables.*
C.Q.F.D.

Cette démonstration est très courte, et tiendrait facilement dans la fameuse marge du livre de Diophante! La démonstration de Fermat, si elle existait, devait donc être différente...

Le lecteur fera remarquer qu'il manque quelques détails! Les articles de Wiles et Taylor–Wiles occupent plus de 130 pages dans la revue prestigieuse "*Annals of Mathematics*", et

se basent sur de nombreux travaux antérieurs qui se résumeraient difficilement en moins de mille pages réservées aux initiés.

Ainsi, Wiles n'a pas réussi à faire tenir sa démonstration dans la marge étroite de quelque manuscrit. Les organisateurs d'une conférence sur le Dernier Théorème de Fermat tenue à Boston en Août 1995 en ont été quittes pour faire imprimer la démonstration sur un tee-shirt, porté par le premier auteur lors de son exposé au colloque, et dont le contenu est reproduit en appendice.

Pour la relation entre le dernier théorème de Fermat et la conjecture de Shimura–Taniyama, qui ne sera pas abordée dans cet exposé, on renvoie aux articles cités dans la bibliographie. On se bornera ici à expliquer, en termes élémentaires, la conjecture de Shimura–Taniyama. On aimerait surtout faire entrevoir au lecteur l'importance de cette conjecture, qui va bien au-delà du dernier théorème de Fermat, et touche à certaines des questions les plus profondes et les plus fondamentales en théorie des nombres.

§2. L'équation de Pythagore

Commençons par l'équation de Pythagore

$$\boxed{x^2 + y^2 = 1} \tag{2}$$

dont les *solutions rationnelles* $(x, y) = (\frac{a}{c}, \frac{b}{c})$ donnent lieu aux triplets de Pythagore (a, b, c) vérifiant l'équation $a^2 + b^2 = c^2$. Cette équation était à l'honneur dans le traité de Diophante et a poussé Fermat à se pencher sur le cas des exposants plus grands que 2. (Ainsi, notre point de départ est celui de Fermat, même s'il ne sera pas question de son dernier théorème...)

Les *solutions rationelles* de l'équation de Pythagore sont données de façon paramétrique par

$$(x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right), \quad t \in \mathbf{Q} \cup \{\infty\}, \tag{3}$$

ce qui fournit la classification des triplets de Pythagore et la solution complète de l'équation de Fermat pour $n = 2$.

Les solutions entières (à valeurs x et y dans $\mathbf{Z}$) sont encore plus simples à décrire. Il y

en a 4, à savoir $(\pm 1, 0)$ et $(0, \pm 1)$, et on pose

$$N_{\mathbf{Z}} = 4. \tag{4}$$

On peut aussi étudier l'équation $x^2 + y^2 = 1$ sur des corps autres que les rationnels; par exemple, le corps $\mathbf{R}$ des réels, ou les corps finis $\mathbf{F}_p = \{0, 1, 2, ..., p-1\}$ des classes de congruence modulo p, où p est un nombre premier.

Les solutions réelles de l'équation $x^2 + y^2 = 1$ correspondent aux points sur le cercle de rayon 1; on donne donc à l'ensemble des solutions réelles une mesure quantitative en posant

$$N_{\mathbf{R}} = 2\pi, \tag{5}$$

la circonférence du cercle.

Les solutions de $x^2 + y^2 = 1$ sur $\mathbf{F}_p$ forment un ensemble fini, et on pose

$$N_p = \#\{(x, y) \in \mathbf{F}_p^2 : x^2 + y^2 = 1\}. \tag{6}$$

Pour calculer N_p, on peut faire varier x entre 0 et $p-1$ et rechercher les solutions dont la première coordonnée est x. Il y en a 0, 1, ou 2, selon que $1 - x^2$ n'est pas un carré modulo p, est égal à 0, ou est un carré non-nul modulo p respectivement. Comme la moitié des entiers non-nuls modulo p sont des carrés, on s'attend à ce que N_p soit à peu près égal à p, et on définit a_p comme étant le "terme d'erreur" de cette estimation grossière:

$$a_p = p - N_p. \tag{7}$$

On en arrive au *problème central*, qui, comme on le verra plus tard, mène directement à la conjecture de Shimura–Taniyama.

Problème 1. *Existe-t-il une formule simple pour les nombres N_p en fonction de p (ou, ce qui revient au même, pour les a_p)?*

Le méthode expérimentale joue un rôle important en théorie des nombres, plus peut-être que dans d'autres branches des mathématiques pures. Gauss fut un calculateur prodigieux, et découvrit sa loi de réciprocité quadratique de façon empirique, avant d'en donner plusieurs démonstrations rigoureuses. Empruntant les pas du maître, dressons la liste des N_p pour quelques valeurs de p.

p	N_p	a_p
2	2	0
3	4	-1
5	4	1
7	8	-1
11	12	-1
13	12	1
17	16	1
19	20	-1
23	24	-1
29	28	1
31	32	-1
37	36	1
41	40	1
$\vdots$	$\vdots$	$\vdots$
10007	10008	-1
$\vdots$	$\vdots$	$\vdots$

Table 1: $x^2 + y^2 = 1$

Une inspection de cette table suggère tout de suite la conjecture suivante.

Conjecture 2. *On a* $N_p = 2$ *si* $p = 2$, *et*

$$N_p = \begin{cases} p-1 & \text{si } p \equiv +1 \pmod 4, \\ p+1 & \text{si } p \equiv -1 \pmod 4. \end{cases} \tag{8}$$

(En particulier, on constate que $p \neq N_p$, ce qui intéressera nos collègues informaticiens...)

Comment démontrer la conjecture 2? Revenons à la paramétrisation

$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right). \tag{9}$$

Les valeurs $t = 0, 1, ..., p-1, \infty$ donnent lieu à une liste complète de $p+1$ solutions distinctes, sauf lorsque $-1 = i^2$ est un carré modulo p. Dans ce dernier cas, le dénominateur $t^2 + 1$ s'annule pour les deux valeurs $t = \pm i$, et ces valeurs ne sont donc pas admissibles. Par conséquent, lorsque p est impair,

$$N_p = \begin{cases} p-1 & \text{si } -1 \text{ est un carré modulo } p, \\ \\ p+1 & \text{si } -1 \text{ n'est pas un carré modulo } p. \end{cases} \tag{10}$$

La condition que -1 soit un carré modulo p peut paraître subtile à priori. Heureusement, on dispose du théorème suivant, démontré par Fermat.

Théorème 3 (Fermat). *L'entier* -1 *est un carré modulo* p *si et seulement si* $p = 2$ *ou* $p \equiv 1 \pmod 4$.

En voici une démonstration, un peu différente de celle de Fermat. Le groupe multiplicatif $\mathbf{F}_p^\times$ est cyclique d'ordre $p-1$, et l'élément -1 d'ordre 2 a une racine carrée si et seulement si $\mathbf{F}_p^\times$ possède des éléments d'ordre 4.

Le théorème 3 que nous venons de démontrer, joint à la formule (10) fournit une démonstration de la conjecture 2 sur la valeur de N_p.

A quoi sert d'avoir une telle formule explicite pour N_p? Considérons, par exemple, le produit infini suivant (pris sur tous les premiers p) :

$$\prod_p \frac{p}{N_p} = \prod_p \left(1 - \frac{a_p}{p}\right)^{-1} \tag{11}$$

$$\text{“}=\text{”} \quad \left(\prod_{p\equiv 1(4)} \left(1-\frac{1}{p}\right)^{-1}\right) \cdot \left(\prod_{p\equiv -1(4)} \left(1+\frac{1}{p}\right)^{-1}\right) \tag{12}$$

$$\text{“}=\text{”} \quad \left(\prod_{p\equiv 1(4)} \left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)\right) \cdot \left(\prod_{p\equiv -1(4)} \left(1-\frac{1}{p}+\frac{1}{p^2}-\frac{1}{p^3}+\cdots\right)\right) \tag{13}$$

$$\text{“}=\text{”} \quad 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \cdots \tag{14}$$

$$= \quad \frac{\pi}{4} \qquad \text{(d'après la formule de Leibniz)}, \tag{15}$$

où l'avant-dernière égalité résulte (*formellement*) de la factorization unique des entiers en produits de puissances de nombres premiers. On en déduit que $\prod_p \frac{N_p}{p} = \frac{4}{\pi}$. En vérité, notre démonstration de cette égalité est fallacieuse, à cause de notre mépris un peu cavalier pour les questions de convergence, qui ferait frémir un analyste! C'est pourquoi nous avons mis certains des signes d'égalité entre guillemets. Les mathématiciens du 18^e siècle comme Euler étaient tout à fait à l'aise avec ces manipulations de séries formelles[2], se fiant à leur instinct

[2]Ainsi, ils faisaient du “prolongement analytique” un peu comme Monsieur Jourdain faisait de la prose, c'est-à-dire, sans le savoir.

pour éviter les pièges et parvenir à un résultat exact. Il est tout de même vrai que que

$$\prod_p \frac{N_p}{p} \quad \text{converge vers} \quad \frac{4}{\pi},$$

quoique la convergence soit très lente.

Rappelons que $N_{\mathbf{R}} = 2\pi$ et que $N_{\mathbf{Z}} = 4$. On constate alors que

$$\left(\prod_p \frac{N_p}{p}\right) \cdot N_{\mathbf{R}} \;=\; 2N_{\mathbf{Z}}. \tag{16}$$

Cette formule un peu magique laisse entrevoir une relation mystérieuse entre les solutions de l'équation $x^2 + y^2 = 1$ sur les corps finis $\mathbf{F}_p$, sur les réels, et sur l'anneau des entiers. En particulier, les nombres N_p, qui ne dépendent que des solutions de l'équation $x^2 + y^2 = 1$ sur $\mathbf{F}_p$, "connaissent" le comportement de cette équation sur les réels: on récupère grâce à eux le nombre π, lié à la circonférence du cercle. Il s'agit là au fond d'une *simple réinterprétation* de la formule de Leibniz, mais combien féconde! A l'aube du 21^e siècle, la théorie des nombres n'a pas encore digéré le sens profond de cette formule et de ses généralisations, comme on le verra plus tard.

§3. L'équation de Fermat–Pell

Fermat aimait lancer des défis mathématiques dans une correspondance régulière qu'il entretenait avec ses collègues à travers l'Europe. C'est ainsi qu'il invita les mathématiciens anglais Wallis et Brouncker à résoudre en entiers l'équation

$$\boxed{x^2 - 61y^2 = 1}\,. \tag{17}$$

Il s'agit là d'un cas particulier de l'équation $x^2 - Dy^2 = 1$, dite de Fermat–Pell. Cette équation était très chère a Fermat qui avait développé une méthode générale pour la résoudre, basée sur les fractions continues. Dans le cas où $D = 61$, la plus petite solution non-triviale est

$$(x, y) = (1766319049, 226153980)\,. \tag{18}$$

C'est la grosseur inhabituelle de cette plus petite solution qui poussa Fermat à prendre $D = 61$, bien qu'il prétendît, non sans malice, avoir choisi cette valeur de D au hasard!

Cette équation de Fermat–Pell, de degré 2, décrit une *conique* dans le plan, tout comme l'équation de Pythagore. Notons par N_p le nombre de solutions de cette équation modulo p, et dressons une fois de plus la liste des N_p pour quelques valeurs de p.

p	N_p	a_p
2	2	0
3	2	1
5	4	1
7	8	−1
11	12	−1
13	12	1
17	18	−1
19	18	1
23	24	−1
29	30	−1
31	32	−1
37	38	−1
41	40	1
43	44	−1
47	46	1
53	54	−1
59	60	−1
61	122	−61
67	68	−1
71	72	−1
73	72	1
⋮	⋮	⋮
10007	10006	1
10009	10008	1
⋮	⋮	⋮

Table 2: $x^2 - 61y^2 = 1$

En utilisant la paramétrisation

$$(x, y) = \left(\frac{1 + 61t^2}{1 - 61t^2}, \frac{2t}{1 - 61t^2} \right), \quad t \in \mathbf{Q} \cup \{\infty\}, \tag{19}$$

de la conique (2), on trouve de la même façon qu'avant que $N_2 = 2$, que $N_p = 2p$ si $p = 61$, et qu'autrement,

$$N_p = \begin{cases} p - 1 & \text{si 61 est un carré modulo } p, \\ \\ p + 1 & \text{si 61 n'est pas un carré modulo } p. \end{cases} \tag{20}$$

On invoque maintenant la loi de réciprocité quadratique de Gauss, qui dans notre contexte, affirme que pour p impair, 61 est un carré modulo p si et seulement si p est un carré modulo 61. Ainsi, on trouve pour $p \neq 2, 61$,

$$N_p = \begin{cases} p - 1 & \text{si } p \text{ est un carré modulo 61}, \\ \\ p + 1 & \text{si } p \text{ n'est pas un carré modulo 61}. \end{cases} \tag{21}$$

Cette formule simple (et périodique, puisqu'elle ne dépend que de p modulo 61) pour les N_p permet de déterminer, par un calcul formel calqué sur celui des équations (11) à (15),

l'identité

$$\prod_p \frac{p}{N_p} \quad \text{“}=\text{”} \quad \sum_n \frac{a_n}{n}, \tag{22}$$

où

$$a_n = \begin{cases} 0 & \text{si } 61|n, \text{ ou si } n \text{ est pair,} \\ +1 & \text{si } n \text{ impair est un carré non-nul modulo 61,} \\ -1 & \text{si } n \text{ impair n'est pas un carré modulo 61.} \end{cases} \tag{23}$$

On vérifie (par la formule de sommation d'Abel, par exemple) que la somme infinie dans l'équation (22) converge (conditionellement). Un calcul quelque peu héroïque (que nous invitons le lecteur à tenter!) permet de trouver l'identité, analogue de la formule (15) de Leibniz,

$$\sum_n \frac{a_n}{n} \;=\; \frac{4\sqrt{61}}{\log(1766319049 + 226153980\sqrt{61})}\,. \tag{24}$$

On reconnaît dans cette expression les coefficients qui apparaissent dans la solution (18) de l'équation (17). En conclusion, la connaissance des N_p nous a permis ici de “récupérer” une solution de l'équation de Fermat–Pell.

L'identité (22) peut en fait se réécrire formellement:

$$\left(\prod_p \frac{N_p}{p}\right) \cdot N_{\mathbf{R}} \quad \text{“}=\text{”} \quad \frac{1}{4\sqrt{61}} N_{\mathbf{Z}}. \tag{25}$$

Les quantités $N_{\mathbf{R}}$ et $N_{\mathbf{Z}}$ sont toutes les deux infinies, l'hyperbole d'équation $x^2 - 61y^2 = 1$ n'ayant pas de longueur finie, et l'équation de Fermat–Pell possédant une infinité de solutions entières. Il est tout de même naturel de définir leur rapport $\frac{N_{\mathbf{Z}}}{N_{\mathbf{R}}}$ comme étant

$$\frac{N_{\mathbf{Z}}}{N_{\mathbf{R}}} := \log(1766319049 + 226153980\sqrt{61})\,, \tag{26}$$

à savoir la quantité qui apparaît au dénominateur du membre de droite de l'expression (24). En effet, l'ensemble des solutions entières de l'équation (17) est un groupe abélien isomorphe à $\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, et l'application

$$(x, y) \mapsto \log(|x + y\sqrt{61}|) \tag{27}$$

envoie ce groupe dans un sous-groupe discret G de $\mathbf{R}$, isomorphe à $\mathbf{Z}$. Il est naturel donc de définir $N_{\mathbf{R}}/N_{\mathbf{Z}}$ comme le volume de $\mathbf{R}/G$, c'est-à-dire comme en (26).

Après quelques mois, Wallis et Brouncker répondirent à la question de Fermat, lui envoyant la solution (18) de l'équation (17), ainsi qu'une méthode générale (essentiellement identique à la méthode de Fermat basée sur les fractions continues) pour résoudre l'équation de Fermat–Pell $x^2 - Dy^2 = 1$. On ignore quelle fut la réaction du mathématicien toulousain, mais on peut imaginer qu'il n'alla pas sans ressentir une pointe de dépit... Toujours est-il que Wiles et Taylor ne sont pas les premiers mathématiciens anglais à relever avec brio les défis de Fermat!

§4. L'équation $x^3 + y^3 = 1$

Après les coniques, continuons sur notre lancée et passons aux équations de degré 3. En l'honneur de Fermat, étudions par exemple l'équation

$$\boxed{x^3 + y^3 = 1}. \tag{28}$$

Y a-t-il, comme avant, une formule simple pour le nombre N_p de solutions de cette équation modulo p? Comme avant, dressons une table.

p	N_p	a_p
2	2	0
3	3	0
5	5	0
7	6	1
11	11	0
13	6	7
17	17	0
19	24	−5
23	23	0
29	29	0
31	33	−2
37	24	13
41	41	0
⋮	⋮	⋮
10007	10007	0
10009	9825	184
⋮	⋮	⋮

Table 3: $x^3 + y^3 = 1$

Contrairement au cas de l'équation de degré 2, les a_p ne sont pas tous 0 ou ± 1, et semblent varier de façon plus imprévisible. L'inspection permet quand même de discerner quelques

propriétés des a_p. Par exemple, il semblerait que a_p soit toujours égal à 0 lorsque 3 divise $p+1$.

Mais qu'en est-il du cas où $p \equiv 1 \pmod 3$? Encore une fois, c'est Gauss qui a répondu à cette question en démontrant le théorème suivant.

Théorème 4 (Gauss).

(1) *Si $p \equiv -1$ (mod 3), alors $a_p = 0$.*

(2) *Si $p \equiv 1$ (mod 3), alors le nombre $4p$ peut s'écrire sous la forme $4p = A^2 + 27B^2$ avec $A \equiv -1$ (mod 3), ce qui détermine A uniquement. On a alors $a_p = A + 2$.*

La table suivante nous permet de vérifier le théorème de Gauss pour quelques valeurs de p:

p	N_p	a_p	$4p = A^2 + 27B^2$
2	2	0	$---$
3	3	0	$---$
5	5	0	$---$
7	6	1	$28 = (-1)^2 + 27 \cdot 1^2$
11	11	0	$---$
13	6	7	$52 = 5^2 + 27 \cdot 1^2$
17	17	0	$---$
19	24	-5	$76 = (-7)^2 + 27 \cdot 1^2$
23	23	0	$---$
29	29	0	$---$
31	33	-2	$124 = (-4)^2 + 27 \cdot 2^2$
37	24	13	$148 = 11^2 + 27 \cdot 1^2$
41	41	0	$---$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
10007	10007	0	$---$
10009	9825	184	$40036 = 182^2 + 27 \cdot 16^2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 4: $x^3 + y^3 = 1$ (suite)

§5. Les courbes elliptiques

Une courbe elliptique est une équation Diophantienne de degré 3, ayant au moins une solution rationelle. L'équation $x^3+y^3 = 1$ en est un exemple. On démontre que toute courbe elliptique sur les rationnels peut s'écrire, après un changement de variables, sous la forme

$$y^2 = x^3 + ax + b, \tag{29}$$

où a et b sont des nombres rationnels. On dénote comme avant par N_p le nombre de solutions de l'équation (29) sur le corps fini à p éléments.

Question 5. *Y a-t-il une formule explicite pour les N_p associés à une courbe elliptique, comme pour l'équation $x^3 + y^3 = 1$?*

Autrement dit, on aimerait généraliser le résultat de Gauss pour l'équation $x^3+y^3 = 1$, à une courbe elliptique quelconque. C'est précisément la portée de la conjecture de Shimura–Taniyama démontrée par Wiles pour une très grande classe de courbes elliptiques.

Avant d'en donner un énoncé précis, préparons le terrain en considérant la courbe elliptique

$$\boxed{y^2 + y = x^3 - x^2} \tag{30}$$

étudiée par Eichler. Voici quelques valeurs des N_p, calculées sur l'ordinateur:

p	N_p	a_p
2	4	-2
3	4	-1
5	4	1
7	9	-2
11	10	1
13	9	4
17	19	-2
19	19	0
23	24	-1
29	29	0
31	24	7
⋮	⋮	⋮
10007	9989	18
⋮	⋮	⋮

Table 5: $y^2 + y = x^3 - x^2$

Cette fois-ci, il est plus difficile de discerner une structure dans la valeur des a_p, qui semble osciller de façon assez aléatoire. Hasse a pu démontrer l'inégalité

$$|a_p| \leq 2\sqrt{p}$$

(valable pour toute courbe elliptique), mais ceci est très loin de donner une *formule exacte* pour les N_p.

Eichler, se basant sur les travaux profonds de Hecke, a quand même pu déterminer une telle formule exacte. On commence par étendre la définition du coefficient a_p (valable pour p premier) à tout entier n, en posant:

$$\begin{cases} a_p & = p - N_p, \\ a_{p^r} & = a_p a_{p^{r-1}} - p a_{p^{r-2}}, \quad \text{où } a_1 = 1, \\ a_n & = \prod_{i=1}^{r} a_{{p_i}^{e_i}}, \qquad\qquad \text{où } n = \prod_{i=1}^{r} {p_i}^{e_i}. \end{cases} \tag{31}$$

On remarque que cette extension est assez naturelle: si on dénote par N_{p^r} le nombre de solutions de la courbe elliptique sur le corps fini avec p^r éléments, alors

$$a_{p^r} = p^r - N_{p^r}. \tag{32}$$

Théorème 6 (Eichler). La série formelle $\sum_{n=1}^{\infty} a_n q^n$ est donnée par la formule:

$$\begin{aligned} q \prod_{n=1}^{\infty} (1-q^n)^2 \cdot (1-q^{11n})^2 \quad = \quad & q - \mathbf{2q^2} - \mathbf{q^3} + 2q^4 + \mathbf{q^5} + 2q^6 - \mathbf{2q^7} \\ & - 2q^9 - 2q^{10} + \mathbf{q^{11}} - 2q^{12} + \mathbf{4q^{13}} + 4q^{14} \\ & - q^{15} - 4q^{16} - \mathbf{2q^{17}} + 4q^{18} + 2q^{20} + 2q^{21} \\ & - 2q^{22} - \mathbf{q^{23}} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} \\ & + 2q^{30} + \mathbf{7q^{31}} + \cdots + \mathbf{18q^{10007}} + \cdots \end{aligned}$$

Le lecteur pourra vérifier le théorème d'Eichler pour quelques valeurs de p, en comparant les coefficients de q^p marqués en caractères gras, avec les valeurs qui apparaissent dans la table 5.

La conjecture de Shimura–Taniyama, démontrée par Wiles, est une généralisation directe du théorème d'Eichler, dans le sens que Wiles donne une *description* très précise de la fonction génératrice $\sum_n a_n q^n$, où les a_n sont les coefficients associés à une courbe elliptique quelconque.

Plus précisément, soit

$$f(z) \; = \; \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \tag{33}$$

une série de Fourier avec coefficients $a_n \in \mathbf{R}$, et soit N un entier positif. On dit que $f(z)$ est une *forme modulaire* de niveau N si les conditions suivantes sont satisfaites:

1. La série qui définit f converge lorsque $\mathrm{Im}(z) > 0$, i.e., quand $|e^{2\pi iz}| < 1$. La série f définit alors une fonction holomorphe dans le demi-plan de Poincaré des nombres complexes ayant une partie imaginaire strictement positive.

2. Pour tout $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in SL_2(\mathbf{Z})$, on a

$$f\left(\frac{az+b}{Ncz+d}\right) = (Ncz+d)^2 f(z). \tag{34}$$

   Ici $SL_2(\mathbf{Z})$ est le groupe des matrices 2×2 à coefficients dans $\mathbf{Z}$ de déterminant 1.

Voici, enfin, la conjecture de Shimura–Taniyama.

Conjecture 7 (Shimura–Taniyama). *Soit $y^2 = x^3 + ax + b$ une courbe elliptique, et soit a_n ($n = 1, 2, \ldots$) les entiers définis à partir de cette courbe, par les équations (31). Alors la fonction génératrice*

$$f(z) \;=\; \sum_{n=1}^{\infty} a_n e^{2\pi inz} \tag{35}$$

est une forme modulaire.

En fait, la conjecture est plus précise:

1. Elle prédit la valeur du niveau N de la forme modulaire associée à la courbe elliptique. Ce niveau serait égal au *conducteur arithmétique* de la courbe, qui ne dépend que de ses nombres premiers de "mauvaise réduction". La définition exacte de N ne sera pas utilisée dans notre discussion.

2. L'espace des formes modulaires de niveau N donné est un espace vectoriel sur $\mathbf{R}$ dont la dimension, finie, se calcule sans grande difficulté à partir de N. Cet espace est muni de certains opérateurs linéaires naturels définis par Hecke. La conjecture affirme aussi que la forme modulaire f est un *vecteur propre* de tous les opérateurs de Hecke.

On démontre qu'il n'y a qu'un *nombre fini* de formes modulaires de niveau N qui sont vecteurs propres pour tous les opérateurs de Hecke, et dont le premier coefficient de Fourier a_1 est égal à 1. Ainsi, une fois que l'on a calculé le conducteur N d'une courbe elliptique, on est ramené à une liste finie de possibilités pour la suite (a_n) associée à cette courbe. C'est en ce sens que la conjecture de Shimura–Taniyama donne une formule explicite pour les nombres N_p de points rationnels sur une courbe elliptique modulo p.

Grâce aux travaux de Wiles et Taylor–Wiles, on sait maintenant que la conjecture de Shimura–Taniyama est vraie pour une très grande classe de courbes elliptiques. En fait, Diamond démontre, améliorant les résultats de Wiles et Taylor–Wiles, qu'il suffit que la courbe elliptique ait bonne réduction, ou au pire un seul point double, modulo 3 et 5.

La formule de Wiles pour les N_p associés à une courbe elliptique semble à prime abord moins concrète que celle de Fermat (conjecture 2) pour l'équation $x^2 + y^2 = 1$, ou que le théorème 4 de Gauss pour l'équation $x^3 + y^3 = 1$. Mais elle permet quand même de donner un sens à l'expression $\prod_p \frac{p}{N_p}$, ou pour être plus précis [3], à la quantité

$$\prod_p \frac{p}{N_p + 1}.$$

Cela se fait en introduisant la série L associée à la courbe elliptique E:

$$L(E, s) \;=\; \prod_p \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} \;=\; \sum_n \frac{a_n}{n^s}. \tag{36}$$

On note que, formellement,

$$L(E, 1) \quad \text{“}=\text{”} \quad \prod_p \frac{p}{N_p + 1}, \tag{37}$$

bien que la série qui définit $L(E, s)$ ne converge que pour $\mathrm{Re}(s) > \frac{3}{2}$. Pour donner un sens à $L(E, 1)$ il faudrait savoir que la série qui définit $L(E, s)$ admet tout au moins un prolongement analytique jusqu'à la valeur $s = 1$.

Or, on a le résultat fondamental de Hecke.

Théorème 8 (Hecke). *Si la suite (a_n) provient d'une forme modulaire, alors la fonction $L(E, s)$ admet un prolongement analytique à tout le plan complexe, et en particulier la valeur $L(E, 1)$ est bien définie.*

Si on sait que la courbe elliptique E est modulaire, alors le résultat de Hecke nous permet de *définir*

$$\prod_p \frac{p}{N_p + 1} := L(E, 1). \tag{38}$$

Comme dans les exemples précédents, on peut s'attendre à ce que la valeur $L(E, 1)$ (ou, plus généralement, le comportement de $L(E, s)$ au voisinage de $s = 1$) contienne des

[3] Dans notre définition, trop naïve, de N_p, on a systématiquement omis de compter une solution, qui correspond au “point à l'infini” et qui apparaît naturellement quand on considère une équation de la courbe elliptique dans le plan projectif de Desargues. Il est donc naturel de remplacer N_p par $N_p + 1$.

renseignements de nature arithmétique sur la courbe E. C'est précisément le contenu de la conjecture de Birch–Swinnerton-Dyer, dont nous n'énoncerons ici qu'un cas particulier.

Conjecture de Birch et Swinnerton-Dyer faible. *La courbe elliptique E admet un nombre fini de points rationnels si et seulement si $L(E,1) \neq 0$.*

Cette conjecture est loin d'être démontrée, et demeure l'une des questions ouvertes les plus importantes dans la théorie des courbes elliptiques.

On dispose quand même de certains résultats partiels, par exemple, le suivant, qui découle des travaux de Gross–Zagier et Kolyvagin, joints à un résultat analytique de Bump–Friedberg–Hoffstein et Murty–Murty.

Théorème 9 (Gross–Zagier, Kolyvagin). *Soit E une courbe elliptique modulaire. Si la fonction $L(E,s)$ a un zéro d'ordre 0 ou 1 en $s = 1$, alors la conjecture de Birch et Swinnerton-Dyer faible est vraie pour E.*

Le cas où la fonction $L(E,s)$ a un zéro d'ordre > 1 demeure encore très mystérieux. On s'attend à ce que l'équation de la courbe E ait toujours des solutions rationelles dans ce cas, mais on ignore comment les construire de façon systématique, ou même s'il y a un algorithme pour déterminer l'ensemble des solutions rationelles dans tous les cas. Malgré les progrès spectaculaires des dernières années, les théoriciens des nombres, amateurs de courbes elliptiques, ont encore du pain sur la planche!

Appendice: Le tee-shirt de la conférence de Boston University

Sur le devant du tee-shirt en question, on peut lire ce qui suit.

FERMAT'S LAST THEOREM: *Let* $n, a, b, c \in \mathbf{Z}$ *with* $n > 2$. *If* $a^n + b^n = c^n$ *then* $abc = 0$.

Proof. The proof follows a program formulated around 1985 by Frey and Serre [F,S]. By classical results of Fermat, Euler, Dirichlet, Legendre and Lamé, we may assume that $n = p$, an odd premier ≥ 11. Suppose $a, b, c \in \mathbf{Z}, abc \neq 0$, and $a^p + b^p = c^p$. Without loss of generality we may assume $2|a$ and $b \equiv 1 \pmod 4$. Frey [F] observed that the elliptic curve $E : y^2 = x(x - a^p)(x + b^p)$ has the following "remarkable" properties:
(1) E is semistable with conductor $N_E = \prod_{\ell|abc} \ell$; and
(2) $\bar{\rho}_{E,p}$ is unramified outside $2p$ and is flat at p.
By the modularity theorem of Wiles and Taylor–Wiles [W,T–W], there is an eigenform $f \in S_2(\Gamma_0(N_E))$ such that $\rho_{f,p} = \bar{\rho}_{E,p}$. A theorem of Mazur implies that $\bar{\rho}_{E,p}$ is irreducible, so Ribet's theorem [R] produces a Hecke eigenform $g \in S_2(\Gamma_0(2))$ such that $\rho_{g,p} \equiv \rho_{f,p} \pmod{\mathcal{P}}$ for some $\mathcal{P}|p$. But $X_0(2)$ has genus zero, so $S_2(\Gamma_0(2)) = 0$. This is a contradiction and Fermat's Last Theorem follows. Q.E.D.

Sur l'arrière du tee-shirt apparaît la bibliographie suivante.

[**F**] Frey, G: Links between stable elliptic curves and certain Diophantine equations. *Ann. Univ. Sarav.* **1** (1986), 1-40.

[**R**] Ribet, K: On modular representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$) arising from modular forms. *Invent. Math.* **100** (1990), 431-476.

[**S**] Serre, J.-P.: Sur les représentations modulaires de degré 2 de $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.* **54** (1987), 179-230.

[**T–W**] Taylor, R.L., Wiles, A.: Ring-theoretic properties of certain Hecke algebras. *Annals of Math.* **141** (1995), 553-572.

[**W**] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. *Annals of Math.* **141** (1995), 443-551.

Bibliographie annotée

Les références sont divisées en 7 sections, chacune portant sur un thème donné. Les lectrices et les lecteurs qui souhaitent ne consulter que des articles de synthèse de niveau accessible seront très bien servis par les références 1 à 4, 8 à 11, 14 à 18 de la section (**B**).

(A) Le dernier théorème de Fermat

Les sources suivantes contiennent des renseignements historiques sur le dernier théorème de Fermat, et sur les métodes qui ont précédé celles basées sur les courbes elliptiques.

1. E.T. Bell, *The Last Problem*, 2^e édition, MAA Spectrum, Mathematical Association of America, Washington, DC. 1990. 326 pages.

2. H.M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Graduate Texts in Math. **50**, Springer-Verlag, New York, Berlin, Heidelberg, 1977, 410 pages.

3. C. Houzel, *De Diophante à Fermat*, dans *Pour la Science* **220**, janvier 1996, 88-96.

4. P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, Berlin, Heidelberg, 1979, 302 pages.

5. L.C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. **83**, Springer-Verlag, New York Berlin 1982, 389 pages.

(B) Courbes elliptiques et le dernier théorème de Fermat

Pour en savoir plus sur la relation entre les courbes elliptiques et le dernier théorème de Fermat, on suggère:

1. N. Boston, *A Taylor-made Plug for Wiles' Proof*, College Math. J. **26**, No. 2, 1995, 100–105.

2. B. Cipra, *"A Truly Remarkable Proof"*, dans *What's happening in the Mathematical Sciences*, AMS Volume **2**, 1994, 3–7.

3. D.A. Cox, *Introduction to Fermat's Last Theorem*, Amer. Math. Monthly **101**, (1994) no. 1, 3–14.

4. G. Faltings, *The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles*, Notices AMS **42**, No. 7, 743–746.

5. G. Frey, *Links Between Stable Elliptic Curves and Certain Diophantine Equations*, Ann. Univ. Sarav. **1**, (1986), 1–40.

6. G. Frey, *Links Between Elliptic Curves and Solutions of* $A - B = C$, Indian Math. Soc. **51**, 1987, 117–145.

7. G. Frey, *Links Between Solutions of* $A - B = C$ *and Elliptic Curves*, dans *Number Theory, Ulm, 1987, Proceedings*, Lecture Notes in Math. **1380**, Springer-Verlag, New York, 1989, 31–62.

8. C. Goldstein, *Le théorème de Fermat*, La Recherche **263**, Mars 1994, 268–275.

9. C. Goldstein, *Un théorème de Fermat et ses lecteurs*, Presses Universitaires de Vincennes, 1995.

10. F.Q. Gouvêa, *A Marvelous Proof*, Amer. Math. Monthly **101**, (1994) no. 3, 203–222.

11. B. Hayes and K. Ribet, *Fermat's Last Theorem and Modern Arithmetic*, Amer. Scientist **82**, 1994, 144–156.

12. Y. Hellegouarch, *Points d'ordre* $2p^h$ *sur les courbes elliptiques*, Acta Arith. **26**, 1974/75, 253–263.

13. Y. Hellegouarch, *Fermat enfin démontré*, dans *Pour la Science* **220**, février 1996, 92-97.

14. S. Lang, *Old and New Conjectured Diophantine Inequalities*, Bull. AMS (New Series) **23**, No. 1, 1990, 37–75.

15. B. Mazur, *Number theory as gadfly*, Amer. Math. Monthly **98**, (1991) no. 7, 593–610.

16. B. Mazur, *Questions about Number*, in *New Directions in Mathematics*, Cambridge Univ. Press, Cambridge, à paraître.

17. M.R. Murty, *Fermat's Last Theorem: An Outline*, Gazette Sc. Math. Québec, Vol. **XVI**, No. 1, 1993, 4–13.

18. M.R. Murty, *Reflections on Fermat's Last Theorem*, Elem. Math. **50** (1995) no. 1, 3–11.

19. J. Oesterlé, *Nouvelles aproches du "théorème" de Fermat"*, Séminaire Bourbaki No. **694** (1987-88), Astérisque **161–162**, 1988, 165–186.

20. K. Ribet, *On Modular Representations of Gal($\bar{\mathbf{Q}}/\mathbf{Q}$)) Arising from Modular Forms*, Invent. Math. **100**, 1990, 431–476.

21. K. Ribet, *From the Taniyama–Shimura Conjecture to Fermat's Last Theorem*, Ann. Fac. Sci. Toulouse (5) **11** (1990) no. 1, 116–139.

22. K. Ribet, *Wiles Proves Tanyama's Conjecture; Fermat's Last Theorem Follows*, Notices Amer. Math. Soc. **40**, 1993, 575–576.

23. K. Ribet, *Galois Representations and Modular Forms*, Bull. AMS (New Series) **32**, No. 4, 1995, 375–402.

24. M. Rosen, *New Results on the Arithmetic of Elliptic Curves*, Gazette Sc. Math. Québec, Vol. **XIV**, No. 1, 1993, 30–43.

25. K. Rubin and A. Silverberg, *A Report on Wiles' Cambridge Lectures*, Bull Amer. Math. Soc. (New Series) **31**, 1994, 15–38.

26. J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de Gal*($\bar{\mathbf{Q}}/\mathbf{Q}$), Duke Math. J. **54**, 1987, 179–230.

27. J.-P. Serre, *Lettre à J.-F. Mestre*, dans *Current Trends in Arithmetical Algebraic Geometry*, éd. par K. Ribet, Contemporary Mathematics **67**, AMS, 1987.

28. A. van der Poorten, *Notes on Fermat's Last Theorem*, Canadian Math. Society Series of Monographs and Advanced Texts, Wiley Interscience, Jan. 1996.

29. A. Wiles, *Modular Forms, Elliptic Curves, and Fermat's Last Theorem*, Proc. International Congress of Math., 1994, Birkhauser Verlag, Basel, 1995, 243–245.

(C) Autour des travaux de Wiles et Taylor

Les références suivantes se penchent de plus près sur les travaux de Wiles et la démonstration proprement dite de la conjecture de Shimura–Taniyama.

1. J. Coates and S.T. Yau, *Elliptic Curves and Modular Forms*, Comptes Rendus d'une conférence à Hong Kong en 1993, International Press, Cambridge (MA) and Hong Kong, 1995.

2. H. Darmon, F. Diamond et R. Taylor, *Fermat's Last Theorem*, Current Developments in Math. **1**, International Press, 1995, 1–154.

3. H. Darmon, *The Shimura–Taniyama Conjecture, (d'après Wiles)*, (en Russe) Uspekhi Mat. Nauk **50** (1995), no. 3(303), pages 33–82. (Version anglaise à paraître dans Russian Math Surveys).

4. V.K. Murty, ed., *Elliptic Curves, Galois Representations and Modular Forms*, CMS Conference Proc., AMS, Providence RI, 1996.

5. J. Oesterlé, *Travaux de Wiles (et Taylor...), Partie II*, Séminaire Bourbaki 1994-95, exposé No. **804**, 20 pages.

6. K. Ribet, *Galois Representations and Modular Forms*, Bull. AMS (New Series) **32**, 1995, No. **4**, 375–402.

7. J.-P. Serre, *Travaux de Wiles (et Taylor...), Partie I*, Séminaire Bourbaki 1994-95, exposé No. **803**, 13 pages.

8. R.L. Taylor and A. Wiles, *Ring Theoretic Properties of Certain Hecke Algebras*, Annals of Math. **141**, 1995, 553–572.

9. A. Wiles, *Modular Elliptic Curves and Fermat's Last Theorem*, Annals of Math. **141**, 1995, 443–551.

(D) Vidéocassettes

A l'ère de l'audio-visuel, on découvre avec plaisir un grand nombre de vidéocassettes consacrées au dernier théorème de Fermat et à sa démonstration.

1. Fermat Fest, *Fermat's Last Theorem. The Theorem and Its Proof: an Exploration of Issues and Ideas.* Présenté à l'occasion du "Fermat Fest" à San Francisco, CA, le 28 juillet 1993, Vidéo, *Selected Lectures in Mathematics*, AMS, Providence, RI, 1994, (98 min.)

2. B. Mazur, *Modular Elliptic Curves and Fermat's Last Theorem*, Réunion SMC de Vancouver, Août 1993, Vidéo, *Selected Lectures in Mathematics*, AMS, Providence, RI, 1995, (50 min.)

3. K. Ribet, *Modular elliptic curves and Fermat's last theorem*, exposé donné à l'U. George Washington , Washington DC, 1993, Vidéo, *Selected Lectures in Mathematics*, AMS, Providence, RI, 1993, (100 min.)

(E) Fermat et Gauss

Pour en apprendre plus sur les travaux de Fermat et de Gauss, notamment sur la démonstration par Fermat du théorème 3, sur l'équation de Fermat–Pell, et sur l'équation $x^3 + y^3 = 1$:

1. H. Darmon, *Pell's equation and elliptic curves: from Fermat to Wiles*, à paraître, dans les Comptes Rendus de la conférence sur les travaux de Wiles, Août 1995, Boston University, Boston, MA.

2. L.E. Dickson, *History of the Theory of Numbers*, Vol. II, Chelsea Publ. Co., New York, 1971.

3. K. Ireland et M. Rosen, *A Classical Introduction to Modern Number Theory*, 2^e édition, Graduate Texts in Mathematics, **84** Springer-Verlag, New York, 1990, 389 pages.

4. W. Scharlau et H. Opolka, *From Fermat to Minkowski. Lectures on the Theory of Numbers and Its Historical Development,* Traduit de l'allemand par Walter K. Bühler et G. Cornell, Undergraduate Texts in Math., Springer-Verlag, New York-Berlin, 1985, 184 pages.

5. A. Weil, *Fermat et l'équation de Pell*, paru dans *Collected Papers*, Vol. III, Springer-Verlag, New York, 1979, 413–420.

6. A. Weil, *Number Theory. An Approach Through History. From Hammurapi to Legendre*, Birkhauser Boston Inc., Boston, MA, 1984, 375 pages.

(F) Courbes elliptiques

Le lecteur qui désire en savoir plus sur les courbes elliptiques n'aura que l'embarras du choix!

1. J.W.S. Cassels, *Lectures on Elliptic Curves*, London Math. Society Student Texts **24**, Cambridge University Press, 1991, 137 pages.

2. D. Husemöller, *Elliptic Curves*, Graduate Texts in Math. **111**, Springer-Verlag, New York, 1987, 350 pages.

3. H. Kisilevsky and M.R. Murty, *Elliptic Curves and Related Topics*, CRM Proceedings and Lecture Notes, AMS, 1994, 195 pages.

4. A.W. Knapp, *Elliptic Curves*, Mathematical Notes **40**, Princeton U. Press, Princeton, NJ, 1992, 427 pages.

5. S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, New York, 1978, 261 pages.

6. M.R. Murty and V.K. Murty, *Lectures on Elliptic Curves*, Lectures given at Andhra U., India, 1989, 92 pages.

7. M.R. Murty, *Topics in Number Theory*, Lectures given at the Mehta Research Institute, India, 1993, 117 pages.

8. J.H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math., Springer-Verlag, New York, 1992, 281 pages.

9. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, New York, 1992, 400 pages.

10. J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. **151**, Springer-Verlag, New York, 1994, 525 pages.

11. J. Tate, *Rational Points on Elliptic Curves*, Philips Lectures, Haverford College, 1961, notes non publiées.

(G) Fonctions et formes modulaires, et la conjecture de Shimura–Taniyama

1. T. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Graduate Texts in Math. **41**, Springer-Verlag, New York, 1976, 248 pages.

2. J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, Cambridge, 1992, 343 pages.

3. N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2^{nd} edition, Graduate Texts in Math. **97**, Springer-Verlag, New York, 1993, 248 pages.

4. S. Lang, *Introduction to Modular Forms*, Springer-Verlag, New York, 1976, 261 pages.

5. T. Miyake, *Modular Forms*, Springer-Verlag, New York, 1989.

6. M.R. Murty, *Elliptic Curves and Modular Forms*, Bull. Can. Math. **34** (3), 1991, 375–384.

7. A. Ogg, *Modular Forms and Dirichlet Series*, Benjamin, New York, 1969.

8. J.-P. Serre, *A Course in Arithmetic*, 2^{nd} edition, Graduate Texts in Math. **7**, Springer-Verlag, New York, Berlin, Heidelberg, 1973, 115 pages.

Henri DARMON
CICMA
Mathematics Dept.
McGILL University
Montréal
P. Québec
Canada H3A 2K6

Claude LEVESQUE
CICMA
Dép. de Mathématiques
et de Statistique
Université LAVAL
Québec
Canada G1K 7P4