A PROPOS DU "THÉORÈME" DE FERMAT ET AUTRES QUESTIONS D'ARITHMÉTIQUE.

Par Marc Reversat, Université Paul Sabatier, Institut de Mathématiques de Toulouse (FR 2802), Laboratoire de Mathématiques Émile Picard (U.M.R. 5580).

Le “théorème” de Fermat est en fait un problème posé par Fermat vers le milieu du 17ème siècle et résolu à la fin du 20ème.

Cet exposé a pour but de dire quelques mots sur la grande aventure intellectuelle suscitée par la quête de sa démonstration.

En langage moderne le Théorème de Fermat s'énonce ainsi:

Théorème. Soit $p \geq 3$ un nombre entier. Si x, y et z sont des entiers tels que

$$x^p + y^p = z^p,$$

alors l'un d'entre eux est nul.

(Cela veut dire que les solutions x, y et z sont banales: si $x = 0$, l'équation devient $y^p = z^p$, donc $y = z$.)

Parenthèse pour les non mathématiciens.

Un entier naturel est dit premier s'il n'est divisible que par 1 et lui-même.

Tout entier s'écrit de manière **unique** sous la forme d'un produit fini de nombres premiers. Exemples:

$$6 = 2 \times 3 \quad , \quad -715 = -5 \times 11 \times 13$$

La notation x^p signifie que l'entier x est multiplié p fois par lui-même. Exemples:

$$3^2 = 3 \times 3 = 9 \, , \, (-5)^3 = (-5) \times (-5) \times (-5) = -125,$$

$$2^{10} = \underbrace{2 \times \cdots \times 2}_{10 \text{ fois}} = 1024.$$

L'équation $x^2 + y^2 = z^2$ admet une infinité de solutions, les triplets pythagoriciens:
$3^2 + 4^2 = 5^2$, $6^2 + 8^2 = (10)^2$, etc. On va amorcer une démonstration moderne de cela dans un instant.

Soient p et q deux entiers naturels, l'équation

$$x^{pq} + y^{pq} = z^{pq}$$

peut s'écrire

$$(x^p)^q + (y^p)^q = (z^p)^q,$$

on voit donc qu'il suffit d'examiner l'équation de Fermat pour $p \geq 3$ premier et $p = 4$.

L'APPROCHE MULTIPLICATIVE.

Prenons l'exemple de $p = 2$, c'est à dire de l'équation $x^2 + y^2 = z^2$ et cherchons ses solutions en nombres entiers. La généralisation à $p > 2$ de la méthode, pour cette fois montrer qu'il n'y a pas de solution, a donné la *théorie algébrique des nombres*.

Soit i un nombre complexe tel que $i^2 = -1$. On écrit

$$(x + iy)(x - iy) = x^2 + y^2 = z^2.$$

On est amené à calculer, non plus avec des nombres entiers, mais avec des quantités, les "entiers de Gauss", qui sont de la forme $x + iy$, où x et y sont des entiers. On note usuellement $\mathbb{Z}[i]$ l'ensemble des entiers de Gauss ($\mathbb{Z}$ désigne l'ensemble des entiers); $\mathbb{Z}[i]$ a des propriétés très voisines de $\mathbb{Z}$ l'ensemble des entiers,

- addition: $(x+iy)+(x'+iy') = (x+x')+i(y+y')$,
- multiplication: $(x+iy)(x'+iy') = (xx'-yy')+i(xy'+x'y)$,
- (la propriété essentielle) factorisation en "nombres premiers", que l'on appelle ici des éléments iréductibles: tout élément $x+iy$ s'écrit de manière **unique** sous la forme d'un produit

$$x+iy = \varepsilon \prod_{1\leq k\leq r} (a_k+ib_k),$$

où les a_k+ib_k sont des éléments irréductibles et où $\varepsilon = \pm 1, \pm i$. Les éléments irréductibles de $\mathbb{Z}[i]$ sont
- les nombres premiers qui divisés par 4 ont pour reste 3 (exemple 3, 7, 11, 19...),
- $1+i$ ($1+i = -i(1-i)$ et $2 = (1+i)(1-i)$),
- les éléments de $\mathbb{Z}[i]$ de la forme $a+ib$ avec a et b entiers tels que $a^2+b^2 = (a+ib)(a-ib)$ soit un nombre premier (nécessairement tel que le reste de sa division par 4 soit 1).

Voici un raisonnement typique. Soient x, y et z trois entiers tels que

$$(x+iy)(x-iy) = x^2 + y^2 = z^2.$$

et soit q un élément irréductible de $\mathbb{Z}[i]$, alors

si q divise $x+iy$ et $x-iy$ il divise leur somme et leur différence, donc q divise $(x+iy)+(x-iy) = 2x$ et $(x+iy)-(x-iy) = 2iy$, il suit que si q ne divise par 2, il est alors un diviseur commun à x et à y, par suite q divise aussi z.

Ainsi si l'on suppose que x, y et z sont des entiers sans diviseurs communs, on a que tout diviseur irréductible commun à $x+iy$ et $x-iy$ divise 2, donc est égal à $1+i$. Etc.

De cette manière on détermine la factorisation de z en irréductibles à partir de celles de $x+iy$ et $x-iy$ et on aboutit à des formules donnant les solutions.

On peut raisonner de même avec l'équation $x^3 + y^3 = z^3$. On considère alors un nombre complexe j tel que $j^3 = 1$ et $j \neq 1$, on a

$$(x + y)(x + jy)(x + j^2 y) = x^3 + y^3 = z^3$$

et on fait comme précédemment, de l'arithmétique, cette fois dans l'ensemble des $u + jv$, où u et v sont entiers. Cet ensemble est noté $\mathbb{Z}[j]$, il possède lui aussi les propriétés précédentes, en particulier celle de la factorisation **unique** en produit d'irréductibles. On arrive ainsi à prouver qu'il n'y a pas de solution avec x, y et z tous trois non nuls.

On peut être tenté de continuer , c'est à dire qu'étant donné $p \geq 3$ premier, considérer une racine primitive p-ème de l'unité ζ et examiner

$$\prod_{0 \leq k \leq p-1} (x + \zeta^k y) = x^p + y^p = z^p,$$

où x, y et z sont des entiers. Malheureusement, dans $\mathbb{Z}[\zeta]$, qui remplace ici $\mathbb{Z}[i]$ ou $\mathbb{Z}[j]$ (et qui est plus compliqué à écrire), il n'y a plus en général la propriété de la décomposition unique en produit d'irréductibles. De fait cette propriété n'est vraie que pour un nombre fini de p.

La recherche d'équivalents à cette décomposition unique occupa beaucoup du temps de mathématiciens célèbres du 19ème siècle (Kummer, Dedekind, Eisenstein...) et des deux premiers tiers du 20ème (Hilbert, Artin, Frölich, Serre...), cela a donné une belle théorie, qui a de nombreuses applications, la théorie algébrique des nombres. Elle a produit (et d'ailleurs continue) de nombreux résultats concernant les équations d'une variable à coefficients entiers, mais elle n'a pas abouti à une preuve du théorème de Fermat. Elle s'en est approchée, l'un des derniers résultats dans cette voie, spectaculaire, est dû à un mathématicien toulousain Guy Terjanian, qui a prouvé en 1977:

Soit$p \geq 3$ un nombre premier, alors si x, y et z sont des entiers tels que

$$x^{2p} + y^{2p} = z^{2p},$$

alors $2p$ divise x ou y.

UN PEU D'HISTOIRE.

Ce théorème de Terjanian s'insère dans l'histoire des résultats partiels concernant le théorème de Fermat.

- Lorsque $p = 2$ les solutions de l'équation de Fermat s'appellent des triplets pythagoriciens, l'équation est un exemple d'équation diophantienne. Les prémices du problème sont donc très anciennes.

- Vers 1640 démonstration dans le cas $p = 4$ par Fermat.

- 1770 démonstration dans le cas $p = 3$ par Euler.

- 1825 démonstration dans le cas $p = 5$ par Dirichlet et Legendre.

- 1835 démonstration dans le cas $p = 7$ par Lamé.

- 1844 Kummer montre le théorème pour les nombres premiers réguliers: soit ζ une racine primitive p-ème de l'unité (p premier, $p \geq 3$), Kummer attache un entier à l'ensemble $\mathbb{Z}[\zeta]$, qui mesure "sa distance à la propriété de décomposition unique en produit d'irréductibles", **le nombre de classes**; p est dit régulier s'il ne divise pas le nombre de classes. On ne sait toujours pas s'il existe ou non une infinité de nombres premier réguliers.

- 1977 Terjanian.

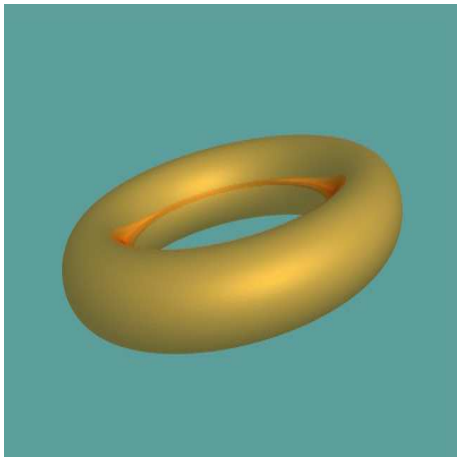
- 1982 Faltings, on va en parler dans le prochain paragraphe.

- 1984 Adleman, Fouvry et Heath-Brown montrent le "premier cas" du théorème de Fermat: soient $p \geq 3$ un nombre premier et x, y et z des entiers tels que $x^p + y^p = z^p$, alors p divise x, y ou z.

- 1994 Wiles. On en dira un mot plus loin.

L'APPROCHE GÉOMÉTRIQUE.

La relation $x^p + y^p = z^p$ peut être vue comme l'équation d'un objet géométrique, l'objet étant l'ensemble des points $[x : y : z]$ du plan projectif complexe. Plus simplement: si l'on pose $u = x/z$ et $v = y/z$ (donc on suppose $z \neq 0$), l'équation de Fermat devient $u^p + v^p = 1$, c'est l'équation d'une courbe plane sans singularité, le problème est de trouver ses points à coordonnées rationnelles. Par exemple pour $p = 2$ on a un cercle, en général on a une courbe de genre $g = \frac{(p-1)(p-2)}{2}$.



Les points d'une telle courbe sont à coordonnées complexes, si on regarde la courbe comme un objet géométrique à coordonnées réelles, cela devient (topologiquement) une surface , dite **surface de Riemann**; c'est une surface compacte, sans bords, le nombre d'anses étant son genre.

La recherche de points à coordonnées rationnelles sur de tels objets géométriques a conduit à la création de la géométrie arithmétique, c'est à dire d'une géométrie dont les coordonnées varient dans des lieux intéressants du point de vue de l'arithmétique (comme les entiers, les rationnels, dans les corps finis...). La construction des fondements de cette théorie a occupé les deux premiers tiers du 20ème siècle, elle a abouti en 1983 au

Théorème de G. Faltings (1983): Toute courbe de genre au moins 2 ne possède qu'un nombre fini de points à coordonnées rationnelles.

Ce théorème était depuis les années cinquante la conjecture de Mordell, beaucoup de noms célèbres sont liés aux progrès qui ont abouti à la preuve: Grothendieck, Manin, Mumford, Néron, Parshin, Raynaud, Serre, Shafarevich, Tate, Szpiro, Weil...

Donc l'équation de Fermat n'a qu'un "nombre fini" de solutions, pour $p \geq 5$ premier. Mais ce résultat n'est pas effectif, il ne fournit pas une borne pour ce nombre de points. La recherche de telles bornes est l'objet de la théorie d'Arakelov...

L'APPROCHE ADDITIVE (AUTOMORPHE).

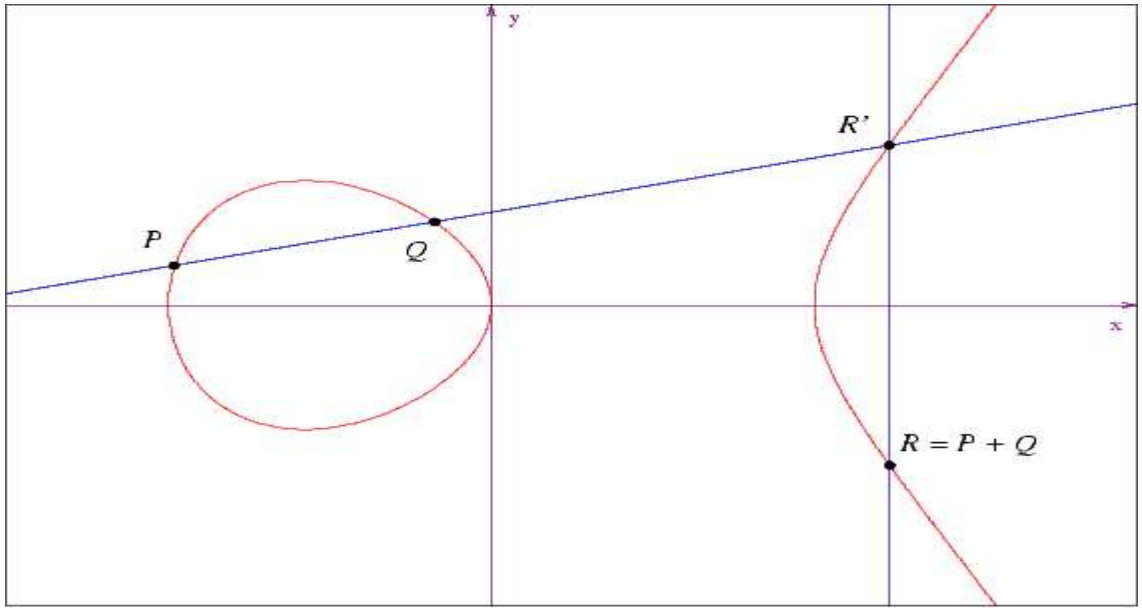
Soit $p \geq 5$ un nombre premier et a, b, c trois entiers tels que $a^p + b^p = c^p$. La relation suivante définit la **courbe de Frey-Hellegouarch**:

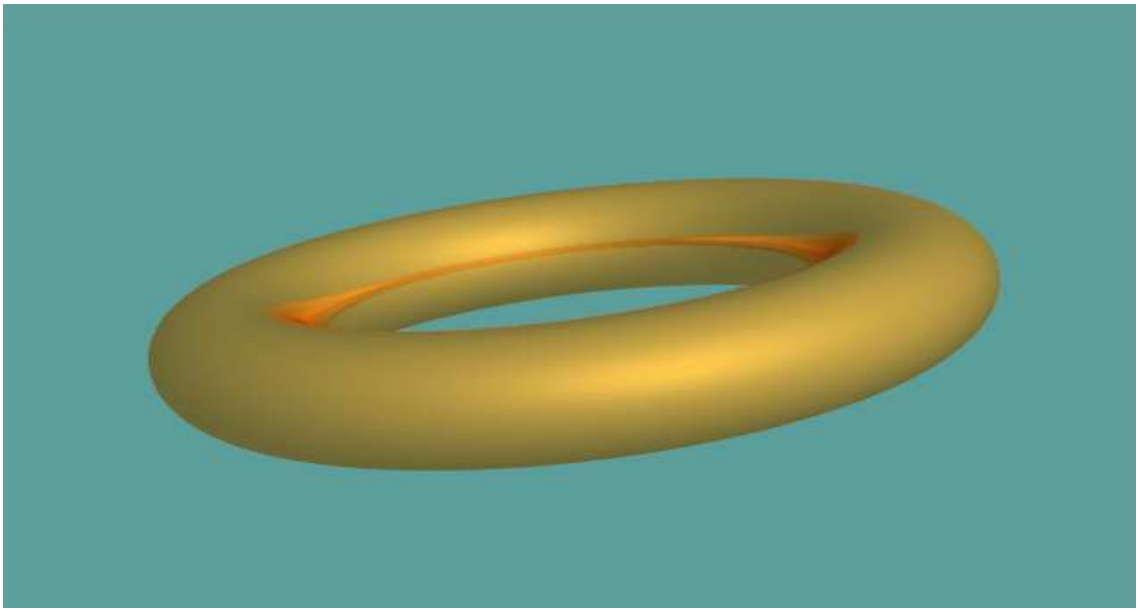
$$y^2 = x(x - a^p)(x + b^p),$$

c'est une courbe elliptique, c'est à dire de genre 1; écrivons plus simplement une telle courbe sous la forme

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

où A et B sont des entiers.





Deux nombres sont attachés à une courbe elliptique dont l'équation est à coefficient entiers.

- *Le discriminant*. IL permet de déterminer les situations où la courbe admet des singularités, ici il est (presque) égal à

$$\Delta := AB(A+B).$$

Si $\Delta \neq 0$, le polynôme $x(x-A)(x+B)$ n'a que des racines simples et la courbe est sans singularité.

- *Le conducteur*. Une idée sans doute naturelle lorsque l'on veut trouver les points de la courbe $y^2 = x(x - A)(x + B)$ est de s'autoriser des restes, donc que x et y ne vérifient pas exactement cette équation, mais qu'il y ait un reste divisible par un nombre premier ℓ fixé à l'avance. Cela revient à examiner la courbe avec A et B définis à un multiple de ℓ près (à examiner la courbe sur le corps fini $\mathbb{F}_\ell$ à ℓ éléments) et il peut se produire ici aussi des situations où la courbe a des singularités. Le conducteur de la courbe est (presque) le produit des nombres premiers ℓ tels que la courbe ait des singularités, quand on l'examine à des multiples de ℓ près. Ici le conducteur est

$$N := \prod_{l|AB(A+B)} \ell.$$

Une célèbre conjecture, de Szpiro, propose une comparaison entre ces deux quantités (donc entre les singularités de la courbe et les singularités à multiple de ℓ près):

Conjecture (Szpiro). Pour tout $\varepsilon > 0$ il existe une constante C telle que, quelle que soit la courbe elliptique, l'on ait

$$| \Delta |^2 \leq C N^{6+\varepsilon}.$$

Cette conjecture a té précisée par Masser et Oesterlé, sous le nom de **conjecture ABC**.

Revenons à la courbe de Frey-Hellegouarch $y^2 = x(x - a^p)(x + b^p)$, on a

$$\Delta = 2^{-8}(abc)^{2p} \quad \text{et} \quad N = \prod_{l|abc} \ell$$

et il résulte de la conjecture de Szpiro que

$$(abc)^{2p} \leq 2^8 C \left(\prod_{l|abc} \ell \right)^{6+\varepsilon}.$$

On voit que cette relation est impossible dès que p est assez grand. Donc, une propriété conjecturale des courbes elliptiques implique le théorème de Fermat, sauf pour un nombre fini de p.

La démonstration, par Andrew Wiles, passe par d'autres propriétés des courbes elliptiques, différentes mais qui ne sont pas sans relation avec celles juste énoncées. On ne cherche pas à factoriser d'une manière ou d'une autre $x^p + y^p$, on cherche à comprendre autrement cette addition.

Quelques mots de la démonstration. Soient ω_1 et ω_2 deux nombres complexes tels que ω_1/ω_2 ne soit pas un nombre réel, soit Λ l'ensemble des $n_1\omega_1 + n_2\omega_2$, où n_1 et n_2 sont des entiers; on dit que Λ est un réseau du plan complexe. Soit

$$\wp(z) = \wp(z,\Lambda) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda,\lambda\neq 0} \left(\frac{1}{(Z-\lambda)^2} - \frac{1}{\lambda^2}\right),$$

c'est la fonction $\wp$ de Weierstrass relative au réseau Λ, c'est une fonction méromorphe sur tout le plan complexe, elle est périodique de période Λ. On a la relation fonctionnelle

$$\left(\wp'\right)^2 = 4\wp^3 - 60G_4\wp - 140G_6$$

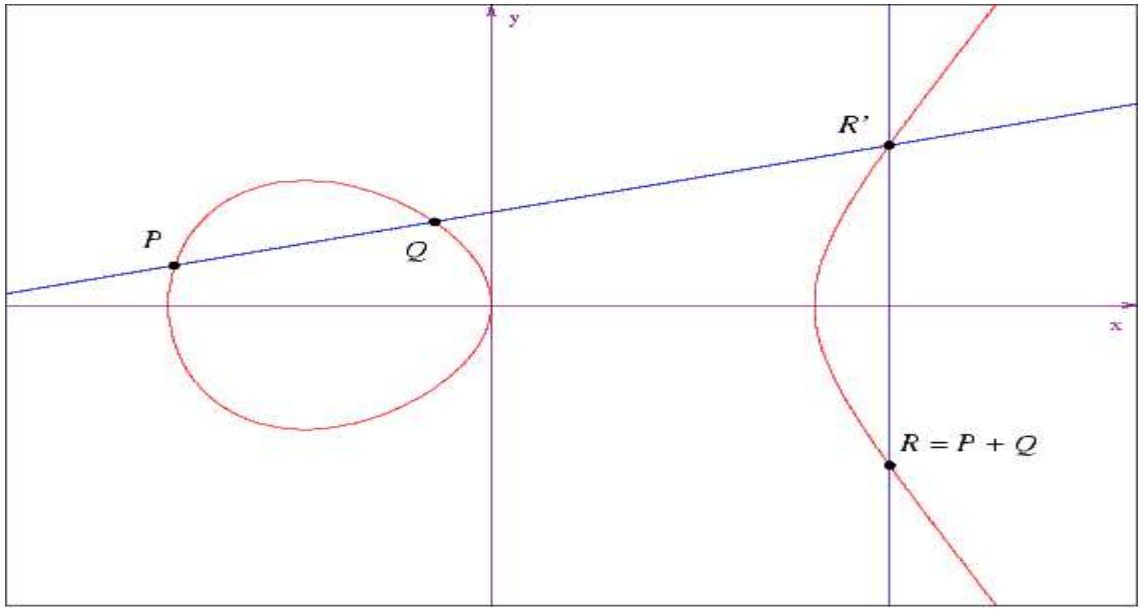
où $G_{2k} = \sum_{\lambda\in\Lambda,\lambda\neq 0} \lambda^{2k}$.

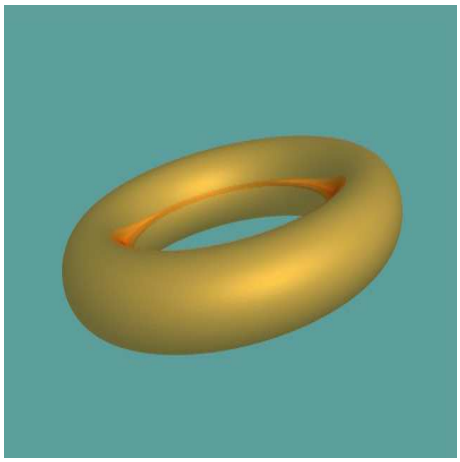
On voit que l'association

$$z \mapsto \left(\wp(z), (\wp(z)')\right)$$

induit une bijection entre la courbe elliptique et le tore $\frac{\mathbb{C}}{\Lambda}$.

Ceci retrouve l'aspect surface de Riemann des courbes elliptiques, cela montre aussi qu'il y a une opération (une addition) entre les points d'une courbe elliptique.





Soit p un nombre premier, on note $E[p]$ les points annulés par p sur la courbe elliptique E, c'est

$$\frac{(1/p)\Lambda}{\Lambda} \subset \frac{\mathbb{C}}{\Lambda},$$

c'est un espace vectoriel de dimension 2 sur le corps fini $\mathbb{F}_p$ à p éléments.

Revenons à la courbe de Frey-Hellegouarch

$$E_{(a,b,c)} : \ y^2 = x(x - a^p)(x + b^p),$$

où a, b et c sont des entiers tels que $a^p + b^p = c^p$ (et $p \geq 5$, premier). L'équation de cette courbe est à coefficients entiers, donc rationnels, par suite le groupe de Galois absolu G du corps $\mathbb{Q}$ (l'ensemble des rationnels) agit sur les points de $E_{(a,b,c)}$.

[Parenthèse: Le groupe de Galois absolu de $\mathbb{Q}$ est constitué par des permutations de l'ensemble des racines des polynômes à coefficients rationnels (et à une indéterminée).]

On a donc trouvé “une représentation galoisienne de degré 2 sur $\mathbb{F}_p$”. Andrew Wiles (1994) a montré que cette représentation, obtenue avec la courbe de Frey-Hellegouarch (1984, ≈1970), possède des propriétés contradictoires avec un résultat de Kenneth Ribet (1986) dans lequel est démontré partiellement une conjecture de Jean-Pierre Serre (la conjecture epsilon, 1985/6).

J'ARRÊTE, CELA DEVIENT TROP TECHNIQUE!

QUELQUES PROBLÈMES.

On va seulement parler de quelques uns relatifs à la factorisation des nombres entiers en nombres premiers. Commençons par la conjecture ABC, dont on a vu qu'elle n'est pas très éloignée de la démonstration du théorème de Fermat. Par exemple on n'a aucune idée des diviseurs premiers de

$$2^{1000} + 3^{500}$$

La conjecture ABC s'énonce ainsi.

Pour tout $\varepsilon > 0$ il existe une constante C possédant la propriété suivante: quels que soient les nombres entiers A, B et $C = A + B$, l'on a

$$\max(|A|, |B|, |C|) \leq C \prod_{\ell | ABC} \ell,$$

où comme toujours ℓ désigne un nombre premier.

On voit que conjecturalement le nombre

$$2^{1000} + 3^{500}$$

possède énormément de diviseurs premiers différents: pour $A = 2^{1000}$ et $B = 3^{500}$ la conjecture ABC donne

$$2^{1000} + 3^{500} \leq 6C \prod_{\ell | 2^{1000}+3^{500}} \ell.$$

Les nombres premiers jumeaux. Il s'agit de trouver les nombres premiers p tels que $p+2$ soit encore premier. Exemple: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$,... Mais pour $p = 7, 13, 19, 23, 31...$, $p+2$ n'est pas premier. On sait peu de chose sur ces nombres premiers, on ne sait même pas s'ils sont en nombre infini ou non.

Les conjectures de Goldbach. La conjecture de Goldbach la plus célèbre et la plus impénétrable affirme que tout nombre pair plus grand que 2 est la somme de deux nombres premiers. Exemple: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, ... , $44 = 13 + 31 = 3 + 41 = 7 + 37$,... On sait actuellement que tout nombre pair est la somme d'un nombre premier et d'un nombre qui est le produit d'au plus deux nombres premiers.

La conjecture de Goldbach pour les nombres impairs dit que tout nombre impair est somme de trois nombres premiers au plus. Ceci a été prouvé, par Vinogradov, pour tout nombre impair plus grand qu'un certain nombre N, mais bien qu'ayant été diminué plusieurs fois, N est plus grand que le nombre estimé de particules élémentaires de l'univers, certains affirment donc qu'il est impossible de construire un ordinateur permettant de vérifier le nombre fini

de cas restant, par conséquent que cette conjecture n'est toujours pas réduite à l'examen d'un nombre fini de cas.

Je termine par cette polémique (presque) philosophique, tout en oubliant beaucoup de problèmes passionnants, portant toujours sur la factorisation des nombres (et qui intéressent les cryptographes), ou encore des questions plus techniques mais tout aussi intéressantes, comme celle de l'existence d'une infinité de nombres premiers réguliers. Il y a aussi un programme de recherche tellement vaste et tellement conjectural, que lui est donné le nom de philosophie, la philosophie de Langlands, dans laquelle s'insère la démonstration de Wiles et qui vise à la compréhension du groupe de Galois absolu du corps des rationnels, c'est à dire à la résolution de beaucoup d'équations diophantiennes.