Association Mathématique du Québec

Le cauchemar du professeur De Koninck

Claude Levesque,
Département de mathématiques et de statistique,
Université Laval

L'histoire que je m'apprête à vous raconter est un peu compliquée, et je prends le risque que vous y perdiez votre latin. Elle implique le professeur Jean-Marie De Koninck du département de mathématiques et de statistique de l'Université Laval, une figure publique jouissant d'une réputation bien méritée comme professeur, chercheur, enseignant, entraîneur de natation et commentateur sportif.

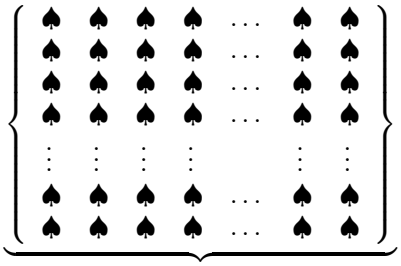
Le professeur De Koninck est aussi une personnalité bien connue dans le Québec pour son implication dans Nez Rouge, un organisme qu'il a fondé il y a plus de 25 ans et qui vise à raccompagner des gens qui sentent le besoin de ne pas conduire leur auto après avoir consommé de l'alcool.

Auteur de plusieurs articles et volumes, le professeur De Koninck est un chercheur respecté par les membres de la communauté mathématique, tant au niveau de l'enseignement des mathématiques que de la recherche. Monsieur De Koninck a reçu en 2004 le prix Adrien-Pouliot de la Société mathématique du Canada, en reconnaissance de ses réalisations dans le domaine de l'enseignement. J'ai déjà lu un témoignage d'un chercheur canadien de très haut niveau qui affirme avoir découvert sa vocation de mathématicien grâce à un cours qu'il a suivi sous la direction de Jean-Marie lors d'un camp mathématique d'été à l'Université de Sherbrooke. Ancien nageur élite de niveau universitaire, il a su toute sa vie conjuguer « âme saine » et « corps sain » via la natation, le vélo et le jogging : mens sana in corpore sano !

À la suite de son mandat comme vénérable (et, qui sait, vénéré) président de l'Association mathématique du Québec (AMQ), Jean-Marie décida de faire une journée *Portes ouvertes* en vue de faire connaître son joli petit volume *En chair et en maths* (Septembre Éditeur), un opuscule qui, selon les auteurs, se veut « *Une rencontre avec les mathématiques qui façonnent notre quotidien* ». Du coup, Jean-Marie voulait aussi décrire le rôle important de l'AMQ au Québec et en profiter pour recruter de nouveaux membres lors de cette rencontre au cours de laquelle des beignes et du café seraient distribués à tout un chacun. Il me chargea de faire la publicité de cette journée *Portes ouvertes*, et au risque de passer pour un petit vantard, j'aimerais vous dire immédiatement que ce fut un succès monstre, comme vous aurez bientôt l'occasion de le constater.

Le grand jour venu, Jean-Marie contempla tous ces mathématiciens venus pour s'impliquer au sein de l'AMQ. Toutes ces personnes se tenaient bien disciplinées en rangs serrés et formaient un carré parfait :

© Association mathématique du Québec



Carré parfait C^2

Cet attroupement de mathématiciens était composé de **314 régiments égaux** de *mathématiciens francophones* et de **1 régiment** de *mathématiciens non francophones*. Jean-Marie ordonna alors à tous ces mathématiciens de se répartir en **carrés parfaits**, en demandant à chaque régiment de mathématiciens francophones de former un **carré parfait** et en demandant au régiment de mathématiciens non francophones de former aussi un **carré parfait**. Ce que tous firent dans le respect et sans difficulté.

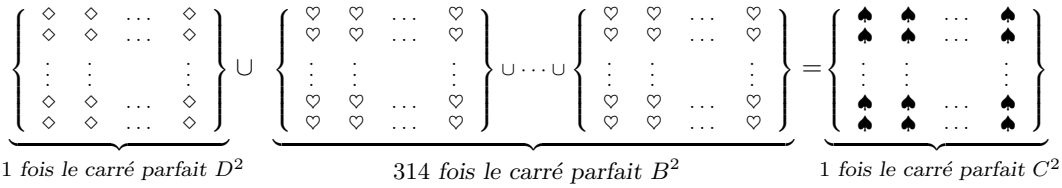
Puis se ravisant, comme cela lui arrivait parfois dans sa sagesse, Jean-Marie changea d'avis et désigna **157** régiments de mathématiciens francophones et leur ordonna de se joindre aux mathématiciens non francophones pour former ensemble un autre **carré parfait**.

Je veux maintenant vous poser la question

« Combien y avait-il de mathématiciens ? »

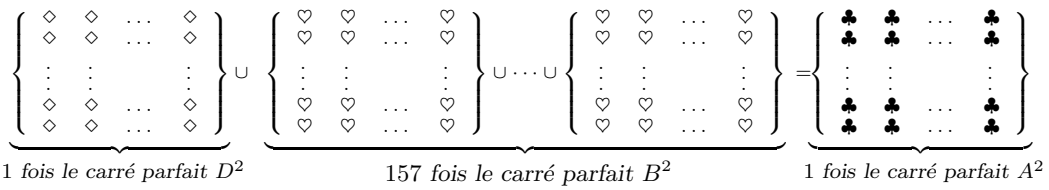
car il y a suffisamment de renseignements pour résoudre ce problème mathématique. Vous pouvez y réfléchir, mais pas trop longtemps...

Appelons D^2 le nombre de mathématiciens non francophones puisque ceux-ci justement forment un carré parfait. Appelons B^2 le nombre de mathématiciens qu'il y a dans chacun des régiments égaux de mathématiciens francophones, puisque justement chacun de ces 314 régiments égaux de mathématiciens francophones forme un carré parfait. Il y a donc $314B^2$ mathématiciens francophones. Mis ensemble, tous les mathématiciens sont alors formés des D^2 mathématiciens non francophones et des $314B^2$ mathématiciens francophones. Comme tous les mathématiciens réunis ensemble forment un carré parfait, nous allons appeler C^2 le nombre total de mathématiciens présents. On sait alors que C^2 est la somme de D^2 et de $314B^2$:



1 *fois le carré parfait* D^2 — 314 *fois le carré parfait* B^2 — 1 *fois le carré parfait* C^2

De même, les D^2 mathématiciens non francophones et les $157B^2$ mathématiciens francophones choisis par Jean-Marie forment un carré parfait que cette fois-ci nous allons appeler A^2 :



En conclusion, les quatre entiers A, B, C, D vérifient les deux équations suivantes :

$$\begin{cases} D^2 + 314\,B^2 &= C^2, \\ D^2 + 157\,B^2 &= A^2. \end{cases}$$

Après avoir soustrait la deuxième équation de la première, on conclut que ceci revient à trouver des nombres entiers A, B, C, D vérifiant les deux équations de Fermat-Pell

$$\begin{cases} A^2 + 157\,B^2 &= C^2, \\ A^2 - 157\,B^2 &= D^2. \end{cases}$$

En pratique, il y a une infinité de solutions possibles, mais il s'avère en fait que la plus petite est, veuillez me croire,

$$\begin{cases} A = 224403517704336969924557513090674863160948472041, \\ B = 178246645378577191760510703579343271400329616 60, \\ C = 316605068345983991287469841722668300352741098609, \\ D = 217969771710702471041124552665861477219359798 09. \end{cases}$$

Comme la valeur de C^2 donne le nombre total de mathématiciens, eh bien, le nombre de mathématiciens présents est alors égal à

$$100238769302365194296666515800317276094581136373506411315467664435308722606223072047884261734881.$$

Si nous écrivons ce nombre avec une suite de blocs de 6 chiffres, cela donne

$$\begin{array}{cccccccc} 100238 & 769302 & 365194 & 296666 & 515800 & 317276 & 094581 & 136373 \\ 506411 & 315467 & 664435 & 308722 & 606223 & 072047 & 884261 & 734881\,. \end{array}$$

Ce nombre est de l'ordre de 10^{95}. C'est beaucoup plus que le nombre d'atomes dans l'univers fini connu, qui selon certains physiciens comporte environ 10^{80} atomes.

Comment peut-on en arriver à calculer explicitement de tels monstres ? C'est avec les *courbes elliptiques* ! Ce sont des équations qui ont l'allure suivante :

$$Y^2 = X^3 - 24649X.$$

C'est d'ailleurs avec cette dernière courbe elliptique que les solutions A, B, C, D données ci-dessus ont été trouvées. Elles font l'objet de recherches intensives et de puissants algorithmes ont été mis au point pour faire de savants calculs. Les courbes elliptiques interviennent aujourd'hui dans la téléphonie cellulaire et même dans les transactions électroniques sur internet.

Expliquons d'où vient ce lien avec les courbes elliptiques. Supposons d'abord que n est un entier positif pour lequel il existe des entiers non nuls A, B, C, D vérifiant

$$\begin{cases} A^2 + n\,B^2 &= C^2, \\ A^2 - n\,B^2 &= D^2. \end{cases}$$

On dit alors que n est un *nombre congruent* et on vérifie aisément que les nombres rationnels non nuls

$$X = \frac{A^2}{B^2}, \quad Y = \frac{ACD}{B^3}$$

vérifient l'équation de la courbe elliptique

$$E : Y^2 = X^3 - n^2 X.$$

Inversement, s'il existe un couple (x, y) de nombres rationnels non nuls qui est une solution de la courbe elliptique

$$E : Y^2 = X^3 - n^2 X,$$

alors on vérifie aisément que l'on peut définir des entiers A, B, C, D, à partir des égalités

$$\frac{A}{B} = \frac{x^2 + n^2}{2y}, \qquad \frac{C}{B} = \frac{x^2 + 2nx - n^2}{2y}, \qquad \frac{D}{B} = \frac{x^2 - 2nx - n^2}{2y},$$

et qui auront la propriété de vérifier

$$\begin{cases} A^2 + n\,B^2 &= C^2, \\ A^2 - n\,B^2 &= D^2. \end{cases}$$

En effet, en utilisant d'abord $A = \dfrac{B(x^2 + n^2)}{2y}$, puis en nous rappelant que $y^2 = x^3 - n^2 x$, nous avons

$$\begin{aligned} A^2 + n\,B^2 &= \frac{B^2(x^2 + n^2)^2}{(2y)^2} + nB^2 \;=\; \frac{B^2(x^4 + 2n^2x^2 + n^4 + 4ny^2)}{4y^2} \\ &= \frac{B^2(x^4 + 2n^2x^2 + n^4 + 4n(x^3 - n^2x))}{4y^2} \\ &= \frac{B^2(x^4 + 2n^2x^2 + n^4 + 4nx^3 - 4n^3x)}{4y^2} \;=\; \frac{B^2(x^2 + 2nx - n^2)^2}{(2y)^2} \;=\; C^2. \end{aligned}$$

On prouve de la même façon que $A^2 - n\,B^2 = D^2$.

Pour satisfaire la curiosité des lecteurs désireux de connaître les valeurs de X, Y qui satisfont à la courbe elliptique

$$Y^2 \;=\; X^3 - 157^2 X,$$

j'aimerais mentionner que c'est Don Zagier qui, il y a plusieurs années, a trouvé que les valeurs

$$X = \frac{r}{s} \quad \text{et} \quad Y = \frac{t}{u}$$

font l'affaire pour les valeurs de r, s, t et u suivantes :

$$\begin{cases} r = & 503569387580806759044784284151489931213552539425109692787039743300107183966584214183325587056 81, \\ s = & 317718665887162537529860429204893522122457849878951860106775096212089198787035991271029955600, \\ t = & 154861618129816988077745182125449759208828670614060766769549057891134437037031674674236696464168214378839145906402295492008915019717441084492 1, \\ u = & 566322863685437111858421713766551991831194355630294582933508383803571880138219815171903098069750667738000194805160322522211364124630229600 0. \end{cases}$$

Zagier a réussi ce tour de force en utilisant brillamment les propriétés de la hauteur d'un point d'une courbe elliptique. Ce fut donc facile pour nous d'établir les valeurs de A, B, C, D à partir de ces valeurs de X et Y.

Les courbes elliptiques ont rendu Andrew Wiles célèbre : il a reçu de nombreux prix très prestigieux pour ses résultats. Wiles (secondé par les membres de son école) a prouvé que *toute courbe elliptique sur* $\mathbf{Q}$ *de la forme*

$$E : Y^2 \ = \ X^3 + aX + b, \qquad \textit{avec } a, b \in \mathbf{Z},$$

est modulaire.

Expliquons ce que cela veut dire. À la courbe elliptique E est attachée une fonction

$$L(E, s) \ = \ L(s) \ = \ \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

(définie via un produit infini pris sur tous les premiers p faisant intervenir le nombre de solutions de la courbe elliptique E sur le corps fini des entiers modulo p). Par définition, la transformation de Mellin correspondant à $L(s)$ est

$$f(t) = \sum_{n=1}^{\infty} a_n e^{-nt}$$

et elle vérifie la propriété de modularité suivante :

Il existe un entier N (*qui s'avère être le conducteur* N *de la courbe elliptique* E) *tel que pour toute matrice* 2 *par* 2 *de déterminant* 1 *de la forme* $\begin{pmatrix} c & d \\ Nu & v \end{pmatrix}$ *avec coefficients dans* $\mathbf{Z}$ *et pour tout nombre complexe* z *du demi-plan supérieur* (*i.e.* $Im(z) > 0$) *nous avons*

$$f\left(\frac{cz + d}{Nuz + v}\right) \ = \ (Nuz + v)^2 f(z).$$

En fait, Wiles a obtenu son résultat pour les courbes elliptiques semi-stables, i.e. lorsque le dit *conducteur* N de la courbe elliptique E, qui s'avère être un diviseur du discriminant $\Delta = -16(4a^3 + 27b^2)$, est un entier sans facteur carré. Ce sont les membres de son école de pensée (C. Breuil, B. Conrad, F. Diamond et R. Taylor) qui ont traité le cas où le conducteur N contient des facteurs carrés.

Andrew Wiles est toutefois plus connu pour avoir prouvé le dernier théorème de Fermat, à savoir le résultat suivant.

Théorème (Dernier théorème de Fermat)**.** *Soit n un entier ≥ 3. L'équation diophantienne*

$$A^n + B^n = C^n$$

ne possède aucune solution entière vérifiant $ABC \neq 0$.

En fait, il avait annoncé son théorème le 23 juin 1993 à Cambridge, mais il y avait dans sa preuve une lacune qu'il a comblée un an plus tard avec l'aide de son ancien étudiant Richard Taylor. On peut en quelque sorte résumer sa preuve en quelques lignes :

Supposons qu'il existe des entiers A, B, C non nuls tels que pour $n \geq 5$ l'on ait $A^n + B^n = C^n$. Ribet a prouvé que la courbe elliptique

$$E : Y^2 = X(X - A^n)(X + B^n)$$

ne sera alors pas modulaire. Or, selon Wiles, toute coube elliptique est modulaire. Contradiction.

Il s'avère que la modularité des courbes elliptiques sur $\mathbf{Q}$ jouent un rôle important pour résoudre beaucoup d'équations diophantiennes, comme en témoignent les résultats de Darmon, Merel, Bennett, et plusieurs autres mathématiciens.

Revenons au professeur De Koninck. Le visage de Jean-Marie s'allongea soudainement. Il se demandait comment il pourrait réussir à distribuer des beignes à autant de personnes. À la seule pensée qu'il aurait à distribuer plus de 10^{95} beignes à tous ces mathématiciens, il paniqua. Il avait bien raison, car même si chacune des six milliards de personnes de ce bas monde possédait la fortune de Bill Gates et celle de Warren Buffet, tout cet argent ne suffirait pas pour payer le coût de ces beignes. C'est alors que Jean-Marie se réveilla en sursaut et constata qu'il venait de faire un cauchemar. Il s'avère que je me réveillai moi aussi presqu'en même temps pour réaliser que j'avais rêvé que Jean-Marie avait fait un mauvais rêve.

Ceci termine l'histoire du cauchemar du professeur De Koninck. Plus jamais Jean-Marie De Koninck ne fit appel à mes services pour organiser une journée *Portes ouvertes*.

Addendum. Cette histoire est basée sur des faits véridiques (en particulier sur *le rêve de Napoléon*), et n'allez surtout pas croire que toute ressemblance avec la réalité est une simple coincidence ou le fruit du hasard.