FERMAT PRESQUE VAINCU.

Yves HELLEGOUARC'H.

Plan.

*
* *

"Il n'y a de Science que de ce qui est général."
Aristote.

1. Nature du problème.

On sait que c'est en marge d'une page de son exemplaire des *Arithmétiques* de Diophante (édition de Bachet) que Fermat inscrivit sa fameuse assertion :

Pour tout entier $n > 2$ *et pour tout triplet* $(a, b, c) \in (\mathbb{N}^*)^3$ *on a :*

$$a^n + b^n \neq c^n.$$

Fermat ajouta qu'il en possédait une preuve merveilleuse mais que la marge était trop étroite pour la contenir.

Bien que ce "dernier théorème de Fermat" ait eu une célébrité extraordinaire, notre but n'est pas de nous interroger sur cette célébrité, ni de savoir si la preuve de Fermat pouvait être correcte, mais d'examiner l'ensemble des efforts qui ont été déployés depuis 350 ans pour le démontrer et, plus particulièrement, les derniers événements qui ont défrayé la chronique.

Mais pour commencer nous devons expliquer quelle est la nature du problème : nature nouvelle à l'époque de Fermat qui fut, connne l'on sait, le créateur de la théorie des nombres en exhibant les premiers paradigmes de cette branche des mathématiques ([G_1], [W]).

Le philosophe B. Russel est l'auteur d'une boutade aussi brillante que célèbre selon laquelle *"les mathématiques sont une science où l'on ne sait jamais de quoi l'on parle, ni si ce que l'on dit est vrai"*. Il est curieux de constater que la première partie de cette boutade donne la clé d'un procédé qui permet de démontrer que la seconde partie de cette même boutade est fausse. Nous allons illustrer ce point à l'aide de l'assertion de Fermat afin d'éclairer la nature arithmétique de celle-ci.

Supposez, en effet, qu vous vous trouviez en face d'une soi-disant démonstration de l'assertion de Fermat qui n'utilise que les ressources de l'algèbre.

Alors, en vertu du principe selon lequel "on ne sait pas de quoi l'on parle", on pourrait prendre a, b et c dans $\mathbb{C}$, i. e. le corps des nombres

complexes. Mais dans ce cadre, l'assertion de Fermat est trivialement fausse (n'en déplaise à B. Russell) donc il ne peut exister de démonstration purement algébrique du théorème de Fermat.

Allons plus loin et supposons que, outre l'algèbre, cette "démonstration" utilise la notion d'ordre total, mais rien d'autre. Alors la même démonstration serait valable pour $(a, b, c) \in (\mathbb{R}_+^*)^3$, c'est-à-dire dans un cadre où elle est trivialement fausse, donc cette "démonstration" est fausse.

On peut faire la même remarque dans les anneaux de nombres p-adiques (voir annexe 1) et dans les anneaux qui sont des produits finis d'anneaux de nombre p-adiques (et éventuellement $\mathbb{R}$) et on aurait autant de situations qui prouveraient la fausseté de la "démonstration" (et de la boutade de B. Russel).

On en déduit qu'il ne peut exister une démonstration correcte de l'assertion de Fermat qui n'utilise que l'algèbre, la relation d'ordre total de $\mathbb{N}$ et les propriétés de divisibilité par un nombre fini de nombres premiers : on exprime ceci en disant que le théorème de Fermat est de nature "globale".

Or Fermat a effectivement trouvé une *"route tout à fait singulière"* pour résoudre les problèmes de nature globale. Voici comment il la décrit, avec plus d'humour que de franchise :

> *"Pour ce que les méthodes ordinaires, qui sont dans les livres, étaient insuffisantes à démontrer des propositions si difficiles, je trouvai enfin une route tout à fait singulière pour y parvenir.*
>
> *J'appelai cette manière de démontrer la descente infinie ou indéfinie : je ne m'en servis au commencement que pour démontrer les propositions négatives, comme par exemple :*
>
> *Qu'il n'y a aucun nombre, moindre de l'unité qu'un multiple de 3, qui soit composé d'un carré et du triple d'un autre carré ;*
>
> *Qu'il n'y a aucun triangle rectangle en nombres dont l'aire soit un nombre carré.*
>
> *La preuve se fait par réduction à l'absurde en cette manière :*
>
> *S'il y avait aucun triangle rectangle en nombres entiers qui eût son aire égale à un carré, il y aurait un autre triangle moindre que celui-là qui aurait la même propriété. S'il y en avait un second, moindre que le premier, qui eût la même propriété, il y en aurait, par un pareil raisonnement, un troisième, moindre que ce second, qui aurait la même propriété, et enfin un quatrième, un cinquième, à l'infini en descendant. Or est-il qu'étant donné un nombre, il n'y en a point infinis en descendant moindres que celui-là (j'entends parler toujours des nombres entiers). D'où on conclut qu'il est donc impossible qu'il y ait aucun triangle rectangle dont l'aire soit carrée.*

On infère de là qu'il n'y en a non plus en fractions dont l'aire soit carrée ; car, s'il y en avait en fractions, il y en aurait en nombres entiers, ce qui ne peut être, comme il se peut prouver par la descente.

Je n'ajoute pas la raison d'où j'infère que, s'il y avait un triangle rectangle de cette nature, il y en aurait un autre de même nature moindre que le premier, parce que le discours en serait trop long et que c'est là tout le mystère de ma méthode. Je serai bien aise que les Pascal et les Roberval et tant d'autres savants la cherchent sur mon indication."

Autrement dit, Fermat s'étend sur ce qui est facile et se fait mystérieux sur la partie la plus originale de sa méthode.

Cependant les problèmes traités par Fermat ont été les paradigmes, au sens de Kuhn [K], de la révolution scientifique qui a donné naissance à la théorie des nombres (à ce sujet, voir [G_1] et [W]). Mais la science dite "normale", elle, devra attendre beaucoup plus longtemps pour comprendre ces paradigmes et elle n'est pas encore achevée, comme nous allons le voir.

*
* *

2. Les différents chemins empruntés jusqu'ici.

Il me semble que ces chemins sont au nombre de quatre au plus[1]. Mais s'ils sont peu nombreux, la comparaison des itinéraires qu'ils suivent est très intéressante.

* * * * *

2,1. La route des prisonniers (méthodes "élémentaires").

Il s'agit de la route suivie par des captifs enchaînés à l'arithmétique de $\mathbb{Z}$. Cette route a été empruntée par Fermat lui-même dans le cas où $n = 4$ et également par Lamé (1839) et Lebesgue (1840) pour le cas où $n = 7$.

Bien que la démonstration de Lamé soit techniquement beaucoup plus sophistiquée que celle de Fermat, elle ressemble à celle-ci.

---

1 Dans [G_2] C. Goldstein réduit ce nombre à trois.

L'essentiel de la démonstration repose sur l'impossibilité de l'équation $t^2 = r^4 + 4s^4$ dans le cas où $n = 4$ et de celle de $t^2 = r^4 - \frac{3}{4}r^2s^2 + \frac{1}{7}s^4$ dans le cas où $n = 7$ (naturellement il s'agit de solutions non triviales).

Dans les deux cas, cette impossibilité est prouvée par descente infinie, c'est-à-dire par une méthode à la Fermat.

* * * * *

2,2. Les formes quadratiques (corps quadratiques).

La descente infinie n'était pas la seule arme de Fermat. Il est certain que, pour s'évader de la caverne de Platon, Fermat s'intéressait à d'étranges machines volantes que l'on appelle des formes quadratiques binaires à coefficients entiers (voir [W]).

Par exemple, on peut penser que dans le cas de son assertion et pour des puissances d'ordre p premier impair, Fermat considérait la forme quadratique $X^2 + (-1)^{\frac{p+1}{2}} pY^2$. C'est du moins ainsi que procéda Euler en 1753 pour le degré 3 et Legendre (après Dirichlet) en 1825 pour le degré 5.

La démonstration repose alors sur les propriétés des entiers représentables par les formes quadratiques $X^2 + 3Y^2$ pour le degré 3 et $X^2 - 5Y^2$ pour le degré 5, puis sur une descente infinie. Chemin faisant, on est conduit à faire intervenir le groupe des automorphismes (groupe orthogonal) de ces formes, groupe qui avait été étudié par Fermat lui-même (équations dites de "Pell-Fermat" bien que Pell ne s'en soit jamais occupé !).

* * * * *

2,3. Les extensions cyclotomiques.

Vers la fin de sa vie, Euler s'est aperçu que l'usage des formes quadratiques pour l'exposant 3 revenait à celui de l'anneau $\mathbb{Z}[\sqrt{-3}]$ qui est engendré sur $\mathbb{Z}$ par une racine carrée de - 3.

La voie était ouverte à une généralisation[2] : pour l'exposant premier p, on considérait une racine primitive $p^{\text{ième}}$ de l'unité ζ_p et l'anneau des entiers

2 En fait, on généralise en ce sens que $\mathbb{Z}[\zeta_p]$ est un anneau de Dedekind, tandis que $\mathbb{Z}[\sqrt{-3}]$ n'en est pas un !

cyclotomiques $\mathbb{Z}[\zeta_p]$ correspondant, et on espérait que l'assertion de Fermat serait le reflet en ce bas monde de propriétés, à découvrir, de l'arithmétique supérieure de l'anneau des entiers cyclotomiques. Ce programme a été mené à bien en 1847 par Kummer pour une classe étendue d'exposants p : les nombres premiers réguliers. Or il se trouve que les nombres premiers réguliers sont assez nombreux puisque parmi les nombres premiers ≤ 100, seuls 37, 59 et 67 sont irréguliers[3].

En dehors des outils venus de l'arithmétique de $\mathbb{Z}[\zeta_p]$ on utilisait encore une descente infinie et deux groupes avaient un rôle à jouer : le groupe des unités de l'anneau $\mathbb{Z}[\zeta_p]$ et le groupe de Galois de l'extension cyclotomique de $\mathbb{Q}$ engendrée par ζ_p.

Avec Kummer la science "normale" avait fait un grand pas en avant ; pour la première fois apparaissait une preuve presque générale, i. e. une démonstration s'appliquant à plusieurs exposants p à la fois[4].

* * * * *

2,4. Les courbes elliptiques

C'est aux *Journées Arithmétiques* de 1969, à Bordeaux, que l'auteur de ces lignes a proposé d'associer à toute solution non triviale (a, b, c) de l'équation de Fermat

$$a^p + b^p + c^p = 0$$

où a, b, c sont trois entiers premiers entre eux deux à deux, la cubique affine :

$$\text{E :} \qquad y^2 = x(x + a^p)(x - b^p).$$

À vrai dire, ni l'ordre de a, b, c, ni les signes de ces trois nombres ne sont bien déterminés de sorte que l'on obtient en fait deux courbes à isomorphisme près (i. e. correspondance birationnelle).

On associe donc uniformément à toute solutuion (a, b, c) de n'importe quelle équation de Fermat de degré ≥ 5 (pour des raisons techniques) un grand cerf-volant dont on espère qu'il sera trop beau, ou qu'il vole trop bien, pour appartenir à ce bas monde.

---

3 Malheureusment, on sait prouver qu'il existe une infinité de nombres premiers irréguliers !

4 Une triste ironie veut que l'on ne sache pas démontrer qu'il existe une infinité de nombres premiers réguliers.

Pour montrer ceci deux groupes sont pressentis. La cubique n'ayant pas de point double (parce que la solution (a, b, c) est non triviale)[5], l'ensemble de ses points à coordonnées rationnelles $E(\mathbb{Q})$ possède une structure de groupe particulièrement belle et géométrique : le sous-groupe $E[p]$ des points d'ordre p de $E(\mathbb{Q})$ (auxquels on adjoint l'élément neutre) sera notre premier groupe.

Notre second groupe sera encore un groupe de Galois : ce sera le groupe de Galois de l'extension de $\mathbb{Q}$ engendré par les coordonnées des points d'ordre p de $E(\mathbb{Q})$, i. e. le groupe qui permute ces points sans changer leurs ombres dans la caverne de Platon.

*
* *

3. Courbes elliptiques $E_{A, B, C}$.

La courbe E introduite dans le paragraphe 2,4. présente un défaut majeur : selon toute vraisemblance, elle n'existe pas !

Il se trouve qu'Abel ([A] p. 217) avait rencontré un problème analogue dans ses recherches sur l'impossiblité de la résolution par radicaux des équations générales de degré ≥ 5 et qu'il avait découvert une *"méthode générale"* pour l'étude des problèmes d'impossibilité. Voici ce qu'il en dit ([A] p. 217, cité dans [V] p. 209) :

> *"On doit donner au problème une forme telle qu'il soit toujours possible de le résoudre, ce qu'on peut toujours faire d'un problème quelconque.*
>
> *Au lieu de demander une relation dont on ne sait pas si elle existe ou non, il faut (se) demander si une telle relation est en effet possible."*

C'est ce que nous allons faire en étudiant des courbes $E_{A, B, C}$ qui généralisent la courbe E et qui existent bel et bien.

* * * * *

5 C'est ce qui explique la disparition des "deux cas" du théorème de Fermat dans la démonstration de Wiles : le fait de dire qu'une cubique $E_{A, B, C}$ est elliptique revient à exclure les solutions triviales et place le "deuxième cas" sur un pied d'égalité avec le "premier cas".

3,1. Cubiques de Weierstrass.

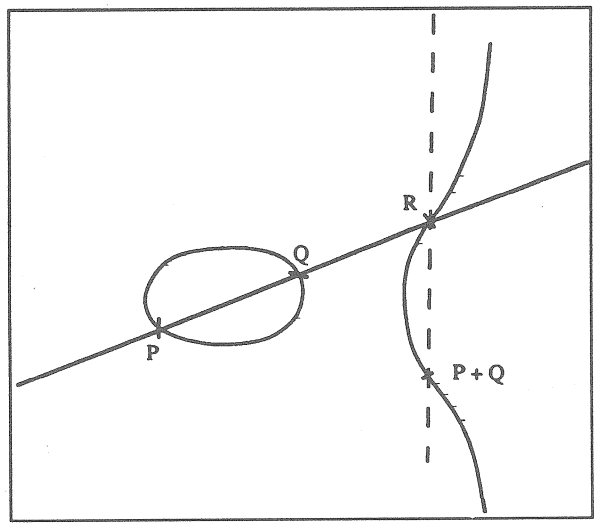
Une courbe elliptique, comme tout objet mathématique aurait dit É. Galois, n'est définie qu'à isomorphisme près. Or il se trouve qu'une courbe elliptique définie sur un corps K peut être représentée par une cubique de Weierstrass, c'est-à-dire une cubique d'équation :

$$(W) : \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

où les coefficients a_i appartiennent à K. On voit facilement que la complétée projective de (W) possède toujours un point rationnel dans $\mathbf{P}_2(K)$, à savoir le point de coordonnées homogènes (0, 1, 0).

Mais toute cubique de la forme (W) n'est pas une courbe elliptique : pour qu'il en soit ainsi, il faut que cette cubique soit non singulière, c'est-à-dire qu'elle ne possède pas de point multiple dans une extension de K (lorsque $a_1 = a_3 = 0$, cela signifie que le polynôme du second membre de l'équation de (W) n'a pas de racine double).

Les points de la complétée projective de (W) dans $\mathbf{P}_2(K)$, c'est-à-dire les points de (W) dans K^2 plus un point "à l'infini", forment un groupe abélien pour la loi d'addition représentée par le dessin suivant :



dans lequel P, Q, R sont alignés et $P + Q$ est le symétrique de R par rapport à l'axe des abscisses (lorsque $a_1 = a_3 = 0$).

On verra facilement que le point à l'infini est l'élément neutre du groupe (le zéro pour l'addition) et que $-P$ est la symétrique de P par rapport à l'axe des abscisses (lorsque $a_1 = a_3 = 0$).

Supposons maintenant que $K \subset \mathbb{Q}$. Soit n un entier ≥ 1, on désigne par $[n]P$ le point obtenu en ajoutant P à lui-même n - 1 fois et on dira que P est un point de n-division si $[n]P = 0$ = point à l'infini de la courbe.

L'ensemble $W[n]$ des points de n-division (ou de n-torsion) de (W) dans $\mathbb{C}$ forme un groupe fini isomorphe à $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

Comme tout automorphisme[6] de $\mathbb{C}$ envoie $W[n]$ en lui-même on voit que, si $P \in W[n]$, l'orbite de P dans le groupe des automorphismes de $\mathbb{C}$ est finie : on dit alors que P est un point algébrique de (W) et on écrit que $W[n] \subset W(\overline{\mathbb{Q}})$ où $\overline{\mathbb{Q}}$ désigne la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$, c'est-à-dire l'ensemble des éléments de $\mathbb{C}$ dont l'orbite, sous l'action du groupe des automorphismes de $\mathbb{C}$ est finie. Le groupe $W[p]$ et le groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$ seront les principaux objets que nous allons considérer, mais avant de le faire, nous avons besoin de quelques définitions élémentaires supplémentaires.

Revenons à un corps quelconque (mais commutatif !). On dit qu'une cubique singulière d'équation :

$$(W) : \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

est de type multiplicatif si son point double admet des tangentes distinctes dans un corps contenant les coefficients.

On voit alors que les points de $W(K)$ distincts du point double forment encore un groupe et, en paramétrant convenablement la cubique, on voit que ce groupe est isomorphe au groupe multiplicatif de K.

On dit que la cubique singulière (W) est de type additif si son point double est à tangentes confondues : on voit de même que les points de $W(K)$ distincts du point double forment encore un groupe et que ce groupe est isomorphe au groupe additif de K.

* * * * *

3,2. Courbes $E_{A,B,C}$.

Définition. *Une relation ABC est une relation du type* $A + B + C = 0$ *où* A, B, C *sont trois entiers premiers entre eux tels que* $ABC \neq 0$.

6 Le groupe des automorphismes de $\mathbb{C}$ est infini. Les automorphismes les plus populaires, l'identité et la conjuguaison, sont les automorphismes continus de $\mathbb{C}$.

À toute relation ABC on peut associer deux courbes elliptiques définies à isomorphisme près par :

$$\begin{cases} E_{A,B,C} & y^2 = x(x-A)(x+B) \\ E_{B,A,C} & y^2 = x(x+A)(x-B) \end{cases}$$

a. Si le nombre premier ℓ ne divise pas ABC, nous pouvons "réduire" les points rationnels de la courbe $E_{A,B,C}$ modulo ℓ : si ℓ ne divise pas le dénominateur de x, il ne divise pas celui de y et le point (x, y) se réduit selon un point de la courbe $y^2 = x\,(x - \overline{A})\,(x + \overline{B})$ à coordonnées dans $\mathbb{F}_\ell$. Si ℓ divise le dénominateur de x, il divise celui de y ; dans ce cas, ou bien encore si (x, y) est le point "à l'infini" de $E_{A,B,C}$, on dit que (x, y) se réduit suivant le point "à l'infini" de $\mathbb{F}_\ell^2$. Dans ce cas, la courbe $y^2 = x\,(x - \overline{A})\,(x + \overline{B})$ est une courbe non singulière définie sur $\mathbb{F}_\ell$ et la réduction est un homomorphisme du groupe des points rationnels de $E_{A,B,C}$ dans celui de la courbe réduite :

$$E_{A,B,C}(\mathbb{Q}) \xrightarrow[\text{mod } \ell]{\text{réd.}} \overline{E}_{\overline{A},\overline{B},\overline{C}}(\mathbb{F}_\ell)$$

On dit que $E_{A,B,C}$ admet une <u>bonne réduction</u> en ℓ.

b. Lorsque ℓ est un nombre premier impair qui divise ABC, la courbe réduite est une cubique à point double de type multiplicatif : on dit que $E_{A,B,C}$ admet une <u>réduction semi-stable</u> en ℓ.

c. Lorsque $\ell = 2$ et que $A \equiv 3 \bmod 4$ et $B \equiv 0 \bmod 32$, on peut remplacer $E_{A,B,C}$ par une courbe birationnellement équivalente qui admet encore une <u>réduction semi-stable</u> en 2.

Résumons tout ceci dans un énoncé :

Si, dans la relation ABC, le nombre A est congru à 3 modulo 4 et le nombre B est divisible par 32, la courbe $E_{A,B,C}$ est <u>semi-stable</u> (i. e. admet bonne réduction ou réduction semi-stable pour tout ℓ premier).

Finalement nous aurons besoin d'une dernière définition. On appelle <u>radical</u> d'un entier n, le produit des nombres premiers (positifs) qui divisent n. Dans le cas d'une courbe $E_{A,B,C}$ du type ci-dessus, le radical de ABC est appelé (pour des raisons qu'on ne peut donner ici) le <u>conducteur</u> de la courbe $E_{A,B,C}$.

*

* *

4. Magie noire ou magie blanche ?

Depuis 1955, les mathématiciens se livrent à des pratiques peu orthodoxes sur les courbes elliptiques et une grande fumée s'élève de leur chaudron : *la conjecture de Shimura-Taniyama-Weil*, présentée d'abord sous une forme quelque peu métaphysique (c'est-à-dire non falsifiable) par Taniyama, puis agrémentée de positivisme[7] par A. Weil. Rappelons que dans ses *Défis aux mathématiciens* Fermat disait :

> *"On sait qu'Archimède n'a pas dédaigné de travailler sur des propositions de Conon qui étaient vraies, mais non prouvées, et qu'il a su les munir de démonstrations d'une haute subtilité. Pourquoi n'espérerais-je pas un semblable secours de vos éminents correspondants, pourquoi, Conon français, ne trouverais-je pas des Archimède anglais ?"*

Or, le 23 juin 1993, un fils de professeur de théologie anglais, dénommé Andrew Wiles, a cru pouvoir affirmer au Newton Institute de Cambridge, qu'une partie des réactions qui se faisaient dans le chaudron, était imputable à la magie blanche et qu'il en résultait une démonstration de la proposition de Fermat (voir [R - S]). Mais aujourd'hui, 28 mai 1994, on n'en est plus si sûr ...

À défaut de preuve, imitons Euclide et énonçons un *"postulat de Wiles"*[8] qui, espérons-le, aura un sort plus brillant que le postulat d'Euclide.

Postulat de Wiles : *Toute courbe elliptique semi-stable définie sur* $\mathbb{Q}$ *est une courbe de Weil.*

L'essentiel étant maintenant postulé, il ne reste plus qu'à décrypter ce jargon ...

Soit E une courbe semi-stable de conducteur N[9], alors ce postulat affirme l'existence d'une série formelle $F(q) = \sum_{n\geq 1} A_n q^n \in \mathbb{Z}[[q]]$ sui possède les propriétés suivantes :

i) F est vecteur propre des opérateurs de Hecke.

ii) $A_1 = 1$ et si ℓ est premier ne divisant pas N

---

7 Mise sous une forme falsifiable : on peut vérifier algorithmiquement cette conjecture sur toute courbe elliptique donnée.

8 C'est naturellement un cas particulier de la conjecture de Shimura-Taniyama-Weil.

9 Le conducteur d'une courbe elliptique définie sur $\mathbb{Q}$ est un entier facile à calculer.

$$A_\ell = \ell + 1 - \#\overline{E_\ell}(\mathbb{F}_\ell)$$

où $\overline{E_\ell}$ désigne la courbe elliptique définie sur $\mathbb{F}_\ell$ déduite de E par réduction modulo ℓ.

iii) L'application $z \mapsto F\left(e^{2i\pi z}\right)$ est une "forme modulaire parabolique de poids 2 pour le groupe $\Gamma_0(N)$ définie sur le demi-plan de Poincaré $\mathcal{H}$".

Nous renvoyons à l'annexe 3 pour la définition de ces termes. Pourtant nous pouvons dire tout de suite que $\Gamma_0(N)$ est simplement le groupe

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}) \, ; \, ad - bc = 1, c \equiv 0 \mod N \right\}.$$

L'ensemble des conditions i) ii) et iii) est extrêmement contraignant et ce qui est surprenant c'est que l'on puisse effectivement trouver F. En fait, et ce point sera l'élément qui portera le coup de grâce à la résistance de l'assertion de Fermat, la condition iii) est suffisamment forte pour être irréalisable pour $N = 2$ (et plus généralement pour $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13$). Cela se voit en calculant la dimension de l'espace vectoriel $S_2(\Gamma_0(N))$ de toutes les formes modulaires paraboliques de poids 2 pour le groupe $\Gamma_0(N)$ (voir [Sh] ou [H]).

Exemple : On a pu remarquer que le nombre premier 11 manque dans la liste ci-dessus des conducteurs N pour lesquels iii) est irréalisable. C'est qu'en effet, il existe une forme parabolique de poids 2 qui est modulaire pour le groupe $\Gamma_0(11)$.

Pour $z \in \mathcal{H}$, demi-plan de Poincaré, nous savons que la fonction êta de Dedekind est définie par :

$$\eta(z) = e^{2i\pi z/24} \prod_{n \geq 1} \left(1 - e^{2i\pi n z}\right)$$

et que cette fonction vérifie les équations fonctionnelles :

$$\begin{cases} \eta(z+1) = e^{\pi i/12} \eta(z) \\ \eta(-1/z) = (-iz)^{1/2} \eta(z) \end{cases}$$

dans lesquelles la racine carrée prolonge à $\mathcal{H}$ la détermination qui est positive sur $\mathbb{R}$.

Maintenant si nous considérons la fonction

$$f(z) = \eta(z)^2 \eta(11z)^2$$

nous pouvons facilement vérifier que f est une forme parabolique de poids 2 pour le groupe $\Gamma_0(11)$.

La série formelle $F(q)$ qui lui est associée est particulièrement agréable, c'est

$$F(q) = q\prod_{n=1}^{\infty}\left(1-q^n\right)^2\left(1-q^{11n}\right)^2 = \sum_{m=1}^{\infty} A_m q^m$$

Comme l'espace $S_2(\Gamma_0(11))$ est de dimension 1 (c'est une droite), que f appartient à cet espace et n'est pas nulle (puisque son premier coefficient A_1 est égal à 1), on voit que $F(q)$ est vecteur propre de tous les opérateurs de Hecke dont l'indice est premier à 11.

Maintenant, si l'on considère la courbe elliptique

$$E: \quad y^2 - y = x^3 - x^2$$

on constate (on peut démontrer) que pour tout nombre premier $\ell \neq 11$, on a :

$$A_\ell = \ell + 1 - \#\overline{E_\ell}(\mathbf{F}_\ell).$$

Revenant en arrière, on voit que E est une courbe semi-stable de conducteur $N = 11$ et que $F(q)$ répond bien aux conditions i), ii) et iii).

*
* *

5. Conjecture de Serre.

Dans le paragraphe 3, nous avons donné une définition "du" corps $\overline{\mathbb{Q}}$ de tous les nombres algébriques ; ensemble des nombres complexes qui n'admettent qu'un nombre fini de conjugués. En fait il s'agit ici de l'avatar de $\overline{\mathbb{Q}}$ qui apparaît à l'intérieur du corps des nombres complexes (voir annexe 2) : comme tout objet mathématique, le corps $\overline{\mathbb{Q}}$ n'est défini qu'à isomorphisme près (d'où les guillemets).

Or il se trouve qu'un groupe de magiciens, cachés derrière le mur, s'amusent à permuter les objets de $\overline{\mathbb{Q}}$ sans modifier leurs ombres dans la caverne de Platon tout en respectant les règles structurelles qui relient entre eux ces divers objets (addition, soustraction, multiplication, division). Ce groupe de magiciens est appelé le groupe de Galois absolu et se note $\mathrm{Aut}(\overline{\mathbb{Q}})$ ou $\mathrm{Gal}_{\mathbb{Q}}$.

Depuis longtemps J.-P. Serre s'intéresse à ce groupe et il a été conduit, en 1987, à reprendre sous une forme plus falsifiable une conjecture qu'il avait déjà émise en 1973 ; de sorte que, désormais, K. Popper[10] ne puisse plus rien trouver à redire !

Les objets auxquels s'intéresse J.-P. Serre sont (entre autres) les homomorphismes de groupes continus :

$$\rho : G_{\mathbb{Q}} \to GL(V)$$

où V désigne un espace vectoriel de dimension 2 défini sur un corps fini $\mathbb{F}_p$ et où p désigne un nombre premier.

Nous avons expliqué dans le paragraphe 3,1. comment on peut associer à toute courbe elliptique E définie sur $\mathbb{Q}$ un tel espace vectoriel $V = E[p]$ et nous avons dit que $E[p]$ est contenu dans $\overline{\mathbb{Q}}^2$, de sorte que $\mathrm{Aut}(\overline{\mathbb{Q}})$ agit naturellement sur $E[p]$ puisque nous avons supposé que E est définie sur $\mathbb{Q}$.

Cette action donne un objet du type cherché : on l'appelle une "représentation continue" de $G_{\mathbb{Q}}$

$$\rho : G_{\mathbb{Q}} \to GL(V)$$

À cet objet ρ, la conjecture de Serre associe de manière précise les trois compères suivants :

1. Un conducteur d'Artin qui est un entier N positif défini à partir de ρ par une recette déjà ancienne et vénérable,

2. Un caractère de Dirichlet ε qui est un homomorphisme de groupes :

$$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{F}_p^*$$

du groupe multiplicatif des unités de l'anneau quotient $\mathbb{Z}/N\mathbb{Z}$ dans le groupe multiplicatif des éléments inversibles du corps $\mathbb{F}_p$,

3. un poids k qui est un entier ≥ 2 défini par une recette précise qui a été concoctée par J.-P. Serre.

> Exemple :
> Si l'on suppose que E est une courbe $E_{A,B,C}$ associée à une hypothétique solution (a, b, c) de l'équation de Fermat, c'est-à-dire si $A = a^p$, $B = b^p$, $C = c^p$ et si $p \geq 5$ et $A \equiv 3 \bmod 4$, $B \equiv 0 \bmod 32$, on a ([Se_2] ou [H]) : $N = 2$, ε = caractère trivial, $k = 2$.

10 Il me paraît probable que le simple bon sens, beaucoup plus que K. Popper, a été le guide de J.-P. Serre.

Lorsque nos trois compères sont aux mains des prisonniers de la caverne de Platon, la conjecture de Serre leur fait cadeau d'une série $f = \sum_{n\geq 1} a_n q^n \in \bar{\mathbf{F}}_p[[q]]$, non nulle, qui appartient à un certain espace vectoriel $S_2(N)$ et qui vérifie des propriétés analogues à la série F du paragraphe précédent (voir annexe 3).

Exemple :
Si l'équation de Fermat avait une solution (pour une valeur de $p \geq 5$) la conjecture de Serre entraînerait l'existence d'un élément non nul dans $S_2(2)$.

* * *

6. Théorème de Ribet.

L'épilogue de notre histoire se trouve dans le théorème suivant, pressenti par G. Frey, qui a été démontré par K. A. Ribet vers 1987.

Théorème de Ribet : *Soit une représentation "modulaire"* ρ

$$\rho : G_{\mathbf{Q}} \to GL_2(\mathbf{F}_p)$$

absolument irréductible, finie en p, de niveau N et de poids 2. Alors on peut choisir pour N le conducteur d'Artin de la représentation.

Nous ne pouvons donner ici la définition de tous les termes techniques de ce théorème (pour ceci on renvoie à [O] ou [H]) et encore moins sa démonstration ! (voir [Rt]).

Corollaire 1 : *Si* $p \geq 5$, *le postulat de Wiles entraîne le théorème de Fermat.*

Démonstration. Supposons le contraire et désignons par (a, b, c) une solution primitive non triviale de l'équation de Fermat de degré p.
Prenons $E = E_{a^p, b^p, c^p}$ et considérons la représentation

$$\rho_E : G_{\mathbf{Q}} \to GL(E[p]).$$

Elle vérifie les conditions énumérées dans l'énoncé du théorème de Ribet, à ceci près que nous ne savons pas encore que ρ_E est "modulaire".

Mais le postulat de Wiles entraîne l'existence d'une forme modulaire $F \in S_2(\Gamma_0(N_E))$ telle que $F(q) = \sum_{n\geq 1} A_n q^n$, et

$$\begin{cases} \mathrm{tr}(Frob_\ell) & \equiv \ell + 1 - \#\tilde{E}_\ell(\mathbb{F}_\ell) = A_\ell \\ \det(Frob_\ell) & \equiv \ell \end{cases} \pmod{p}$$

lorsqu'il y a bonne réduction en ℓ. Le symbole $Frob_\ell$ désigne une classe d'éléments remarquables de $G_{\mathbb{Q}}$ qui est attachée canoniquement au nombre premier ℓ.

Donc, ρ_E est une "représentation modulaire" associée à $f = \tilde{F} \in S_2(N_E)$.

Mais nous avons vu dans le paragraphe précédent que le conducteur d'Artin de ρ_E est $N_\rho = 2$, donc il doit exister $g \in S_2(2)$ telle que ρ_E provienne de g. Or ceci est impossible puisque $S_2(\Gamma_0(2)) = \{0\}$.

Peut-être éprouvez-vous un sentiment d'incrédulité devant ce tour de passe-passe ? Ne se moque-t-on pas des prisonniers de la caverne de Platon ?

Le corollaire suivant montre que la théorie est falsifiable.

Considérons l'équation :

$$\alpha x^p + \beta y^p + \gamma z^p = 0$$

où α, β, γ sont des entiers premiers entre eux deux à deux, sans puissance $p^{\text{ième}}$ et tels que $2p$ ne divise pas $\alpha\beta\gamma$.

Corollaire 2 : *Le postulat de Wiles entraîne que, si $p \geq 5$ et si l'équation précédente admet une solution primitive non triviale (a, b, c), il existe $F \in S_2(\Gamma_0(\mathrm{rad}2\alpha\beta\gamma))$, vecteur propre normalisé des opérateurs de Hecke, telle que l'on ait* [11]

$$A_\ell \equiv \ell + 1 - \#\tilde{E}_{A,B,C}(\mathbb{F}_\ell) \pmod{p}$$

pour tous les ℓ premiers ne divisant pas $2\alpha\beta\gamma abc$.

Exemple :

Dans le cas où $p \geq 11$ et où π est un nombre premier appartenant à l'ensemble $S = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$, J.-P. Serre ([$Se_2$] pp. 202-203) a montré que les équations

$$x^p + y^p + \pi^\alpha z^p = 0$$

avec $\alpha \geq 0$ et $\pi \neq p$ n'admettent pas de solutions non triviales.

11 Sous réserve que $E_{A,B,C}$ soit choisie correctement.

Remarques :

1. Henri Darmon a appliqué la même démarche aux équations diophantiennes :

$$x^n + y^n = z^2,\ x^n + y^n = z^3,\ Ax^p + By^q = Cz^r \text{ et } z^m = F(x, y).$$

Voir [D_1] et [D_2 - G].

2. Le paradigme décrit ci-dessus a bourgeonné en un archipel de problèmes et de phénomènes nouveaux, dont l'un des plus remarquables est la "conjecture *abc*". L'étude de ce domaine sort du cadre de cet exposé et on ne peut mieux faire que de renvoyer le lecteur curieux à l'article d'un orfèvre en la matière [O]. Rappelons ce que dit Kuhn au sujet des paradigmes ([K] p. 46) :

> *"Le succès d'un paradigme est en grande partie au départ une promesse de succès, révélée par des exemples choisis et encore incomplets. La science normale consiste à réaliser cette promesse, en étendant la connaissance des faits que le paradigme indique comme particulièrement révélateurs, en augmentant la corrélation entre ces faits et les prédictions du paradigme, et en ajustant davantage le paradigme lui-même."*

*
* *

7. Conclusion en trois remarques.

Une première remarque sera de faire un parallèle entre la recherche dans les sciences empiriques et la recherche actuelle concernant le problème de Fermat : on formule une hypothèse (appelée ici conjecture) qui est motivée par ce que l'on sait d'une foule de situations analogues et qui est en harmonie avec le reste de l'édifice mathématique (aspect esthétique) mais qui doit être suffisamment précise pour être falsifiable.

Comme en sciences expérimentales, la vérifiabilité de la théorie échappe à l'expérience, et les expériences cruciales (appelées ici contre-exemples) doivent se borner à délimiter le domaine de validité des énoncés.

Pourtant la vérifiabilité existe en mathématiques, c'est bien ce qui distingue les mathématiques des sciences expérimentales, mais elle est d'un autre ordre et d'une nature inconnue dans les sciences empiriques. Cette vérification ne peut être que le résultat d'une démonstration (ce qui

manque pour l'instant au "Postulat de Wiles") : en mathématiques, on peut parfois savoir si ce que l'on dit est "vrai" !

Une seconde remarque sera de noter combien l'attitude de la science "normale" vis-à-vis de l'assertion de Fermat, dans les vingt-cinq dernières années, a suivi les schémas décrits par Kuhn dans [K].

Dans les années 70, cette attitude était faite de scepticisme vis-à-vis de cette assertion. On considérait que celle-ci était peut-être fausse et que, au mieux, elle n'avait pas un caractère suffisamment général pour mériter le statut d'énigme significative. Quinze ans après, le théorème de Ribet a transformé ce problème en énigme paradigmatique d'une nouvelle planète de la théorie des nombres ! La communauté mathématique a changé sa perception de la question et, tout à coup, elle est passée d'un désintérêt plus ou moins courtois à l'enthousiasme le plus vif. Qu'il s'agisse d'un changement brutal dans *"la perception et l'évaluation des données familières"* qui présente certains des caractères d'une "révolution scientifique" au sens de Kuhn ([K] p. 11) se voit très clairement en consultant le remarquable ouvrage d'érudition que P. Ribenboim [Rn] a fait paraître en 1979 : les principaux résultats de ma thèse y sont cités, sauf le dernier théorème, c'est-à-dire celui qui allait conduire justement à la nouvelle approche[12]. La science "normale" de 1979, était aussi insensible au nouveau point de vue que la sicence "normale" de 1989 l'est à l'ancien !

Une troisième et dernière remarque sera de noter la distance qui nous sépare désormais de Descartes et de l'induction positiviste. Qu'est devenue la prudence du philosophe masqué qui nous incite à avancer *"comme par degrés"* ? On est loin de ses conseils de défiance si souvent répétés :

> *"Si dans la série des choses à rechercher, il s'en présente quelqu'une, dont notre entendement ne puisse avoir suffisamment bien l'intuition, il faut s'arrêter là, il ne faut pas examiner ce qui suit, mais s'abstenir d'un travail superflu"* (*Règle VIII*).

Dans les grandes conjectures qui innervent la théorie des courbes elliptiques, on a vu que l'intuition, l'imagination, le sens holistique et l'enthousiasme sont au pouvoir. Le théorème de Ribet n'aurait que renforcé le scepticisme d'un Descartes vis-à-vis du Postulat de Wiles. C'est le contraire qui s'est produit : ici la prudence cartésienne a été jetée par-dessus les moulins !

*
* *

12 Selon Kuhn ([K] p. 98), la science normale est une entreprise qui n'est pas dirigée vers les nouveautés et tend d'abord à les supprimer.

Annexe 1 : Nombres p-adiques.

Le corps des réels est loin d'être le seul corps normé complet contenant $\mathbb{Q}$ dans lequel celui-ci est dense, et ceci même à isomorphisme près.

En effet pour tout nombre premier p on peut construire un corps $\mathbb{Q}_p$ possédant ces propriétés et les différents corps obtenus ne sont pas isomorphes entre eux ni isomorphes à $\mathbb{R}$.

Comme pour $\mathbb{R}$ on dispose de plusieurs constructions possibles qui, pour p donné, fournissent le même objet à isomorphisme près. Une construction qui serait très agréable aux élèves des écoles primaires est la suivante. Écrivons les nombres réels en base p en prenant, par exemple, pour système de chiffres l'ensemble $S = \{0, 1, 2, ..., p - 1\}$.

Un nombre réel positif $\leq p$ s'écrit dans ce système :

$$a_0, a_1\, a_2\, a_3 \ldots$$

et l'addition de deux nombres de cette forme est donnée par la règle du report à gauche de la retenue.

Exemple : Si $p = 3$, on a :

$$\begin{array}{rcccccc} & & \leftarrow & \leftarrow & \leftarrow & \leftarrow & \\ & 0, & 1 & 1 & 1 & 1 & \ldots \\ + & 0, & 1 & 1 & 1 & 2 & \ldots \\ \hline & 1, & 0 & 0 & 0 & ? & \end{array}$$

Bien que cette règle soit considérée comme simple, elle est loin de l'être[13] puisqu'il faut connaître le développement des deux nombres jusqu'à l'infini pour être capable décrire le résultat de l'addition !

On obtient un résultat beaucoup plus simple si l'on reporte la retenue sur la droite.

13 Cette écriture présente également d'autres défauts : elle n'est pas unique, l'addition de deux nombres $\leq p$ ne donne pas nécessairement un nombre $\leq p$ etc.

Exemples : Si $p = 3$, on a :
Premier exemple :

$$\begin{array}{rccccc} & & & & & \overrightarrow{} \\ & 0, & 1 & 1 & 1 & 1 \ \ldots \\ + & 0, & 1 & 1 & 1 & 2 \ \ldots \\ \hline & 0, & 2 & 2 & 2 & 0 \ \ldots \end{array}$$

Second exemple :

$$\begin{array}{rccccc} & \rightarrow & \rightarrow & \rightarrow & \rightarrow & \rightarrow \\ & 1, & 1 & 1 & 1 & 1 \ \ldots \\ + & 2, & 1 & 1 & 1 & 1 \ \ldots \\ \hline & 0, & 0 & 0 & 0 & 0 \ \ldots \end{array}$$

On voit que, même si l'on ne sait pas écrire un nombre jusqu'à l'infini, les premiers termes d'une addition sont connus avec certitude, que les nombres ci-dessus forment un anneau (en modifiant aussi la multiplication par un report à droite), que $\mathbb{Z}$ est contenu dans cet anneau[14], etc.

L'anneau ainsi obtenu est appelé l'anneau des entiers p-adiques et est noté $\mathbb{Z}_p$: on le munit de la topologie qui consiste à considérer comme "petits" les nombres qui commencent par beaucoup de zéros. Si l'on ajoute un nombre fini arbitraire de chiffres à gauche de la virgule aux nombres de $\mathbb{Z}_p$, on obtient le corps des nombres p-adiques que l'on note $\mathbb{Q}_p$. Le corps $\mathbb{Q}_p$ est le corps des fractions de $\mathbb{Z}_p$; il contient donc le corps des rationnels $\mathbb{Q}$. On peut le munir d'une valeur absolue p-adique qui en fait un corps normé complet dans lequel $\mathbb{Q}$ est dense.

Exercice :
On montrera que la série :

$$\left(1+p^p\right)^{1/p} = \sum_{i=0}^{\infty} \binom{1/p}{i} p^{ip}$$

est convergente dans $\mathbb{Q}_p$ et on en déduira que l'équation de Fermat possède une solution non triviale dans $\mathbb{Q}_p$ (elle en possède en fait une infinité).

L'anneau des entiers p-adiques $\mathbb{Z}_p$ possède une propriété importante que l'on appelle la réduction modulo p.

14 On identifie 0 à 0, 00... et 1 à 1, 00...

Si $\bar{a}$ désigne la classe modulo p du nombre entier a, alors l'application

$$\begin{cases} a_0, a_1, a_2 \ldots \mapsto \overline{a_0} \\ \mathbf{Z}_p \qquad\qquad \to \mathbf{F}_p \end{cases}$$

est un homomorphisme d'anneaux commutatifs unitaires.

Une autre manière d'exprimer la même chose consiste à dire que les entiers p-adiques $a_0, a_1, a_2 \ldots$ dont le premier chiffre a_0 est nul, forment un idéal maximal de $\mathbf{Z}_p$.

*
* *

Annexe 2 : Nombres algébriques.

1. Dans le paragraphe 3,1. nous avons exhibé un avatar du corps des nombres algébriques que nous avons noté $\overline{\mathbf{Q}}$ (un peu abusivement).

La définition que nous avons donné de $\overline{\mathbf{Q}}$ est la suivante : $\overline{\mathbf{Q}}$ est l'ensemble des $z \in \mathbf{C}$ qui n'ont qu'un nombre fini de conjugués sous l'action de Aut($\mathbf{C}$).

Cette définition est à la fois simple et puissante puisqu'elle rend évident le fait que $\overline{\mathbf{Q}}$ est un corps qui contient $\mathbf{Q}$.

Mais c'est une définition pour les magiciens qui agitent les marionnettes dont les prisonniers de la caverne de Platon ne voient que les ombres.

Définition pour les prisonniers : *Un nombre $z \in \mathbf{C}$ est dit algébrique (sur $\mathbf{Q}$) s'il est racine d'un polynôme non nul à coefficients rationnels (coefficients dans $\mathbf{Q}$).*

L'ensemble de ces nombres algébriques contient donc $\overline{\mathbf{Q}}$: on montre que c'est $\overline{\mathbf{Q}}$.

2. Donnons-nous maintenant un nombre premier quelconque p.

On démontre que le corps des nombres p-adiques $\mathbb{Q}_p$ (voir annexe 1) est contenu dans un corps $\mathbb{C}_p$ qui joue un peu (pour $\mathbb{Q}_p$) le rôle du corps des nombres complexes (pour $\mathbb{R}$) : il est algébriquement clos, métrisable et complet. Nous pouvons répéter pour $\mathbb{C}_p$ ce que nous avons dit plus haut pour $\mathbb{C}$ et nous voyons que le corps des nombres algébriques possède un nouvel avatar dans $\mathbb{C}_p$: c'est l'ensemble des $z \in \mathbb{C}_p$ qui n'admettent qu'un nombre fini de conjugués sous l'action de $\mathrm{Aut}(\mathbb{C}_p)$.

Si nous désignons ce corps par $\overline{\mathbb{Q}}^{(p)}$, nous nous trouvons devant une infinité d'avatars du corps des nombres algébriques :

$$\overline{\mathbb{Q}}, \overline{\mathbb{Q}}^{(2)}, \overline{\mathbb{Q}}^{(3)}, \overline{\mathbb{Q}}^{(5)}, \ldots$$

lequel préférer ?

En général cette question n'a pas de sens : tous ces corps sont isomorphes entre eux, ils sont indiscernables (n'en déplaise à Leibniz) en tant qu'objets algébriques, seules les topologies dont ils héritent de leur plongement dans $\mathbb{C}$, $\mathbb{C}_2$, $\mathbb{C}_3$, $\mathbb{C}_5$, ... peuvent permettre de les distinguer.

Ainsi B. Russell a-t-il bien raison de dire que les mathématiciens ne savent pas de quoi ils parlent : la réalité mathématique (comme celle de la physique quantique) n'est pas leibnizienne : elle n'obéit pas au fameux *principe d'identité des indiscernables* énoncé par Leibniz en 1716, dans une lettre à Clarke[15].

*
* *

15 Ce principe affirme que si deux objets ont les mêmes propriétés, ils sont identiques.

Annexe 3 : Formes modulaires.

1. On attribue à M. Eichler la boutade selon laquelle il n'y a que cinq opérations en arithmétique : l'addition, la soustraction, la multiplication, la division et ... les formes modulaires.

La première apparition officielle de fragments de formes modulaires - étant entendu qu'un "fragment de forme modulaire" n'est pas une forme modulaire ! - semble s'être produite en 1713, année de la parution posthume de l'*Ars Conjectandi* de Jakob Bernoulli.

On trouve en effet dans cet ouvrage, les trois séries (fragments de fonctions thêta) :

$$\sum_{n=0}^{\infty} m^{\frac{1}{2}n(n+3)}, \quad \sum_{n=0}^{\infty} m^{\frac{1}{2}n(n+2)}, \quad \sum_{n=0}^{\infty} m^{n^2}.$$

Seconde apparition en 1748 dans l'ouvrage d'Euler *Introductio in Analysin Infinitorum* sous forme des produits infinis appartenant aux types suivants :

$$\prod_{n=1}^{\infty}\left(1\pm x^{n}\right), \quad \prod_{n=1}^{\infty}\left(1\pm x^{2n}\right), \quad \prod_{n=1}^{\infty}\left(1\pm x^{2n-1}\right)$$

qui sont étroitement liés aux séries précédentes.

De nos jours, la théorie a été pronfondément normalisée et on écrit $q = e^{2i\pi z}$ à la place de m ou de x^2, z désignant un élément du demi-plan de Poincaré $\mathcal{H}$. Par définition $\mathcal{H}$ est l'ensemble des nombres complexes dont la partie imaginaire est strictement positive (de sorte que $|q| < 1$). Il est clair que q ne change pas lorsque l'on remplace z par $z + 1$, mais les fonctions ci-dessus possèdent des propriétés d'invariance beaucoup plus riches comme nous allons le voir sur un exemple.

Exemple : Si l'on pose pour $z \in \mathcal{H}$,

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 z} = \sum_{n=-\infty}^{\infty} q^{\frac{n^2}{2}}$$

on démontre que :

$$\theta\left(\frac{-1}{z}\right) = \left(\frac{z}{i}\right)^{1/2} \theta(z)$$

pour une certaine détermination de la racine carrée. Par ailleurs, $\theta(z + 2) = \theta(z)$.

2. Formes modulaires de poids k pour $\Gamma_0(N)$.

Nous avons déjà donné dans le paragraphe 4, une définition du groupe $\Gamma_0(N)$. Une forme faiblement modulaire de poids k pour $\Gamma_0(N)$ est une fonction holomorphe $f : \mathcal{H} \to \mathbb{C}$ qui vérifie la relation :

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

quel que soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

Exemples :

1. La série d'Eisenstein :

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)\, q^n$$

où $\sigma_3(n)$ désigne la somme des cubes des diviseurs de n, vérifie :

$$E_4\left(-\frac{1}{z}\right) = z^4 E_4(z) ;$$

c'est donc une fonction faiblement modulaire de poids 4 pour le groupe $\Gamma_0(1)$.

2. La fonction $f(z) = F(e^{2i\pi z})$ avec

$$F(q) = q \prod_{n=1}^{\infty} \left(1 - q^n\right)^{24}$$

est telle que

$$f\left(\frac{-1}{z}\right) = z^{12} f(z) ;$$

c'est donc une fonction faiblement modulaire de poids 12 pour le groupe $\Gamma_0(1)$ (voir [Se$_1$] pour plus de détails).

Une forme modulaire parabolique de poids 2 est une forme faiblement modulaire de poids 2, qui est holomorphe et nulle à l'infini (ce qui signifie que $F(q) = \sum_{n\geq 1} A_n q^n$ est convergente dans un voisinage de l'origine) et qui est holomorphe et nulle aux "pointes" de $\Gamma_0(N)$ (ce qui signifie que pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, la fonction $z \mapsto (cz+d)^{-2} f\left(\frac{az+b}{cz+d}\right)$ admet un développement

en série en $q^{1/N}$ analogue à celui de F : pas de terme constant et convergence dans un voisinage de l'origine). Les formes modulaires paraboliques de poids 2 pour $\Gamma_0(N)$ forment un espace vectoriel complexe dont la dimension peut être facilement calculée par les prisonniers de la caverne.

On désigne habituellement cet espace par $S_2(\Gamma_0(N))$ et on pose $g = \dim_{\mathbb{C}} S_2(\Gamma_0(N))$. Alors on a :

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}, \text{ où}$$

$$\begin{cases} \mu = N \sum_{l \mid N} \left(1 + l^{-1}\right) \\ \nu = \prod_{l \mid N} \left(1 + \left(\frac{-1}{l}\right)\right) & \text{si 4 ne divise pas } N, \text{ zéro sinon} \\ \nu_3 = \prod_{l \mid N} \left(1 + \left(\frac{-3}{l}\right)\right) & \text{si 9 ne divise pas } N, \text{ zéro sinon} \\ \nu_\infty = \sum_{\substack{d \mid N \\ d>0}} \varphi\left(\left(d, \frac{N}{d}\right)\right) & \text{où } \varphi \text{ est la fonction d'Euler} \end{cases}$$

les symboles de Legendre $\left(\frac{-1}{\ell}\right)$ et $\left(\frac{-3}{\ell}\right)$ étant définis comme suit :

$$\left(\frac{-1}{\ell}\right) = \begin{cases} 0 & \text{si } \ell = 2 \\ 1 & \text{si } \ell \equiv 1 \mod 4 \\ -1 & \text{si } \ell \equiv 3 \mod 4 \end{cases} ; \quad \left(\frac{-3}{\ell}\right) = \begin{cases} 0 & \text{si } \ell = 3 \\ 1 & \text{si } \ell \equiv 1 \mod 3 \\ -1 & \text{si } \ell \equiv 2 \mod 3 \end{cases} .$$

Pour plus de détails, voir [Sh, pp. 23-25].

Exemples :

1. La fonction $E_4(z)$ est une forme modulaire de poids 4 pour $\Gamma_0(1)$, mais ce n'est pas une forme parabolique (elle vaut 1 à l'infini).

2. La série F du paragraphe 4 correspond à une forme parabolique de poids 2 de $\Gamma_0(11)$. Toute forme de $S_2[\Gamma_0(11)]$ est d'ailleurs égale à λF avec $\lambda \in \mathbb{C}$.

3. Opérateurs de Hecke restreints à $S_2(\Gamma_0(N))$.

Ils s'obtiennent en composant entre eux les opérateurs de Hecke d'indice premier.

Lorsque le nombre premier ℓ ne divise pas N, l'opérateur de Hecke d'indice ℓ est défini par la formule :

$$T_\ell(F) = \sum_{n \geq 1} A_{\ell n} q^n + \ell \sum_{n \geq 1} A_n q^{\ell n}$$

Voir [Se_1] pour plus de précisions.

4. Espace $S_2(N)$.

On peut le définir d'une manière vague comme l'ensemble des réductions "modulo p" (voir annexe 1) des éléments de $S_2(\Gamma_0(N))$ dont les coefficients $A_n \in \overline{\mathbb{Q}}^{(p)}$ sont des "entiers algébriques" (voir annexe 2 pour $\overline{\mathbb{Q}}^{(p)}$, la réduction se fait modulo un idéal maximal de l'anneau des entiers de $\overline{\mathbb{Q}}^{(p)}$).

Exemple :
Si l'on considère la série F du paragraphe 4 :

$$F(q) = q\prod_{n=1}^{\infty}\left(1-q^n\right)^2\left(1-q^{11n}\right)^2$$

et si l'on prend $p = 11$, on a :

$$f(q) = \tilde{F}(q) = q\prod_{n=1}^{\infty}\left(1-q^n\right)^{24} \in \mathbb{F}_{11}[[q]] \ .$$

Pour une définition plus précise, voir [Se_2, pp. 192-194] ainsi que [Sh].

*
* *

Post-scriptum[16].

Il semble que, vexées d'être traitées si légèrement par Wiles en 1993, les mânes de Descartes aient suggéré au Dieu des Mathématiques de jeter quelques obstacles sous les pas dudit Wiles.

Mais, bien sagement, ce dernier sut écouter son collègue Richard Taylor qui lui conseillait de revenir sur sa route et de réexaminer une approche qu'il avait naguère explorée. C'est alors que, le 19 septembre 1994, il vit dans un éclair qu'un procédé récemment découvert par de Shalit ouvrait un chemin plus direct vers la conjecture de Taniyama...

16 Cet *addendum* a été rédigé après les récents développements des travaux d'A. Wiles.

Le "postulat de Wiles", tel qu'il est énoncé dans l'article qui précède, est donc maintenant un théorème dont on trouvera la démonstration complète dans deux articles signalés dans la bibliographie, aux références [T - Wi_1] et [Wi_2].

Cependant le filon découvert par Wiles (et Taylor) est si riche que d'autres ont déjà pris la relève. On sait maintenant qu'il suffit qu'une courbe elliptique soit semi-stable en 3 et en 5, pour être une courbe de Weil. Désormais la conjecture de Shimura-Taniyama-Weil semble bien près de tomber, elle aussi !

*
* *

Références bibliographiques.

[A] ABEL, N. H.
- *Œuvres* ; tome II. Christiana, 1881.

[D_1] DARMON, H.
- *"The equations* $x^n + y^n = z^2$ *and* $x^n + y^n = z^3$*"*, in *Int. Math. Res. Notices* 10 (1993), pp. 263-274.

[D_2 - G] DARMON, H., GRANVILLE, A.
- *"On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$*"*, in *University of Georgia Maths. Preprints* n° 28, vol. II (1994).
- Cet article est paru depuis dans le *Bulletin of the London Math. Soc.*, n° 129, vol. 27, part 6, nov. 1995, pp. 513-543.

[G_1] GOLDSTEIN, C.
- *"Le métier des nombres aux XVII*^{ème} *et XIX*^{ème} *siècles"*, in *Éléments d'Histoire des Sciences*, sous la dir. de M. Serres, Éd. Bordas. Paris, 1989.

[G_2] - *"Autour du théorème de Fermat"*, in *Mnémosyne* n° 7, IREM de Paris-Sud (Jussieu), avril 1994.

[H] HELLEGOUARC'H, Y.
- *"Vers une Arithmétique Nouvelle"*, in *Revue de Maths Spé.*, n° 6, février 1994.

[K] KUHN, T. S.
- *La structure des révolutions scientifiques.* Éd. Flammarion. Paris, 1983.

[O] OESTERLÉ, J.
- *"Nouvelles approches du «théorème de Fermat»"*, in *Sém. Bourbaki* n° 694 (1987-88), pp. 165-186.

[Rn] RIBENBOIM, P.
- *13 Lectures on Fermat's Last Theorem.* Springer. Berlin, New-York, 1979.

[Rt] RIBET, K.
- *"On modular representations of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) arising from modular forms"*, in *Invent. Math.* 100 (1990), pp. 431-476.

[R - S] RUBIN, K., SILVERBERG, A.
- *"A report on Wiles' Cambridge Lectures"*, in *Bull. Am. Math. Soc.* vol 31, n' 1 (july 1994) pp. 15-38.

[Se_1] SERRE, J.-P.
- *Cours d'Arithmétique.* P. U. F., Paris, 1970.

[Se_2] - *"Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)"*, in *Duke Math. J.* 54 (1987), pp. 179-230.

[Sh] SHIMURA, G.
- *Arithmetic Theory of Automorphic Functions* ; Princeton, 1971.

[V] VUILLEMIN, J.
- *La Philosophie de l'Algèbre* ; P. U. F., Paris, 1962.

[W] WEIL, A.
- *Number Theory* ; Birkhaüser, Boston, Bâle, Stuttgart, 1983.

Références complémentaires (cf. note 16).

[T - Wi_1] TAYLOR, R., WILES, A.
- *"Ring theoretic properties of certain Hecke Algebras"*, in *Annals of Mathematics*, vol. 141 (1995), pp. 553-572.

[Wi_2] WILES, A.
- *"Modular Elliptic Curves and Fermat's Last Theorem"*, in *Annals of Mathematics*, vol. 141 (1995), pp. 443-551.

*
* *
*