Chers Dudes,

J'en vois un qui n'écoute pas dans le fond.
J'en vois deux qui tricottent au deuxième rang.
J'en vois cent-quinze au cinquième rang qui aimeraient être deux-cent dix-sept au premier rang.
Je vois pi carré sur six à l'étage.
Je vois l'homme qui a vu l'homme qui a vu l'ours.

Eh bien vous pouvez continuer, il n'y a point de poulpor Seminar cette semaine pour parfaire votre bronzage intégral.

En revanche, dès la semaine prochaine et la fin des frimas, on repart comme en 40 avecques BERNARD WÜTRICKE LUNDI 30 (et non pas mercredi, bande de moules), qui fera un esspossé intitulé de toutes façons et quoiqu'il en dise:

ÜBER ER IST SCHWER DIESER W.

Les ceusses qui pouvaient venir le mercredi et qui ne pouvent plus le lundi n'ont qu'à appeler la REGA (nous, quoi), et on verra ce qu'on peut faire pour eux (en termes financiers).

Date : LUNDI (bande de moules) 30 avril 2001
Heure : 16h15
Salle : 6ème
Tenue du conférencier : Acier trempé[1]

Jo di Mambro bienvenus.
Tabaschnick s'abstenir.

Mathieu Baillif (cosmo-énergie gros, demi gros, détail)
David Cimasoni (live from Sirius)

"Le problème c'est que j'ai obtenu sept, je dois avoir incorrectement copié le truc."
F.S.

P.S : Post scriptum.

# ÜBER KONGRUENZZAHLEN

CHRISTIAN "ER IST SCHWER" WUTHRICH

Et ça tend vers 1 quand 0 est très grand.
SCHMUTZ-SCHALLER

Nos honorables ancêtres, PYTHAGORE (570–480 av. J.-C.) et son école, découvrirent que dans un triangle rectangle les côtés satisfont à l'équation

$$X^2 + Y^2 = Z^2 .$$

Il était connu des savants grecs déjà que les triangles rectangles de côtés rationnels (les triangles pythagoriciens) pouvaient être obtenus par les formules suivantes :

$$X = a^2 - b^2 , \qquad Y = 2ab , \qquad Z = a^2 + b^2 ,$$

avec $a > b$ parcourant tous les nombres rationnels positifs. Les mathématiciens arabes du $10^{\text{ème}}$ siècle furent les premiers à étudier le problème de savoir quelles sont les aires possibles de triangles pythagoriciens. Autrement dit, ils s'intéressaient à la

QUESTION: Soit $n$ un entier positif sans facteur carré différent de 1. Est-ce qu'il existe des solutions $X < Y < Z$ dans $\mathbb{Q}$ du système d'équations ci-dessous ?

$$X^2 + Y^2 = Z^2 \tag{1}$$
$$\tfrac{1}{2} X \cdot Y = n \tag{2}$$

S'il en existe, on appelle $n$ un *nombre de congruence.*

L'exemple canonique $3^2 + 4^2 = 5^2$ donne un premier nombre de congruence: $n = 6$. Le plus petit nombre de congruence est $n = 5$, il est l'aire du triangle de côtés $\frac{3}{2}$, $\frac{20}{3}$ et $\frac{41}{6}$. FERMAT (1601 – 1665), fameux conjectureur prétentieux, démontra que $n = 1$ n'est pas un nombre de congruence. EULER (1707–83), plus connu pour son portrait sur des billets périmés, réussit à trouver un triangle d'aire $n = 7$. La question de déterminer si $n$ est nombre de congruence est loin d'être une question triviale. Voici les côtés du triangle le plus simple d'aire $n = 157$ :

$$
\begin{aligned}
X &= \tfrac{6803298487826435051217540}{411340519227716149383203} \\
Y &= \tfrac{411340519227716149383203}{21666555693714761309610} \\
Z &= \tfrac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}
\end{aligned}
$$

(source: [5], voir aussi [1] où j'ai pompé cet exposé)

Proposition 1. *$n$ est un nombre de congruence si et seulement s'il existe $x$ tel que $x$, $x+n$ et $x-n$ sont des carrés de nombres rationnels.*

*Preuve.* Si on a une solution $(X, Y, Z)$ aux équations (1) et (2), alors

$$(X+Y)^2 = Z^2 + 4n \quad \text{et} \quad (X-Y)^2 = Z^2 - 4n.$$

On pose $x = \left(\frac{Z}{2}\right)^2$, et puis

$$\left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n = x \pm n \tag{3}$$

sont heureusement des carrés. Dans l'autre sens, il suffit de poser

$$
\begin{aligned}
X &= \sqrt{x+n} - \sqrt{x-n} \\
Y &= \sqrt{x+n} + \sqrt{x-n} \\
Z &= 2\sqrt{x}
\end{aligned}
$$

pour un $x$ donné et vérifier que c'est bien une solution aux équations (1) et (2). □

Sans expliquer pourquoi, je vais multiplier les deux équations (3) :

$$\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2 = x^2 - n^2\,.$$

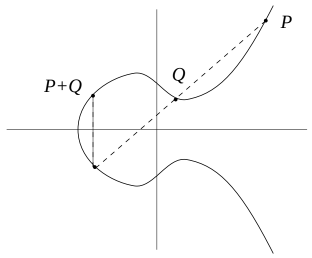
Pour faire encore plus compliqué, on calcule son produit avec $x$ et on introduit une autre quantité

$$y = \frac{Z \cdot (X^2 - Y^2)}{8}\,.$$

L'équation devient

$$E_n\colon \qquad y^2 = x^3 - n^2 x \tag{4}$$

Si $n$ est un nombre de congruence, alors nous avons une solution rationnelle de $E_n$ avec $y \neq 0$. Cette équation $E_n$ est l'équation affine d'une *courbe elliptique*.




Une courbe elliptique $E$ sur $\mathbb{Q}$ est quelqu'un de la forme $y^2 = x^3+Ax+B$ avec $A, B \in \mathbb{Q}$ et $4A^3 + 27B^2 \neq 0$. Elles méritent leur renom arithmétique par le fait qu'elles portent une structure de groupe abélien. Pour additionner deux points $P$ et $Q$ sur la courbe, il faut prendre le point symétrique par rapport à l'axe des $x$ de la troisième intersection de la courbe et la droite qui passe par $P$ et $Q$. Le point à l'infini $O = (0 : 1 : 0)$ sert alors d'élément neutre. Si $P$ et $Q$ ont des coordonnées rationnelles, alors leur somme $P + Q$ aura aussi des coordonnées rationnnelles. $E(\mathbb{Q})$, l'ensemble des points rationnels, forme un groupe abélien. (voir [4])

Théorème de Mordell-Weil.
*Le groupe $E(\mathbb{Q})$ est de génération finie.*

Ce théorème fondamental de la théorie des courbes elliptiques montre que l'on peut écrire

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r .$$

$r$ est appelé le *rang* de la courbe elliptique.

Dans notre cas, la courbe elliptique $E_n$ a trois points d'ordre 2: $P_1 = (0, 0)$, $P_2 = (n, 0)$ et $P_3 = (-n, 0)$. On voit alors que $E_n(\mathbb{Q})_{\text{tors}}$ contient un sous-groupe de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Gauss (1777-1855), dernier des grands illustres qu'il faut nommer dans tout exposé arithmétique, sut montrer que

$$E_n(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} .$$

Ceci implique que $2E_n(\mathbb{Q}) \approx \mathbb{Z}^r$.

Proposition 2. *Le rang $r$ de $E_n$ est plus grand que zéro si et seulement si $n$ est un nombre de congruence. De plus, il y a une bijection entre les triangles pythagoriciens d'aire $n$ et les couple de points $(x, \pm y)$ dans $2E(\mathbb{Q}) \setminus \{O\}$.*

*Preuve.* Soit $P = (x_0, y_0)$ un point de $E_n(\mathbb{Q})$ d'ordre infini. On vérifie que la première coordonnée du point $2 \cdot P = P + P$ est

$$x_1 = \left(\frac{x_0 + n^2}{2y_0}\right)^2$$

et que

$$x_1 \pm n = \left(\frac{x_0^2 \pm 2nx_0 - n^2}{2y_0}\right)^2$$

sont des carrés, tout comme $x_1$ lui-même. □

En principe, il existe un algorithme qui donne une bonne borne supérieure pour le rang $r$ (la démonstration du théorème de Mordell-Weil). Souvent, on trouve suffisamment de générateurs du groupe $E(\mathbb{Q})$ pour déterminer $r$.

Lorsqu'on réduit l'équation d'une courbe elliptique modulo $p$ (premier), on retrouve souvent de nouveau une courbe elliptique définie sur le corps fini $\mathbb{F}_p$. Dans notre cas $E_n$, c'est vrai pour $p \nmid 2n$; sinon, la courbe réduite est singulière. Si $E_n$ a "bonne réduction" modulo $p$, $E(\mathbb{F}_p)$ est un groupe fini. Soit $N_p$ son ordre.

Théorème de Hasse.
$|N_p - (p+1)| \leq 2\sqrt{p}$.

Autrement dit, le nombre de points sur une courbe elliptique n'est pas trop loin du nombre de points sur une droite projective, i.e. $p+1$. On a par exemple :

Proposition 3. *Si $p \equiv 3 \pmod 4$ et $p \nmid n$, alors $N_p = p+1$.*

*Preuve.* On connaît déjà quatre points: $O$, $(0,0)$, $(n,0)$ et $(-n,0)$. Il reste à compter les solutions avec $x \neq 0, n, -n$ de $y^2 = f(x)$ où $f(x) = x^3 - n^2x$. Comme $-1$ n'est pas un carré modulo $p$, soit $f(x)$ soit $-f(x) = f(-x)$ est un carré. Pour chaque couple $\{x, -x\}$ il y a deux solutions pour $y$, namely $\pm\sqrt{f(x)}$ ou $\pm\sqrt{f(-x)}$. Il y a $\frac{p-3}{2}$ couples. Alors $N_p = 4 + 2 \cdot \frac{p-3}{2} = p+1$. □

On pose

$$2a_p = p + 1 - N_p \tag{5}$$

et

$$L(E_n, s) = \prod_{p \nmid 2n} \frac{1}{1 - 2a_p p^{-s} + p^{1-2s}} \tag{6}$$

En utilisant Hasse, i.e. $|a_p| \leq \sqrt{p}$, on peut montrer que $L(E_n, s)$ ne converge que pour $\mathrm{Re}(s) > \frac{3}{2}$ et qu'elle représente une fonction holomorphe sur ce domaine. C'est une série de Dirichlet de la forme $\sum_{m=1}^{\infty} b_m \cdot m^{-s}$, et (6) représente son produit d'Euler.

Conjecture. *$L(E_n, s)$ peut être prolongée sur tout le plan $\mathbb{C}$.*

Pour notre courbe (qui est munie de ce que l'on appelle une "multiplication complexe"), la conjecture a été démontrée par Deuring; en général, elle est une conséquence de la conjecture de Shimura-Taniyama, démontrée en partie par Wiles, Taylor et Diamond dans les années 90 du siècle passé.

Voici pourquoi je parle de tout ça.

WEAK CONJECTURE DE BIRCH, SWINNERTON-DYER. *$L(E_n, 1) = 0$ si et seulement si $r > 0$.*

Il y a un argument heuristique pour justifier une telle conjecture (voir [3]): si on se fout de la convergence dans (6), on peut poser $s = 1$ et on obtient

$$L(E_n, 1) = \prod_{p \nmid 2n} \frac{p}{p - 2a_p + 1} = \prod_{p \nmid 2n} \frac{p}{N_p}$$

On sait que $N_p$ est proche de $p$. Si $N_p$ était aussi souvent plus grand que plus petit que $p$, on pourrait s'attendre à ce que $L(E_n, 1) > 0$. Par contre si $N_p$ est plus souvent plus grand, il faudrait que le produit converge vers 0. Lorsque $r > 0$, on a une infinité de points rationnels, ainsi on peut espérer trouver beaucoup de points sur les courbes réduites. Évidemment, on n'arrive pas à utiliser ça pour en faire une démonstration.

THÉORÈME (COATES, WILES 1977).
*Si $E$ porte une structure de multiplication complexe, alors $r > 0$ implique $L(E, 1) = 0$.*

KOLYVAGIN généralisa ce théorème à toutes les courbes elliptiques. Et c'est à peu près tout ce qu'on sait sur cette conjecture.

À l'aide du théorème ci-dessus, nous sortons de l'autre côté du

THÉORÈME (TUNNEL, 1983).
*Si $n$ est un nombre de congruence, alors le nombre de solutions entières de l'équation*

$$n = 2x^2 + y^2 + 8z^2$$

*est égal au double du nombre de solutions entières de l'équation*

$$n = 2x^2 + y^2 + 32z^2 .$$

*La réciproque est vraie si la conjecture faible de Birch et Swinnterton-Dyer est vraie.*

En particulier, sous la conjecture, les nombres $n$ congrus à 5,6 ou 7 modulo 8 sont toujours des nombres de congruence.

La conjecture de ces deux anglais va encore beaucoup plus loin:

CONJECTURE DE BIRCH, SWINNERTON-DYER (\$ 1'000'000). *Lorsque $s$ s'approche de 1, on a*

$$L(E, s) \sim \frac{|\text{Ш}(E/\mathbb{Q})| \cdot \Omega \cdot 2^r \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|} \cdot (s-1)^r \tag{7}$$

Non seulement, l'ordre du zéro en $s = 1$ devrait être exactement le rang de la courbe elliptique, mais en plus on a une expression pour le premier coefficient de la série. Les facteurs qui apparaissent sont tous d'une manière ou d'une autre liés à l'arithmétique de la courbe. Ils se calculent tous assez facilement sauf le facteur $|\text{Ш}(E/\mathbb{Q})|$ qui représente l'ordre d'un groupe dont on ne sait pratiquement rien. Il est lié au principe de Hasse pour les courbe de genre 1. Jusqu'à 1987, on ne connaissait aucun groupe $Ш(E/\mathbb{Q})$. Pire, on ne sait même pas encore si

CONJECTURE. *Le groupe* $Ш(E/\mathbb{Q})$ *est fini.*

Mais quand BIRCH et SWINNERTON-DYER ont vérifié la conjecture pour quelques courbes, ils avaient trouvé quelques fois un facteur carré qu'ils n'arrivaient pas à expliquer. CASSELS avait montré un peu avant que si $Ш(E/\mathbb{Q})$ était fini, alors son ordre était un carré. De plus, la prédiction de la 2-torsion de $Ш(E/\mathbb{Q})$ par la formule (7) a pu être verifiée pour un grand nombre de courbes.

## Références

[1] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer Verlag, 1984.

[2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer Verlag, 1986.

[3] Peter Swinnerton-Dyer, *An Application of Computing to Class Field Theory*, Algebraic Number Theory (J.W.S. Cassels et A. Fröhlich, ed.), Academic Press, 1967, pp. 280–291.

[4] Tout bouquin qui contient "elliptic" dans le titre, par exemple [2].

[5] Wolfram von Krantzwald, *De numberologis pyramidorum*, Ibister, 1880.