Les courbes elliptiques selon Don Zagier et John Tate

Francis Buekenhout, Charlotte Bouckaert

19 mai 2014

Math-UREM

Unité de Recherche sur l'Enseignement des Mathématiques
Prof. Fr. Buekenhout – Prof. J. Sengier – C. Bouckaert
fbueken@ulb.ac.be – sengier@ulb.ac.be – charlotte.bouckaert@gmail.com
http://www.ulb.ac.be/sciences/urem/

Campus Plaine, CP – 213
Bd du Triomphe — 1050 Bruxelles
Tél. Secr. (32) (2) 650 58 64
Fax (32) (2) 650 58 67

Avertissement

Le titre provisoire de ce travail a été jusqu'il y a peu :

La conférence de Don Zagier à l'Université Libre de Bruxelles le 3 décembre 2009
Equations diophantiennes, courbes elliptiques et un problème du millenium
Développements provenant du livre de Silverman et Tate 1992,
Rational Points on Elliptic Curves.

Francis Buekenhout et Charlotte Bouckaert se sont réunis à de nombreuses reprises entre 2010 et 2014 pour rédiger le présent document.

Table des matières

Chapitre 1

Un grand événement

La conférence de Don Zagier à l'Université Libre de Bruxelles le 3 décembre 2009 fut un grand événement de diffusion mathématique par un grand mathématicien. La conférence fut organisée par le professeur Luc Lemaire dans le cadre de l'Institut des Hautes Etudes de Belgique.

Luc Lemaire présente Don Zagier, un grand mathématicien passionnant et passionné, directeur du fameux *Max Planck Institut* à Bonn et professeur au Collège de France à Paris. Lemaire raconte sa première rencontre avec Don Zagier au cours d'un dîner à l'occasion du Congrès International des Mathématiciens à Madrid en 2006. Zagier avait en quelque sorte fait un exposé de Théorie des Nombres pour Lemaire en utilisant des serviettes en papier.

1.1 Le style du professeur

Zagier dispose de l'estrade, un tableau noir à gauche, un écran et rétroprojecteur au centre et un tableau blanc à droite sans oublier une table au bout à gauche avec craies, torchon, éponge ainsi qu'une table à droite pour ses documents et ses marqueurs. Il enchaîne les actions mathématiques de manière bondissante et en courant d'un site à l'autre. Son utilisation du tableau noir est contraire aux canons d'antan. Il écrit en grand au centre du tableau :

Equations diophantiennes
Courbes elliptiques

Il y poursuit longtemps sans effacer mais en caractères plus petits et en occupant soigneusement toute fenêtre encore découverte jusqu'à ce qu'il décide d'émigrer vers l'autre tableau puis de revenir, d'effacer une petite fenêtre, de la remplir et ainsi de suite.

1.2 Le public

La salle était bondée. Il fallut déployer des piles de chaises. Environ 100 personnes comprenant des jeunes de tout âge. Tout à fait conquis, heureux et chaleureux après l'exposé.

Chapitre 2

Un problème du millenium

Quels sont les problèmes du Millenium ?

Le titre de l'exposé de Don Zagier était *Equations diophantiennes, courbes elliptiques et un problème du millenium.*

Dans la revue *Notices of the AMS* de décembre 2009, on peut lire une critique du livre *The Millenium Prize Problems* (Réf. Carlson, Jaffe et A. Wiles 2006) par Robert C. Gunning (Réf. Gunning 2009).

Gunning commence par rappeler que les problèmes sont sang et vie des mathématiques. Les mathématiciens consacrent une bonne partie de leurs temps et de leur travail à résoudre des problèmes. Il faut que les problèmes ne soient ni trop faciles car dans ce cas ils ne conduisent à rien d'intéressant ni trop difficiles car dans ce cas ils ne conduisent à rien du tout.

Plusieurs mathématiciens ont proposé leurs propres listes de problèmes dans les domaines des mathématiques qui les intéressaient particulièrement et certains d'entre eux comme Paul Erdös ont même proposé des prix pour leurs solutions.

L'exemple le plus renommé est évidemment celui de la liste des vingt-trois problèmes proposée par David Hilbert dans son allocution au Congrès International des Mathématiciens qui a eu lieu à Paris en 1900. L'influence de cette liste de problèmes a influencé l'orientation de la recherche mathématique de manière déterminante à un degré vraiment étonnant. Cela tient bien sûr à la stature de celui qui l'a proposée – un des géants des mathématiques de son époque et de toutes les époques. C'est aussi dû à la vaste culture mathématique d'Hilbert et sa clairvoyance en ce qui concerne l'importance des problèmes qu'il a proposé et qui se mesure à la quantité d'efforts investis pour résoudre ces problèmes. Cet intérêt était encore vivace 74 ans plus tard comme en témoigne le Symposium de Mathématiques de 1974. Dans les proceedings de ce symposium on trouve une liste de problèmes de 27 domaines différents de mathématiques proposée par plusieurs mathématiciens et éditée par Jean Dieudonné, en hommage à la liste de Hilbert et avec le souci de composer une nouvelle liste de problèmes intéressants et importants qui puisse servir de guide à la recherche mathématique pour les prochains trois quarts de siècle.

La liste des problèmes du millenium est d'une autre nature. Elle ne vise pas à prévoir ou prescrire l'orientation des mathématiques du futur. Elle est plutôt une collection de quelques problèmes bien connus qui ont circulé depuis un certain nombre d'années, en l'occurrence depuis la fin du XIX^{e} jusqu'au milieu du XX^{e} siècle. Ces problèmes ont été au cœur de la recherche mathématique depuis longtemps et continueront sans nul doute à attirer les efforts de nombreux mathématiciens sans qu'il soit besoin d'autres incitants pour qu'ils s'y attellent. Cette liste a néanmoins de meilleures chances d'avoir une longue existence que n'importe quelle liste de problèmes post-hilbertienne, non seulement à cause de la qualité des problèmes choisis, mais aussi à cause de l'importance des retombées financières qui sont attribuées pour leurs solutions. L'idée d'attribuer des prix pour les solutions de problèmes mathématiques n'est pas neuve. Landon T. Clay, par l'intermédiaire du *Clay Mathematical Institute* fondé par lui et sa femme Lavinia D. Clay, a été un mécène remarquable pour la recherche mathématique.

La liste des problèmes du millenium patronnée par l'Institut Clay, avec l'excitation et la publicité

engendrée par la munificence des prix, peut bien avoir été conçue dans un but autre que celui des autres listes, celui d'augmenter la conscience et l'intérêt des non-mathématiciens pour la recherche mathématique et d'inspirer de futurs mathématiciens à s'engager dans des carrières stimulantes où interviennent les mathématiques et leurs applications.

Voici la liste des sept problèmes du millenium :

— la conjecture de Birch et Swinnerton-Dyer,
— la conjecture de Hodge,
— l'existence et de solution de l'équation de Navier-Stokes,
— la conjecture de Poincaré,
— le problème ouvert P = NP
— l'hypothèse de Riemann
— la théorie quantique de Yang-Mills.

La conjecture de Poincaré a été démontrée entre temps par Grigori Perelman (2002).

Chapitre 3

Développements provenant du livre de Silverman-Tate

3.1 A propos de John Tate, Prix Abel 2010

John Tate est né à Minneapolis, Minnesota en 1925. Il a toujours été fasciné par les puzzles mathématiques et a lu les livres de Dudeney que possédait son père (voir la section 6.4.2).

Il a fait des études de mathématiques à Harvard. En 1950, il a obtenu son doctorat à Princeton sous la direction d'Emil Artin.

John Tate a enseigné les mathématiques à Harvard et à Austin, Texas pendant plus de 60 ans et il a toujours aimé enseigner à tous les niveaux.

Rappelons que Tate a obtenu le Prix Wolf en 2002 et le Prix Abel en 2010. Voici la citation du jury :

"The Norwegian Academy of Science and Letters has decided to award the Abel Prize for 2010 to John Torrence Tate, University of Texas at Austin, *for his vast and lasting impact on the theory of numbers*."

3.1.1 Avis sur le livre de Silverman et Tate

Souvenons-nous de Paul Libois et de son maître Federigo Enriques qui furent d'ardents défenseurs d'un enseignement génétique qu'on pourrait également qualifier d'évolutif. Une référence qui importe est le traité de géométrie algébrique d'Enriques–Chisini (Réf. Enriques et Chisini 1915–1934).

Le livre de Silverman et Tate, *Rational Points on Elliptic Curves*, est un modèle actuel d'enseignement évolutif qui influence profondément notre parcours (Silverman et Tate 1992).

L'origine du livre se situe en 1961 dans un cours de Tate à Haverford College sous le titre *Rational Points on Cubic Curves*.

Joseph Silverman est un élève de Tate. Il a obtenu son doctorat à Harvard en 1982. Il est professeur à l'Université Brown et un spécialiste en théorie des nombres et en cryptographie.

Andrew Bremner a dit de ce livre :

« Les auteurs ont voulu écrire un manuel sur un sujet techniquement difficile qui soit accessible à des débutants et ils y sont admirablement parvenus. C'est vraiment un livre très agréable. ... L'inconvénient d'un texte pour "undergraduates" sur ce sujet est de ne pouvoir être entièrement rigoureux et comme le disent les auteurs : "beaucoup du matériel de base sur les courbes elliptiques présenté dans le chapitre I est destiné à expliquer et à convaincre plutôt qu'à démontrer rigoureusement". Un appendice développe la géométrie algébrique nécessaire, mais à travers tout le livre l'approche informelle à la géométrie sous-jacente permet un accès plus rapide et intuitif à la théorie des nombres. »

3.2 Importance du sujet

Citons la préface et l'introduction de Silverman-Tate :
"In view of the recent interest in the theory of elliptic curves for subjects ranging from cryptography to physics as well as the tremendous purely mathematical activity in this area, . . . "

Serge Lang à propos des courbes elliptiques a dit :
"It is possible to write endlessly on elliptic curves"

3.3 Application

Citons la préface et l'introduction de Silverman-Tate :
". . . we have described Lenstra's elliptic curve algorithm for factoring large integers. This is one of the recent applications of elliptic curves to the the "real world" , to wit the attempt to break certain widely used key ciphers. ":

". . . It is less well known that if the integer is fairly large, say of the order of 10^{100} or 10^{200}, it may be virtually impossible to perform that factorization. This is true even though there are very quick ways to check that an integer of this size is not itself a prime. In other words, if one is presented with an integer N with (say) 150 digits, then one can easily check that N is not prime, even though one cannot in general find any prime factors of N.

This curious state of affairs has beeen used by Rivest, Shamir, and Adelman to construct what is known as a public key cipher based on a trapdoor function. These are ciphers in which one can publish, for all to see, the method of enciphering a message; but even with encipherment method at hand, a would-be spy will not be able to decipher any messages. Needless to say, such ciphers have numerous applications, ranging from espionage to ensuring secure telecommunications between banks and other financial institutions. To describe the relation with elliptic curves, we will need to briefly indicate how such a "trapdoor cipher" works.

First one chooses two large primes, say p and q, each with around 100 digits. Next one publishes the product $N = pq$. In order to encipher a message, your correspondent only needs to know the value of N. But in order to decipher a message, the factors p and q are needed. So your messages will be safe as long as no one is able to factor N. This means that in order to ensure the safety of your messages, you need to know the largest integers that your enemies are able to factor in a reasonable amount of time.

So how does one factor a large number which is known to be composite? One can start trying possible divisors 2, 3, . . . , but this is hopelessly inefficient. Using techniques from number theory, various algorithms have been devised, with exotic sounding names like the continued fraction method, the ideal class group method, the $p-1$ method, and the quadratic sieve method. But one of the best methods currently available is Lenstra's Elliptic Curve Algorithm, which as the name indicates relies on the theory of elliptic curves. So it is essential to understand the strength of Lenstra's algorithm if one is to ensure that one's public key cipher will not be broken."

3.4 Quelques prix importants en relation avec des travaux sur les courbes elliptiques

Citons la préface et l'introduction de Silverman-Tate. Il convient de retenir
— Gert Faltings, médaille Fields 1986, pour sa démonstration de la conjecture de Mordell,
— Jean-Pierre Serre, Prix Abel 2003. Voici la citation du jury :
« L'Académie des Sciences et des Lettres de Norvège a décidé de décerner le prix Abel 2003 à Jean-Pierre Serre, Collège de France, Paris, France, *pour son rôle central dans l'élaboration de la forme moderne de nombreux domaines des mathématiques, notamment la topologie, la géométrie algébrique et la théorie des nombres.* »

3.5 Le nom « courbe elliptique »

Dans le chapitre I du livre de Silverman-Tate nous trouvons :
"A cubic equation in normal form looks like

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

Assuming that the (complex) roots of $f(x)$ are distinct, such a curve is called *elliptic curve*. (More generally, any curve birationally equivalent to such a curve is called an elliptic curve.) Where does this name come from, because these curves are certainly not ellipses? The answer is that these curves arose in studying the problem of how to compute the arc length of an ellipse. If one writes down the integral which gives the arc length of an ellipse and makes an elementary substitution, the integrand will involve the square root of a cubic or quartic polynomial. So to compute the arc-length of an ellipse, one integrates a function involving $y = \sqrt{f(x)}$, and the answer is given in terms of certain functions on the "elliptic" curve $y^2 = f(x)$."

Et dans le chapitre XI de Stillwell
"Integrals of the form $\int R[t, \sqrt{p(t)}]dt$, where R is a rational function and p is a polynomial of degree 3 or 4 without multiple factors, are called *elliptic integrals*, because the first example occurs in the formula for the arc length of the ellipse. (The functions obtained by inverting elliptic integrals are called *elliptic curves*. This drift in the meaning of "elliptic" is rather unfortunate because the ellipse, being parametrizable by rational functions, is not an elliptic curve!)"

3.6 Existe-t-il une solution en nombres entiers ?

Etant donné une équation diophantienne, plusieurs questions se posent immédiatement. Nous suivons leur énoncé par Tate :
"Here are some natural questions we might ask:

(a) Are there any solutions in integers?
(b) Are there any solutions in rational numbers?
(c) Are there infinitely many solutions in integers?
(d) Are there infinitely many solutions in rational numbers?

In this generality, only question (c) has been fully answered, although much progress has recently been made on (d)."

Réponse à la question (a) : footnote p. 5–6 "For polynomials $f(x_1, \ldots, x_n)$ with more than two variables, our four questions have only been answered for some very special sort of equations. Even worse, work od Davis, Matijasevic, and Julia Robinson has shown that in general it is not possible to find solution to question (a). That is, there does not exist an algorithm which takes as input the polynomial f and produces as output either "YES" or "NO" as answer to question (a)."

Chapitre 4

Diophante et Fermat

4.1 De Diophante à Fermat

Le mathématicien grec Diophante vécut à Alexandrie au 2^{e} siècle de notre ère. Les dates ne sont pas connues de manière précise. Zagier le situe entre 150 et 250. Ses œuvres sont consacrées à la théorie des nombres. Elles furent perdues pendant plus de mille ans. Elles furent retrouvées vers 1470.

Stillwell, dans la notice biographique de Diophante écrit (Stillwell 1989, chap. III, p. 36) :
"Diophantus lived in Alexandria during the period when Greek mathematics, along with the rest of Western civilization, was generally in decline. The catastrophes that engulfed the West with the fall of Rome and the rise of Islam, culminating in the burning of the library of Alexandria in A.D. 640, buried almost all details of Diophantus' life. His dates can be placed between A.D. 150 and 350, since he mentions Hypsicles (known to be c. 150) and is mentioned by Theon of Alexandria (C. 350). One other scrap of evidence, a letter of Michael Psellus (eleventh century), suggests A.D. 250 as the most likely time when Diophantus flourished. Apart from this, the only clue to Diophantus' life is a conundum in the *Greek Anthology* (c. A.D. 600): [Here Stillwell quotes Cohen and Drabkin 1958, p. 27]:

' God granted him to be a boy for the sixth part of his life, and adding a twelfth part to this, he clothed his cheeks with down. He lit him the light of wedlock after a seventh part, and five years after his marriage He granted him a son. Alas! late-born wretched child; after attaining the measure of half his father's life, chill Fate took him. After consoling his grief by this science of numbers for four years he ended his life.'

If this information is correct, then Diophantus married at 33 and had a son who died at 42, four years before Diophantus himself died at 84.

Diophantus' work went almost unnoticed for many centuries, and only parts of it survive. The first stirrings of interest in Diophantus occured in the Middle Ages, but much of the credit for the eventual revival of Diophantus belongs to Rafael Bombelli (1526–1572) and Wilhelm Holtzman (known as Xylander, 1532–1576). Bombelli discovered a copy of Diophantus' *Arithmetic* in the Vatican Library and published 143 problems from it in his *Algebra* [1572]. Xylander published the first Latin translation of the *Arithmetic* in 1575. The most famous edition of the *Arithmetic* was that of Bachet de Meziriac [1621]. Bachet glimpsed the possibility of general principles behind the special problems of the *Arithmetic* and, in his commentary on the book, alerted his contemporaries to the challenge of properly understanding Diophantus and carrying his ideas further. It was Fermat who took up this challenge and made the first significant advances in number theory since the classical era."

Nous poursuivons avec Zagier : « Les œuvres de Diophante étaient restées d'actualité. Cela dépassait de loin ce qu'on pouvait faire en Europe au XV^{e} siècle. »

Avant Fermat, Diophante ne fut pas réellement compris. Fermat (1601–1665) est le premier qui a compris Diophante et qui a apporté des contributions intéressantes aux sujets traités par Diophante.

4.2 Bachet, 1621

4.2.1 A propos de Bachet

Que sait-on de Bachet, de ses textes, de l'influence de Bachet sur Fermat, Descartes, Newton ?

Mathoverflow : Fermat's Bachet-Mordell Equation (Lemmermeyer 2010).

"Fermat once claimed that the only integral solution to $y^2 = x^3 - 2$ are $(3, \pm 5)$. Fermat knew Bachet's duplication formulas ..."

Stillwell : *Mathematics and Its History*, Chap 3., Sec. 3.2, p. 28, (Stillwell 1989)

"... The first is the theorem conjectured by Bachet [1621] (in his edition of Diophantus' work) that every positive integer is the sum of four integer squares. This was proved by Lagrange [1770]."

Descartes et Bachet Il semble que Descartes n'ait pas eu connaissance de la formule de duplication de Bachet.

Citons le livre *Descartes on polyhedra* (FEDERICO 1982, p. 130, note 100)) : "... Tannery states that Descartes did not know Bachet's translation. ..."

Observons que tout se passe comme si Bachet savait écrire la tangente.

4.2.2 La formule de duplication de Bachet

Nous reprenons ce qu'en disent Silverman et Tate dans l'introduction.
"As another example, we consider the problem of writing an integer as the difference of a square and a cube. In other words, we fix an integer$c \in \mathbb{Z}$ and look for solutions to the Diopantine equation

$$y^2 - x^3 = c$$

Suppose we are intereted in solutions in rational numbers $x, y \in \mathbb{Q}$. An amazing property of this equation is the existence of a *duplication formula* discovered by Bachet in 1621. If (x, y) is a solution with x and y rational, then it is easy to check that

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3} \right)$$

is a solution in rational numbers to the same equation. Further it is possible to prove (although Bachet was not able to) that if the original solution has $xy \neq 0$ and if $c \neq 1, -432$, then repeating this process leads to infinitely many distinct solutions. So if an integer can be expressed as the difference of a square and a cube of non-zero rational numbers, then it can be so expressed in infinitely many ways. For example, if we start with the solution $(3, 5)$ to the equation

$$y^2 - x^3 = -2$$

and apply Bachet's duplication formula, we find a sequence of solutions that starts

$$(3, 5), \left(\frac{129}{10^2}, \frac{-383}{10^3} \right), \left(\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3} \right), \ldots .$$

"

Chapitre 5

Situer la théorie des nombres

5.1 Théorie des nombres

Reprenons l'exposé de Zagier.

On s'occupe d'équations qui peuvent être résolues avec des nombres purs. C'est ce qu'on peut faire avec

$$, -1, 0, 1, 2, 3$$

Les Grecs classiques n'avaient pas vraiment la notion de nombre pur. Les nombres étaient une notion géométrique. Ils ne pouvaient pas imaginer

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

en raison du fait que x^2 était une aire, 1 était une longueur et qu'on n'additionnait pas une aire et une longueur.

5.2 Du théorème de Pythagore au théorème de Fermat-Wiles

L'exemple arithmétique le plus connu illustrant le théorème de Pythagore est

$$3^2 + 4^2 = 5^2$$

Zagier mentionne la corde à 12 nœuds pour produire des angles droits. Il donne un autre exemple :

$$8^2 + 15^2 = 17^2$$

Très tôt (Fermat) on s'est intéressé aux relations entre les nombres purs. Une des plus anciennes est

$$a^n + b^n = c^n \tag{5.1}$$

Tout le monde connaît la conjecture de Fermat concernant (5.1) écrite dans la marge du traité de Diophante en 1637. Fermat est mort trente ans après, sans avoir publié la démonstration de sa conjecture. Il s'est probablement rendu compte du fait qu'il s'était trompé.

La conjecture fut convertie en théorème par Andrew Wiles et Richard Taylor en 2000.

On peut faire quelque chose d'intermédiaire entre les problèmes trop faciles comme l'équation de Pythagore et des problèmes très difficiles comme le théorème de Fermat-Wiles.

Ceci se concrétise par les courbes elliptiques qui procurent des problèmes intéressants et difficiles.

5.3 Les solutions de l'équation de Pythagore

Don Zagier part de l'équation diophantienne la plus simple et la plus ancienne

$$x^2 + y^2 = c^2 \text{ où } c \in \mathbb{Q}$$

On en cherche les solutions (x, y) dans le plan affine $A_2(\mathbb{Q})$.

Par homothétie de rapport $\frac{1}{c}$ on se ramène à

$$x^2 + y^2 = 1 \text{ (cercle unité)}$$

On voit la solution $(0, 1) = a$.

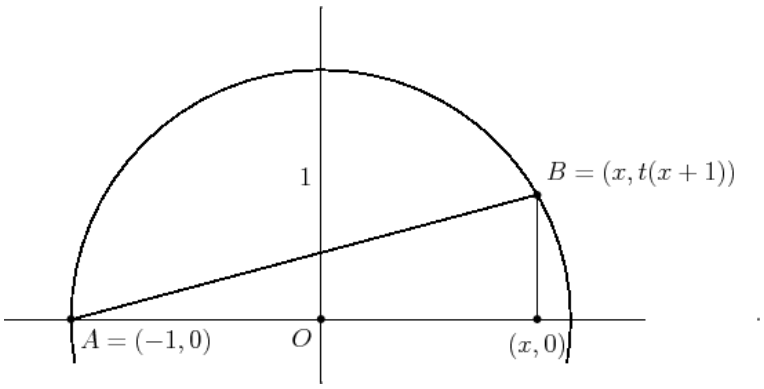


FIGURE 5.1 – ***L'équation de Pythagore : figure provisoire

Si $(u, v) = b$ est une autre solution, la droite ab est

$$y - 1 = \frac{v-1}{u}x$$

Son coefficient angulaire $\frac{v-1}{u} := t$ est rationnel.

Réciproquement, pour tout nombre rationnel t, la droite par a, de pente t est

$$y - 1 = tx$$

Elle recoupe le cercle unité en un point (u, v) tel que

$$\begin{cases} u^2 + v^2 = 1 \text{ et} \\ \dfrac{v-1}{u} = t \end{cases}$$

Eliminant u, on obtient

$$v^2 - \frac{2v}{1+t^2} + \frac{1-t^2}{1+t^2} = 0$$

et

$$v = \frac{1-t^2}{1+t^2}$$

puis

$$u = \frac{-2t}{1+t^2} \tag{5.2}$$

Remarque : Dans (5.2) nous reconnaissons au signe près, des formules de trigono dans lesquelles $t = \tan\frac{\alpha}{2}$.

Conclusion : tout nombre rationnel t livre une solution du problème diophantien $x^2+y^2=1$ à savoir (5.2).

Zagier 1984 écrit que Diophante faisait exactement ça (sans disposer du mode d'écriture qui est le nôtre depuis Descartes).

Nous citons la première page de l'article de Zagier 1984 :

"Consider a Diophantine equation in two variables, i. e., a polynomial equation $f(x, y) = 0$ with rational coefficients which we want to solve in rational numbers. Already in the works of Diophantus it is clear that the level of difficulty of this problem is very different for different classes of polynomials f. If f is quadratic, then , given one solution (x_0, y_0), one can find all solutions in terms of a rational parameter t by solving the linear equation $(1/u)f(x_0 + u, y_0 + tu) = 0$ (this method was used sporadically long before, and systematically by Diophantus). For cubic and certain quartic f, there are methods in Diophantus' work – and later much more extensively in Fermat's – for studying the rational solutions of $f = 0$ and, particularly, for constructing new solutions out of known ones. For higher degree f no general method has ever been found. Poincaré realized that this division into three classes depends on the toplogy of the set of complex points of the curve X defined by the equation $f(x, y) = 0$ (or rather by its projective version $f(x, y, z) = 0$, i. e., on the genus g of the Riemann surface $X(\mathbb{C})$. If $g = 0$ the set of rational points $X(\mathbb{Q})$, if nonempty, is isomorphic to $P^1(\mathbb{Q})$. If $g = 1$ then $X(\mathbb{Q})$, if nonempty, has the structure of an abelian group. (In this case the curve can always be put into the standard Weierstrass form

$$y^2 = 4x^3 - ax - b \quad (a, b \in \mathbb{Z}), \tag{5.3}$$

and the group structure is $O =$ point at infinity, $-P = (x, -y)$ if $P = (x, y)$, $P + Q + R = 0$ if $P, Q, R \in X(\mathbb{Q})$ are colinear). If $g \geq 2$ then we know by Faltings' recent work that $X(\mathbb{Q})$ is a finite set ("Mordell conjecture"); no further structure is known. the most interesting case forme a Diophantine point of view is thus $g = 1$, in which case we call X an elliptic curve and write E instead of X. here Poincaré conjectured, and Mordell proved, that the abelian group $E(\mathbb{Q})$ is finitely generated; the structure theorem for such group then gives

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathcal{F} \tag{5.4}$$

for some integer $r \geq 0$ and some finite abelian group $\mathcal{F}$. For a given curve E one can find $\mathcal{F}$ by a finite algorithm, while for r we can get upper bound by descent (Fermat) and lower bound by exhibiting independent solutions; if we are lucky , these agree. It is known exactly what group $\mathcal{F}$ can occur: $\mathcal{F}$ has the structure $\mathbb{Z}/(2n-1)\mathbb{Z}, \mathbb{Z}/2n\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for some $n \in \mathbb{N}$, depending on whether $4x^3 - ax - b$ in equation 5.3 has 0, 1, or 3 rational roots (this is elementary), and a deep theorem of Mazur (1977) says that n is then $\leq 5, \leq 6,$ or ≤ 4 respectively, all fifteen cases occurring infinitely often. As for r, it is known by recent examples of Mestre (1983, 1984) that value as large as 14 occur, and it is conjectured that all values can occur.

By equation 5.4 the number of rational solutions of $f(x, y) = 0$ is finite or infinite according to whether $r = 0$ or $r > 0$."

Isabella Bashmakova, grande spécialiste de l'histoire de l'algèbre, explique de manière détaillée la relation qu'elle perçoit entre la démarche de Diophante et la démarche actuelle décrite plus haut (Réf. Bashmakova and Smirnova 1999 p.40). Toutefois dans son livre consacré à Diophante (Réf. Meskens 2010), Ad Meskens conteste l'argument de Bashmakova avec d'autres arguments. Nous le citons :

"I. Bashmakova writes:

"In his *Arithmetic* Diophantus [...] entirely solved in a purely algebraic way the problem concerning the rational points of second degree curves. In the same work he used the tangent and secant methods (again treated in algebraic way) for the discovery of rational points on curves of third degree."

This is giving too much honour to Diophantos. Although the problems can be translated into our mathematical language for rational points on curves, this notion is completely absent in Diophantos' oeuvre. He sometimes uses (ingeniously found) algorithms, for which no justification is given. The fact that

Diophantos consistently used these algorithms in the same fashion seems to indicate that he did understand that they were generally applicable.

Footnote 110: In his interpretation Rashed (1984) uses a battery of modern notions which would be in any intrepretation alien to Diophantos or any ancient Greek mathematician."

Pour plus de détails consulter le livre de Meskens 2010.

Cette section illustre la déclaration synthétique faite par Zagier en début de conférence selon laquelle les courbes du 2^{e} degré sont rationnelles (un terme pas expliqué à ce moment) et que toute courbe diophantienne rationnelle possède une infinité de solutions.

Par la suite, il a révélé qu'une courbe est rationnelle si elle peut s'exprimer par des équations paramétriques

$$x = \frac{P(\lambda)}{R(\lambda)}, y = \frac{Q(\lambda)}{R(\lambda)}$$

où P, Q, R sont des polynômes.

Chapitre 6

Courbes elliptiques

6.1 Suivons Zagier

Après l'explication relative à l'équation de Pythagore et aux courbes rationnelles, Zagier explique que d'autres courbes très simples constituent la classe des courbes elliptiques. Dès le 3^{e} degré, celles-ci apparaissent. En fait, toute courbe du 3^{e} degré qui n'est pas rationnelle et qui n'est pas décomposée est une courbe elliptique. Les courbes elliptiques sont centrales dans l'exposé de Zagier.

Leur nombre de solutions peut être infini ou fini et le problème majeur qu'il discute est de trouver un critère simple permettant de faire la différence. Cette idée constitue le fond de la conjecture de Birch et Swinnerton-Dyer.

Toute courbe du 3^{e} non décomposable peut s'écrire moyennant changement d'axes (projectifs) sous la forme

$$y^2 = x^3 + Ax + B \tag{6.1}$$

et la courbe est elliptique ou rationnelle selon que le discriminant $\Delta = -16(4A^3 + 27B^2)$ est différent ou égal à zéro.

En outre, toute courbe elliptique de degré quelconque peut se transformer de manière birationnelle en courbe de la forme équation (6.1).

Les nombreux exemples proposés par Zagier ont été recueillis par Jean-Claude Matthys (Réf. Matthys 2009) et nous les utilisons à présent.

Zagier s'occupe du nombre de solutions (rationnelles) sur une courbe algébrique.

1. Une courbe de degré 1 ou 2 livre une courbe rationnelle (c.-à-d. de genre 0) et elle admet une infinité de solutions.
2. Une courbe de degré 3 (de genre non nul) est elliptique (de genre 1). Elle admet une infinité ou zéro solutions.
3. Une courbe de degré $n \geq 4$ de type général (« la poubelle » dit-il malicieusement) est hyperelliptique ($g \geq 2$). Elle n'admet qu'un nombre fini de solutions vertu de la conjecture de Mordell 1917 convertie en théorème par Gert Faltings en 1984. Ce résultat lui vaut la Médaille Fields.

   Théorème 1. (Faltings' Theorem (Mordell's conjecture)) *Let K be a number field and let $C = K$ be a non-singular curve defined over K of genus $g \geq 2$. Then $C(K)$ is finite.*

$$b^2 - a^2 = c^2 - b^2 = n$$

Zagier illustre la situation générale par des exemples.

6.2 Le nombre congruent

Cette notion provient d'un manuscrit arabe (980 de notre ère) et se retrouve dans le *Liber Quadratorum* de Fibonacci (1225).

Le nombre entier n est *congruent* ssi n est l'aire d'un $\mathbb{Q}$-triangle rectangle, c'est-à-dire qu'il existe $a, b, c \in \mathbb{Q}$ avec $a^2 + b^2 = c^2$ et $n = \frac{ab}{2}$.

« Ainsi 6 est l'aire du triangle rectangle de côtés $3, 4$ et 5 que tout le monde a rencontré lors de la leçon sur le théorème de Pythagore (notez que $3^2 + 4^2 = 5^2$ et $6 = \frac{3\times 4}{2}$)

(Funar Réf. Funar 2009). »

Voici une définition équivalente du nombre congruent :
Le nombre n entier est congruent ssi il existe une suite arithmétique de trois carrés et de raison n.
Nous travaillons donc avec n, x, y, z tels que $x, y, z \in \mathbb{Q}$ et

$$y^2 - x^2 = n,$$
$$z^2 - y^2 = n$$

Pour $n = 6$, on a le triplet

$$(x, y, z) = \left(\frac{1}{2}, \frac{5}{2}, \frac{7}{2}\right)$$

A titre d'exemple, 5 est congruent via

$$(a, b, c) = \left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$$
$$(x, y, z) = \left(\frac{31}{12}, \frac{41}{12}, \frac{49}{12}\right)$$

Déterminer si un entier est congruent ou pas, est un problème très ancien et très difficile. Grâce à Zagier (Koblitz, Réf. Koblitz 1984), nous savons que 157 est congruent via

$$(a, b, c) = \left(\frac{6803298487826435051217540}{411340519227716149383203}, \frac{411340519227716149383203}{21666555693714761309610411340519227716149383203},\right.$$

$$\left.\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}\right)$$

Suivons Colmez (Colmez 2005, p. 2)
« Cet exemple stupéfiant montre que la chasse aux triangles rectangles à côtés rationnels d'aire D risque d'être un peu acrobatique ... Le résultat suivant de Tunnell 1983 n'en est que plus remarquable.

Théorème 2. *Soit D un entier impair sans facteur carré. Si D est congruent, alors*

$$|\{x, y, z \in \mathbb{Z}, 2x^2 + y^2 + 8z^2 = D\}| = 2\Delta|\{x, y, z \in \mathbb{Z}, 2x^2 + y^2 + 32z^2 = D\}|.$$

Réciproquement, si D vérifie le théorème 2, et si une forme faible de)la conjecture de Birch et Swinnerton-Dyer est vraie, alors D est congruent.

Il y a un résultat similaire pour D pair. Comme il est très facile de décider si D vérifie ou non le théorème 2, cela fournit un critère effectif permettant de décider qu'un nombre donné est non congruent, ou (sous Birch et Swinnerton-Dyer) congruent, et ce, sans exhiber de triangle rectangle d'aire D.

Un entier congru à 5 ou 7 modulo 8 vérifie le théorème 2 car les deux ensembles sont vides, mais on ne sait pas montrer que cela implique que D est congruent ... »

6.2.1 Des nombres congruents aux courbes elliptiques chez Koblitz

Voici quelques extraits du chapitre I du livre de KOBLITZ 1984 :
"The theory of elliptic curves and modular forms is one subject where the most diverse branches of mathematics come together: complex analysis, algebraic geometry, representation theory, number theory. While our point of view will be number theoretic, we shall find ourselves using the type of techniques that one learn in basic course in complex variables, real variables, and algebra. A well-known feature of number theory is the abundance of conjectures and theorems whose statements are accessible to high school students but whose proofs either are unknown or, in some cases, are the culmination of decades of research using some of the most powerful tools of twentieth century mathematics."

"It eventually became known that the numbers $1, 2, 3, 4$ are not congruent numbers, but $5, 6, 7$ are. However, it looked hopeless to find a straightforward criterion to tell whether or not a given n is congruent. A major advance in the twentieth century was to place this problem in the context of the raithmetic theory of elliptic curves. It was in this context that Tunnell was able to prove his remarkable theorem.

Here is part of what Tunnell's theorem says (the full statement will be given later):

Théorème 3. (Tunnell). *Let n be an odd squarefree natural number. Consider the two conditions:*

(A) n is congruent;

(B) the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$.

Then (A) implies (B); and, if a weak form of the so-called Birch-Swinnerton-Dyer conjecture is true, then (B) also implies (A).

The central concepts in the proof of Tunnell's theorem – the Hasse-Weil L-function of an elliptic curve, the Birch-Swinnerton-Dyer conjecture, modular forms of half integer weight – will be discussed in later chapters."

6.2.2 Le théorème de Tunnell dans Koblitz

Le livre de Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms* publié en 1984 et destiné à des étudiants avancés a pour objectif de démontrer le théorème de Tunnel publié quelques mois auparavant (KOBLITZ 1984).

Koblitz consacre tout le quatrième et dernier chapitre au théorème de Tunnell et il n'a pas la démonstration complète.

Nous citons ici quelques extraits du livre de Koblitz :

"Thus we can write

$$L(E_1, s) = L_g(s) = \sum b_m m^{-s};$$
$$L(E_n, s) = L_g(\chi_D, s) = \sum \chi_D(m) b_m m^{-s}.$$

We saw that the critical value $L(E_n, 1) = L_g(\chi_D, 1)$ vanishes if and only if n is a congruent number ("only if" here is conditional upon the Birch-Swinnerton-Dyer conjecture). It is this critical value which Waldpurger's theorem provides a means of describing.

Let β denote the "real period" of $E_1 : y^2 = x^3 - x$, which is obtained by integrating dx/y over the segment $[1, \infty)$ where y is real:

$$\beta = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} = 2.622 \cdots .$$

Théorème 4. ([Tunnell 1983]). *There exist a form* $f = \sum a_m q^m \in S_{3/2}(\tilde{\Gamma}_0(128))$ *and a form* $f' = \sum a'_m q^m \in S_{3/2}(\tilde{\Gamma}_0(128), \chi_2)$ *such that* $Shimura(f) = Shimura(f') = g = \sum b_m q^m$ *and*

$$f(x) = \begin{cases} \frac{\beta}{4\sqrt{n}} a_n^2 \text{ for } n \text{ odd;} \\ \frac{\beta}{2\sqrt{n}} a'^2_{\frac{n}{2}} \text{ for } n \text{ even.} \end{cases}$$

„

"We note that very recently B. H. Gross and D. Zagier [1983] have been able to show that the weak Birch-Swinnerton-Dyer conjecture is true for E_n for a large class of n. For such n, Tunnell's theorem becomes an unconditional equivalence between the congruent number property for n and the equalities in the theorem involving the number of representations of n (or $\frac{n}{2}$) by some simple ternary quadratic forms.

As mentioned in Chapter I, Tunnell's theorem has the practical value of leading to an effective and rapid algorithm for determining wether n is a congruent number. In addition, one can give quick new proofs of certain conditions for n not to be a congruent number. For example, if n is a prime congruent to 3 modulo 8, Tunnell shows that $a_n \equiv 2 \mod 4$, and therefore n is not a congruent number.

The only sense in which Tunnell's theorem is not yet a completely satisfactory solution to the ancient congruent number problem is that in one direction it is conditional upon the weak Birch-Swinnerton-Dyer conjecture for certain elliptic curves. But lately, significant progress has been made toward a proof of that conjecture in enough generality to include the curves E_n. In addition to the work of Gross and Zagier mentioned above, R. Greenberg [1983] was able to prove that, if the conjecture were to fail for an elliptic curve such as E_n wich has complex multiplication, then that would imply a highly improbable combination of consequences for the Tate-Shafarevich group of the elliptic curve.

It is remarquable that the nearly complete solution that we now have to such an old and naive question as the congruent number problem, has required some of the most powerful and sophisticated tools from diverse branches of twentieth century mathematics."

6.2.3 Suivons Zagier (bis)

Zagier introduit la notation N_{pair} : nombre de solutions paires et N_{impair} : nombre de solutions impaires. Il déclare que le « nombre magique » S associé à chaque courbe elliptique,

$$S = (N_{\text{pair}} - N_{\text{impair}})^2.$$

On a par exemple le résultat suivant « conjecturé » par Fibonacci (1175-1240) et dû à Fermat (Colmez Réf. Colmez 2005, p.2).

Théorème 5. *1 n'est pas un nombre congruent.*

« C'est une des nombreuses utilisations que Fermat a trouvées pour sa méthode de "la descente infinie". Remarquons que si a, b, c sont des entiers non nuls vérifiant

$$a^4 - b^4 = c^4, \text{ et si } x = \frac{a^2}{b^2},\ y = \frac{ac^2}{b^3}\ , \text{ alors } y = x^3 - x.$$

Le fait que 1 n'est pas congruent implique donc le théorème de Fermat pour l'exposant 4. »
Les nombres 2, 3, 4 ne sont pas congruents.

6.3 Problème de Fermat (1643 : Lettre à Mersenne)

$a^2 + b^2 = c^2$ et $a + b$ carré et c carré.
Solution

$$a = 1061652293520$$
$$b = 4565486027761$$
$$c = 4687298610289$$

C'est la plus petite solution.

6.4 $x^3 + y^3 = m$, avec m entier

Quels sont les nombres premiers qui soient la somme de deux cubes rationnels ?
Exemple

$$13 = \frac{8}{27} + \frac{343}{27} = \left(\frac{2}{3}\right)^3 + \left(\frac{9}{3}\right)^3$$
$$1789 = \left(\frac{2513}{1008}\right)^3 + \left(-\frac{1388}{1005}\right)^3$$

Ce n'est pas vrai pour 5 et 11.

6.4.1 Conjecture de Sylvester (1847)

Si $p \equiv 4, 7, 8 (\mod 9)$, alors p est la somme de deux cubes rationnels (Dasgupta et Voight 2009, p. 90).

6.4.2 Henry Ernest Dudeney, célèbre pour ses puzzles

Dans l'article de Andrew Bremner (Bremner 2011) on peut lire :
"Henry Ernest Dudeney [1857–1930] was a foremost constructor of puzzles during the early part of the twentieth century. His puzzles covered an extraordinary range, from geometric dissections to river crossing problems to puzzles in logic and in combinatorics; Among his books are: *The Canterbury Puzzles and other Curious Problems*, *The World's Best Word Puzzles*, *Modern Puzzles*, *536 Puzzles and Curious Problems*, and *More Puzzles and Curious Problems*.

Of his mathematical puzzles, the most intriguing relate to writing an integer as the sum of two rational cubes. For example, *The Canterbury Puzzles and other Curious Problems* lists the puzzle of the "Silver Cubes", which asks for the dimensions in rational numbers of two cubes of silver that contain precisely 17 cubic inches. This requires finding a pair of (positive) rational numbers x, y satisfying $x^3 + y^3 = 17$. The "Puzzle of the Doctor of Physic" requires finding the diameters of two spheres (in rational numbers) whose combined volume equals that of two spheres of diameters one foot and two feet (and, of course, different from one foot and two feet). This in turn resolves easily into finding positive rational numbers x, y, not equal to $1, 2$ with $x^3 + y^3 = 1^3 + 2^3$.

The solutions given must have startled his readership, who likely were more accustomed to solving simple problems in logic: for the first problem, the solution given is $(x, y) = (\frac{104940}{40831}, \frac{11663}{40831})$, and for the second $(x, y) = (\frac{415280564497}{348671682660}, \frac{676702467503}{348671682660})$. How on earth did Dudeney find these solutions with their big numbers? There were no calculators or other aids at that time, and he could only have used paper and pencil computations. He had little formal education, starting work as a clerk in the English civil service at the age of 13. The solutions astonished me as a young teenager when first coming across these puzzles in the books. It took several years for me to realize just how Dudeney must have done it!

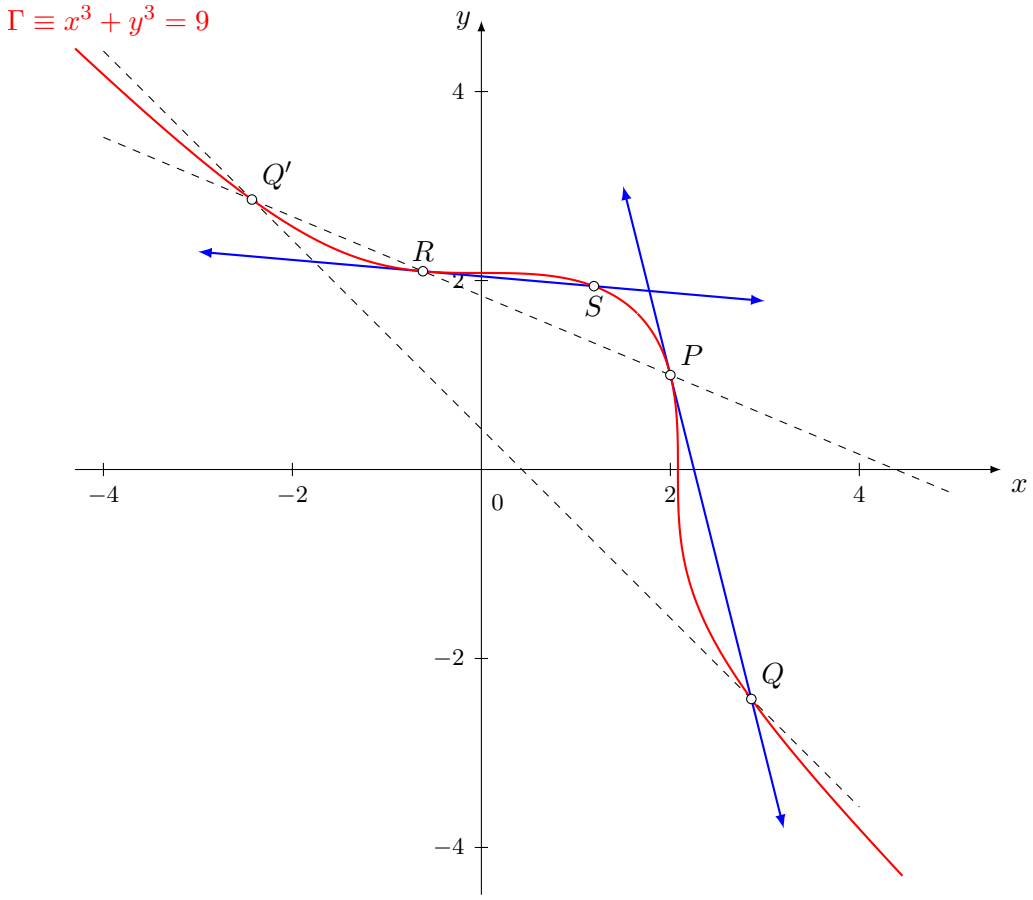


Figure 6.1: Equation $x^3 + y^3 = 9$, $P = (2, 1)$

The key is to think geometrically. The Doctor of Physic for instance asks us to find rational numbers x, y satisfying $x^3 + y^3 = 9$, in other words to find a rational *point* (x, y) on the *curve* with equation $x^3 + y^3 = 9$. The graph of this curve is shown in Figure 6.1. We certainly know one point on the curve, namely $P = (2, 1)$.

Suppose we construct the tangent line l to the curve at the point P. It has an equation of type $y = mx + b$, so has exactly three points of intersection with the cubic curve $x^3 + y^3 = 9$, that is , precisely where $x^3 + (mx + b)^3 - 9 = 0$. Since P is a point of tangency, the cubic will have double root at the x-coordinate(=2) of P; and the third root will correspond to the point Q in Figure 6.1. Now if a cubic with integer coefficients has two rational roots, then the third root will be rational. Let's actually do this, and find the coordinates of Q.

To compute the equation of l, we need to know the value of $\frac{dy}{dx}$ at P. But $x^3 + y^3 = 9$, and using implicite differentiation, $3x^2 + 3y^2 \frac{dy}{dx} = 0$, so that $\frac{dy}{dx} = -\frac{x^2}{y^2}$.

Thus at $P = (2, 1)$, $\frac{dy}{dx} = -\frac{2^2}{1^2} = -4$. The equation of the tangent line l is therefore $y - 1 = -4(x - 2)$, that is $y = -4x + 9$. Where does this line meet the curve? It will do so where $x^3 + (-4x + 9)^3 = 9$, namely, where $9(-7x^3 + 48x^2 - 108x + 80) = 0$. Because of the tangency, we know there is a double root at $x = 2$, and sure enough, the cubic factors to give $9(x - 2)^2(20 - 7x) = 0$. Accordingly, the line meets the curve again at the third point Q with x-coordinates equal to $\frac{20}{7}$. Since Q lies on the tangent line $y = -4x + 9$, it is easy to compute the y-coordinate, namely $y = -\frac{80}{7} + 9 = -\frac{17}{7}$. Thus $Q = (\frac{20}{7}, -\frac{17}{7})$.

We now have found a new solution to $x^3 + y^3 = 9$. The only problem is that one of the numbers is

negative, and spheres of negative diameter pose an existential problem for Doctor of Physic! Well, one suggestion is simply to repeat the previous process, but start with the point Q rather than P; this will in turn deliver a new point. However, by the following trick we can keep the numbers smaller in size. The curve obviously has symmetry about the line $y = x$: that is, if (x, y) is on the curve, then so is (y, x). If we now join the flipped point $Q' = (-\frac{17}{7}, \frac{20}{7})$ to the point $P = (2, 1)$, we have a line which as before meets the cubic in three points, of which we know two: so again we should find a new point R. Here goes. The line joining $(-\frac{17}{7}, \frac{20}{7})$ to the point $P = (2, 1)$ has the equation $(y - \frac{20}{7})/(\frac{20}{7} - 1) = (x + \frac{17}{7})/(-\frac{17}{7} - 2)$, that is, $y = -\frac{13}{31}x + \frac{57}{31}$. This line meets the curve where $x^3 + (-\frac{13}{31}x + \frac{57}{31})^3 = 9$, and so expanding the parenthesis, where $3066x^3 + 3211x^2 - 14079x - 9214 = 0$. We know the cubic must contain the factors $x = \frac{17}{7}$ and $x - 2$: and sure enough, we get $(x - 2)(7x + 17)(438x + 271) = 0$, giving the x-coordinate of the new point R as $x = -\frac{271}{438}$. The y-coordinate of R is now given by $y = -\frac{13}{31}x + \frac{57}{31} = \frac{919}{438}$. Sure thing, $(-\frac{271}{438})^3 + (\frac{919}{438})^3 = 9$. But the sphere still has negative diameter!

Of course, what we seek is a rational point on the curve which lies in the *first* quadrant, where $x > 0, y > 0$. It appears plausible from Figure 6.1 that the tangent line at R meets the curve again in the first quadrant. As a check, the tangent line at R has equation $y = -\frac{73441}{844561}x + \frac{176596}{73441}$, which meets the curve twice at R, and at the new point $(\frac{415280564497}{348671682660}, \frac{6767022467503}{348671682660})$ which does indeed lie in the first quadrant, and provides Dudeney's solution to the problem."

On retrouve une référence à la courbe $C : x^3 + y^3 = 9$ dans l'article de Brunault 2012.

6.4.3 La conjecture de Birch et Swinnerton-Dyer et S le « nombre magique »

Zagier dit : « Birch et Swinnerton-Dyer ont une conjecture brillante en 1965. Ils associent un nombre S « le nombre magique » à chaque courbe elliptique. »

Zagier parle de « Deus S machina ».

— $S = 0$ ssi l'équation possède un nombre infini de solutions (de points rationnels).

— $S \neq 0$ ssi l'équation possède un nombre fini de solutions (de points rationnels).

> Selon Coates-Wiles toute courbe elliptique peut être paramétrée par des formes modulaires par des formes modulaires que nous n'entreprenons pas d'expliquer ici.
>
> Nous citons Eric W Weisstein 2011 :
>
> "In 1976, Coates and Wiles showed that elliptic curves with complex multiplication having an infinite number of solutions have L-functions which are zero at the relevant fixed point. This is a special case of the Swinnerton-Dyer conjecture."
>
> Nous citons Colmez 2005 :
>
> « Coates et Wiles (1977) ont démontré que, si $E = C_D$, ou plus généralement si E est une courbe elliptique sur $\mathbb{Q}$ à multiplication complexe, alors « $L(E, 1) \neq 0$ » ⇒ « $r(E) = 0$ ». »

6.4.4 Pour $x^3 + y^3 = m$

m	12	34	56	7	...	381	382	383
S	11	11	10	0	...	4	0	4

6.4.5 Rodríguez-Villegas et Zagier 1994

Nous citons Dasgupta et Voight 2009 :

"A few words on the case $p \equiv 1(\mod 9)$.

For $p \equiv 1(\mod 9)$, the BSD conjecture predicts that $\mathrm{rk}(E_p(\mathbb{Q})) = 0$ or 2, depending on p. This case was investigated by Rodriguez-Villegas and Zagier (Réf. Rodríguez-Villegas and Zagier 1994)."

Signalons que Villegas et Zagier donnent une suite $B_0, B_1, \ldots$ explicite.

En outre, $S = 0$ implique que B_n est divisible par p.

6.4.6 Mordell 1922

Voici une citation du blog *Le coin des amatheurs* (Amatheurs 2009) :
« La conjecture de Birch et Swinnerton-Dyer
Certaines courbes sont appelées elliptiques. En 1922, Louis Mordell a démontré que pour toute courbe elliptique, on peut trouver un nombre fini de ses points de manière à ce que toute la courbe soit engendrée par ces quelques points. Ces points sont appelés base finie de la courbe. On peut également associer à la courbe une fonction, souvent notée L, qui dénombre les points de la courbe ayant une certaine propriété commune. La conjecture fait un lien entre la base finie de la courbe et la fonction L. »

Dans l'article de Brunault 2012, on peut lire :
« En 1922, le mathématicien britannique Louis J. Mordell démontre le résultat fondamental suivant.

Théorème de Mordell : *Soit C une courbe elliptique. Il existe un ensemble fini S de points rationnels de C tel que tout point rationnel de C s'obtienne à partir de S par un nombre fini d'applications de la méthode des tangentes et sécantes.*

Autrement dit, il existe un système fini de points rationnels de C qui permet d'obtenir tous les autres grâce à la méthode des tangentes et sécantes. Ce théorème marque une étape importante dans l'étude des courbes elliptiques : l'énoncé ne concerne plus une courbe elliptique particulière, ou une famille particulière de courbes elliptiques, mais bien toutes les courbes elliptiques sans exception. »
Pour les courbes elliptiques, le nombre de solutions avec moins de N chiffres est de l'ordre de grandeur $(\sqrt{N})^r$ (r est le rang).

6.5 Fonction elliptique

L'étude des fonctions elliptiques a une histoire très étendue et qui influence celle des courbes elliptiques.

Nous serons brefs sur ce sujet immense.

Suivons d'abord l'exposé des débuts par Takasaki 2012 :
"Elliptic Functions

Early Days

Elliptic functions are now understood in several different ways. The most classical way is to consider the inverse of an elliptic integral. Elliptic integrals were studied in detail by Euler and Legendre, but they did not considered the inverse functions. It is Gauss who first noticed the importance of the inverse functions.

C.F. Gauss

unpublished work on elliptic functions started in 1799 and continued through the first decade of the 19th century Gauss studied the inverse function of the arclength of a lemniscate. The arclength integral is a typical elliptic integral. Gauss considered the inverse function of this integral as an analogue of the trigonometric (sine and cosine) functions, discovered a number of essential properties of these functions, and even arrived at the noion of elliptic theta functions and modular functions. Some of these results were later rediscovered by Abel and Jacobi independently.

The unpublished work of Gauss was rediscovered (and largely extended) by Niels H. Abel more than twenty years later. Of course Abel did not know of Gauss' work on elliptic functions. He was led to elliptic functions through his preceding research on algebraic equations, in particular, the "lemniscate equations" that Gauss considered in his book on number theory (but without any explicit comment on the relation to elliptic functions).

N.H. Abel "Memoire sur une propriété générale d'une classe tres étendue de fonctions transcendents", submitted to the Academy of Science during his first visit to Paris in 1826, but "lost" for many years and finally published in 1841. This paper presents a result that is now known as "Abel's theorem". This is a

generalization of Euler's results on elliptic integrals, and became a prototype of the subsequent studies on algebraic curves and Riemann surfaces. N.H. Abel "Recherches sur les fonctions elliptiques", published in Crelle's journal (J. Reine Angew. Math.) vol. 2 (1827) and vol.3 (1828) In these papers, Abel arrived at the same position as Gauss did, namely the inverse functions of elliptic integrals and the double periodicity. Even some of the notations were the same. That was the true beginning of the studies on elliptic functions in the 19th century.

While Abel was preparing a far extended version of "Recherchez", a paper of Jacobi appeared in "Astronomische Nachrichten". (This is a journal founded by H.C. Schumacher, who was astronomer and a very intimate frend of Gauss.)

C.G.J. Jacobi published two papers on elliptic integrals in "Astronomische Nachrichten", vol. 123 (1827) and vol. 127 (1827) In this paper, Jacobi reported a theorem on elliptic integrals, first without any proof, then with a proof based on the idea of inversion of elliptic integrals and the double periodicity.

Abel was shocked by this paper of Jacobi. This paper showed that Jacobi was catching the most essential part of elliptic functions. Abel was thus suddenly forced to entere a rivalry with Jacobi. Abel did a counterattack by publishing a more general result in the same journal in 1828, but had to suspend the project for the second part of "Recherche". This rivalry, however, was interrupted by Abel's death in 1829. Jacobi continued his researches, studying in particular the theta functions as an independent subject.

E. Galois mentioned a few results on abelian integrals in the letter written the day before his death in 1832 Galois's last letter mentioned, besides his work on algebraic equations, a few general results on abelian integrals. This is quite surprising, because even Jacobi had just started his researches on hyperelliptic functions.

Riemann, Weierstrass, and their successors

The double periodicity, already noticed by Gauss, of elliptic functions implies that the most natural stage of the theory of elliptic function is a torus, namely, a Riemann surface of genus one. The notion of Riemann surfaces (or, equivalently, of complex algebraic curves) provides a unified geometric framework for understanding previously known results on elliptic and hyperelliptic integrals. Of course it was Riemann who first proposed this geometric framework.

G.F.B. Riemann

Theorie der Abelischen Funktionen, J. Reine Angew. Math. 54 (1857), 115 - 155

Weierstrass aimed at a rigorous analytical formulation of theory of complex analytic functions. Of particular importance was the justification of infinite series/product expansion. For elliptic functions, Gauss, Abel and Jacobi already made full use of such expansions. Having the infinite product expansion of Euler's gamma function as a prototype, Weierstrass defined his famous sigma function by an infinite product, and reorganized the theory of elliptic functions in his theory of complex analytic functions:

K. Weierstrass Mathematische Werke, I - VII, Akademische Verlag 1894 - 1927

Along with these theoretical progress, many mathematicians published monographs and textbooks on elliptic functions in the second half of the 19th century (see F. Klein's "Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert, Springer-Verlag 1926 - 27, Chelsea 1956)."

Une histoire approfondie des fonctions elliptiques est due à Houzel (Dieudonné et al. 1986).

Soulignons trois des nombreux thèmes structurant le travail de Houzel

— 5 : Inversion et double périodicité : Gauss, Abel, Jacobi, Riemann, Briot et Bouquet, Weierstrass (1795–1860).

— 6 : Fonctions méromorphes doublement périodiques : Liouville, Eisenstein (1840–1850).

— 11 : Fonctions thêta : Jacobi, Eisenstein, Hermite (1835–1850).

L'influence des fonctions elliptiques sur les courbes elliptiques se situe notamment dans la forme de Weierstrass qui paramétrise les courbes elliptiques et sous une forme réduite de leurs équations particulièrement efficace :

$$y^2 = x^3 + Ux + V$$

Il en va de même pour l'importantissime *Loi d'addition sur les points d'une courbe elliptique* qui peut s'exprimer par une opération sur les fonctions elliptiques paramétrisantes (Koblitz 1984, p. 22).

6.6 Tate et les courbes elliptiques

Extrait de l'interview de John Tate à l'occasion de son prix Abel (Raussen et Skau 2010).
Don Zagier y est cité.

"*In the introduction of your delightful book "Rational points on elliptic curves" that you co-authored with your earlier PhD student Joseph Silverman, you say, citing Serge Lang, that it is possible to write endlessly on elliptic curves. Can you comment on why the theory of elliptic curves is so rich and how it interacts and make contact with so many different branches of mathematics?*

For one thing, they are very concrete objects. An elliptic curve is described by a cubic polynomial in two variables so they are very easy to experiment with. On the other hand, elliptic curves illustrate very deep notions. They are the first non-trivial examples of abelian varieties. An elliptic curve is an abelian variety of dimension one, so you can get into this more advanced subject very easily by thinking about elliptic curves. On the other hand, they are algebraic curves. They are curves of genus one, the first example of a curve which isn't birationally equivalent to a projective line. The analytic and algebraic relations which occur in the theory of elliptic curves and elliptic functions are beautiful and unbelievably fascinating. The modularity theorem stating that every elliptic curve over the rational field can be found in the Jacobian variety of the curve which parametrizes elliptic curves with level structure its conductor is mindboggling. By the way, by my count about one quarter of Abel's published work is devoted to elliptic functions.

Among the Abel-prize laureates so far, you are probably the one whose contributions would have been closest to Abel's own interests. Could we challenge you to make an historical sweep, to put Abel's work in some perspective and to compare it to your research? In modern parlance, Abel studied the multiplicationby-n map for elliptic equal parts, and studied the algebraic equations that arose. He also studied complex multiplication and showed that, in this case, it gave rise to a commutative Galois-group. These are very central concepts and observations, aren't they?

Yes, absolutely, yes. Well, there's no comparison between Abel's work and mine. I am in awe of what I know of it. His understanding of algebraic equations, and of elliptic integrals and the more general, abelian integrals, at that time in history is just amazing. Even more for a person so isolated. I guess he could read works of Legendre, and other great predecessors, but he went far beyond. I don't really know enough to say more. Abel was a great analyst and a great algebraist. His work contains the germs of many important modern developments.

Could you comment on how the concept of "good reduction" for an elliptic curve is so crucial, and how it arose?

If one has an equation with integer coefficients it is completely natural, at least since Gauss, to consider the equation mod p for a prime p, which is an equation over the finite field F_p with p elements. If the original equation is the equation of an elliptic curve E over the rational number field then the reduced equation may or may not define an elliptic curve over F_p. If it does, we say E has "good reduction at p". This happens for all but a finite set of "bad primes for E", those dividing the discriminant of E.

The Hasse Principle in the study of Diophantine equations says, roughly speaking: if an equation has a solution in p-adic numbers then it can be solved in the rational numbers. It does not hold in general. There is an example for this failure given by the Norwegian mathematician Ernst Selmer ...

Yes. The equation $3x^3 + 4y^3 + 5z^3 = 0$.

Exactly! The extent of the failure of the Hasse Principle for curves of genus 1 is quantified by the Shafarevich-Tate group. The so-called Selmer groups are related groups, which are known to be finite, but as far as we know the Shafarevich-Tate group is not known to be finite. It is only a conjecture that it is always finite. What is the status concerning this conjecture?

The conjecture that the Shafarevich group Sha is finite should be viewed as part of the conjecture of Birch and Swinnerton–Dyer. That conjecture, BSD for short, involves the L-function of the elliptic curve, which is a function of a complex variable s. Over the rational number field, $L(s)$ is known to be defined near $s = 1$, thanks to the modularity theorem of A. Wiles, R. Taylor, et al. If $L(s)$ either does not vanish or has a simple zero at $s = 1$, then Sha is finite and BSD is true, thanks to the joint work of B. Gross and D. Zagier on Heegner points, and the work of Kolyvagin on Euler systems. So, by three big results which are the work of many people, we know a very special circumstance in which Sha is finite. If $L(s)$ has a higher order zero at $s = 1$, we know nothing, even over the field of rational numbers. Over an imaginary quadratic field we know nothing, period.

Do you think that this group is finite?

Yes. I firmly believe the conjecture is correct. But who knows? The curves of higher rank, or whose L-functions have a higher order zero – BSD says the order of the zero is the rank of the curve – one knows nothing about.

What is the origin of the Tate Conjecture?

Early on I somehow had the idea that the special case about endomorphisms of abelian varieties over finite fields might be true. A bit later I realized that a generalization fit perfectly with the function field version of the Birch and Swinnerton–Dyer conjecture. Also it was true in various particular examples which I looked at, and gave a heuristic reason for the Sato–Tate distribution. So it seemed a reasonable conjecture.

In the arithmetic theory of elliptic curves, there have been major breakthroughs like the Mordell–Weil theorem, Faltings' proof of the Mordell conjecture, using the known reduction to a case of the Tate conjecture. Then we have Wiles' breakthrough proving the Shimura–Taniyama–Weil conjecture. Do you hope the next big breakthrough will come with the Birch and Swinnerton–Dyer conjecture? Or the Tate conjecture, maybe?

Who knows what the next big breakthrough will be, but certainly the Birch and Swinnerton–Dyer conjecture is a big challenge, and also the modularity, i.e. the Shimura– Taniyama–Weil idea, which is now seen as part of the Langlands program. If the number field is not totally real we don't know much about either of these problems. There has been great progress in the last thirty years, but it is just the very beginning. Proving these things for all number fields and for all orders of vanishing, to say nothing of doing it for abelian varieties of higher dimension, will require much deeper insight than we have now.

Is there any particular work from your hand that you are most proud of, that you think is your most important contribution?

I don't feel that any one of my results stands out as most important. I certainly enjoyed working out the proofs in my thesis. I enjoyed very much proving a very special case of the so-called Tate conjecture, the result about endomorphisms of abelian varieties over finite fields. It was great to be able to prove at least one non-trivial case and not have only a conjecture! That's a case that is useful in cryptography, especially elliptic curves over finite fields. Over number fields, even finitely generated fields, that case of my conjecture was proved by Faltings, building on work of Zarhin over function fields, as the first step in his proof of the Mordell conjecture. I enjoyed very much the paper which I dedicated to Jean-Pierre Serre on the K_2 groups of number fields. I also had fun with a paper on residues of differentials on curves giving a new definition of residue and a new proof that the sum of the residues is zero, even though I failed to see a more important aspect of the construction."

6.7 Points d'ordre fini

6.7.1 Intersection d'une cubique et d'une droite

Si $P \neq Q$ sont rationnels sur C, alors la droite PQ possède une équation rationnelle et l'intersection $C \cap PQ$ donne lieu à un polynôme rationnel du troisième degré. Comme deux racines sont rationnelles, la troisième l'est aussi.

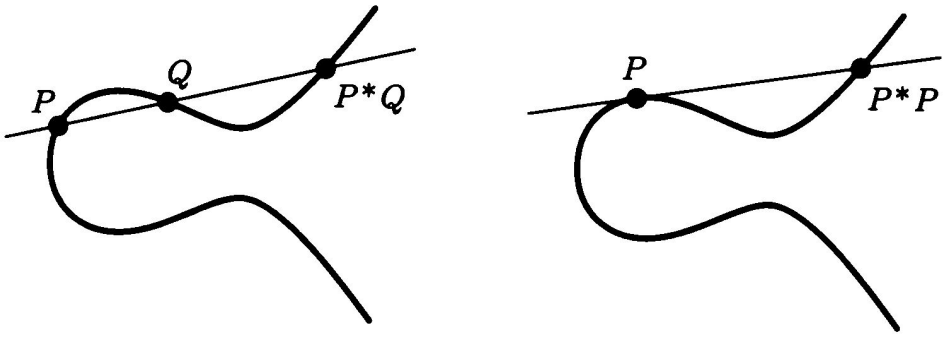


FIGURE 6.2 – Composition de points sur une cubique

Donc PQ recoupe C en un "troisième" point rationnel que nous notons $P * Q$ qui pourrait bien entendu être P ou Q.

Si nous disposons d'un seul point rationnel P sur C , nous pouvons en général, en trouver un deuxième. En dessinant la tangente à C en P, nous traçons essentiellement la droite par P et P ; Elle recoupe C en un point $P * P$ qui est rationnel. Il arrive que $P * P = P$, auquel cas nous disons que P est un point d'inflexion.

Donc si nous débutons avec quelques points rationnels, nous en obtenons généralement beaucoup d'autres par les constructions ci-dessus.

Nous pouvons faire bien mieux. A cet effet, nous examinons d'abord l'intersection de deux cubiques.

6.7.2 Intersection de deux cubiques C_1 et C_2

En général, deux courbes cubiques se coupent en neuf points.

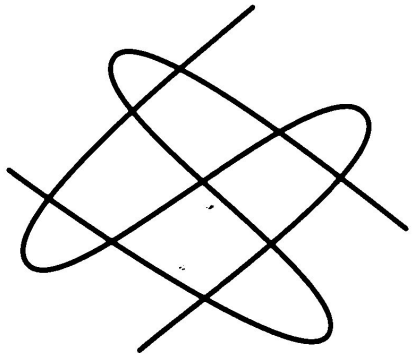


FIGURE 6.3 – Intersection de deux cubiques

Nous ne ferons pas une démonstration qui est cependant délicate. Il faut se situer dans le plan projectif

où C_1 et C_2 pourraient se couper en un ou plusieurs points à l'infini. En outre, il faut introduire des multiplicités d'intersection en comptant notamment l'intersection de C avec la tangente en P comme une multiplicité double.

Enfin, il faut tenir compte de points d'intersection à coordonnées complexes.

De manière générale, une courbe de degré m et une courbe de degre n, sans composante commune, ont exactement mn points communs, compte tenu des contraintes que nous venons d'exposer. Il s'agit du théorème de Bézout. Il fallut plus d'un siècle pour disposer d'une démonstration rigoureuse par Georges-Henri Halphen en 1873 (Bix 1998, p. 230).

6.7.3 Cubiques par huit points

Dès lors, il est possible de démontrer rapidement qu'une cubique C passant par huit des neuf points d'intersection de C_1 et C_2 passe nécessairement par le neuvième (Silverman et Tate 1992, p. 17).

6.7.4 Pas de méthode pour trouver un seul point rationnel

Silverman et Tate signalent en passant qu'une méthode pour déterminer en un nombre fini de pas si une cubique rationnelle possède un point rationnel est inconnue. Cette question très importante demeure ouverte.

6.7.5 Addition sur C

Supposons que C possède un point rationnel $\mathcal{O}$. Il est tout à fait remarquable que C possède une loi de groupe commutatif (notée $+$) dont $\mathcal{O}$ est le neutre.

La construction est simple : pour additionner P et Q, considérons le point $P * Q$, puis la droite qui joint $P * Q$ et $\mathcal{O}$ et $P + Q$ est le troisième point sur C de cette droite.

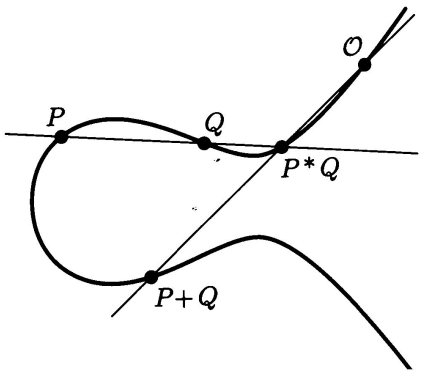


Figure 6.4 – Addition de deux points sur une cubique

Ainsi $P + Q = (P * Q) * \mathcal{O}$.

Il est clair que $\mathcal{O}$ est neutre.

Il est clair que $+$ est commutative du fait que $P * Q = Q * P$.

6.7.6 Le symétrique de P

Comment trouver le point Q, si l'on connaît P et $P + Q$? La droite $(P + Q)\mathcal{O}$ coupe C en $P * Q$ et donc $\mathcal{O} * (P + Q) = P * Q$ et

$$Q = P * (\mathcal{O} * (P + Q)). \tag{6.2}$$

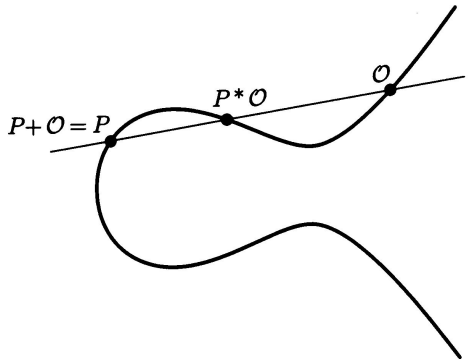


FIGURE 6.5 – $\mathcal{O}$ est neutre

Remplaçons maintenant Q par $-P$ dans l'équation 6.2. On obtient

$$-P = P * (\mathcal{O} * (P + (-P))) = P * (\mathcal{O} * \mathcal{O})$$

6.7.7 Addition associative : $(P + Q) * R = P * (Q + R)$

Il peut surprendre que + soit associative, mais c'est vrai !

Pour montrer que $(P + Q) + R = P + (Q + R)$, il suffit de montrer que que $(P + Q) * R = P * (Q + R)$ (voir la figure 6.6).

Nous allons faire une preuve par le dessin (voir la figure 6.6), qui n'est bien évidemment pas rigoureuse.

Considérons la droite en pointillés passant par les points $(P + Q)$ et R et la droite en trait plein passant par les points P et $Q + R$. Leur intersection appartient-elle à la cubique. Si c'est le cas, nous aurons prouvé que $(P + Q) * R = P * (Q + R)$.

Nous avons neuf points : $\mathcal{O}, P, Q, R, P * Q, P + Q, Q * R, Q + R$, et le point d'intersection des deux droites mentionnées ci-dessus.

Construisons deux cubiques dégénérées en trois droites et qui contiennent ces neuf points.

— C_1 réunion des trois droites en pointillés de la figure 6.6 : les droites PQ, $\mathcal{O}(Q * R)$ et $(P + Q)R$.

— C_2 réunion des trois droites en traits pleins de la figure 6.6 : les droites QR, $\mathcal{O}(P * Q)$ et $P(Q + R)$.

Les cubiques C_1 et C_2 ont pour intersection les neufs points mentionnés ci-dessus.

La cubique C passe par huit de ces points. Elle passe donc par le neuvième point (section 6.7.3). Donc l'intersection des deux droites est un point de la conique C, ce qui prouve que $(P + Q) * R = P * (Q + R)$.

Nous avons « prouvé » que C possède une loi de groupe commutatif (notée +) dont $\mathcal{O}$ est le neutre.

6.7.8 Changement de neutre

Soit C une cubique elliptique, $\mathcal{O}$ un de ses points, $\mathcal{O}'$ son tangentiel et + l'addition que nous venons d'examiner. Alors $C, +$ est un groupe abélien de neutre $\mathcal{O}$. Il vient :

Théorème 6. *Si P, Q, R sont des points non forcément distincts de C,*
P, Q, R sont alignés si et seulement si $P + Q + R = \mathcal{O}'$.

Démonstration. Il suffit d'appliquer les définitions. □

Tour point P de C détermine une transformation d'ordre 2 dite involution σ_P telle que pour tout $Q \in C$, $\sigma_P(Q), Q, P$ sont alignés.

Théorème 7. $\sigma_P(Q) = -Q - P + \mathcal{O}'$.

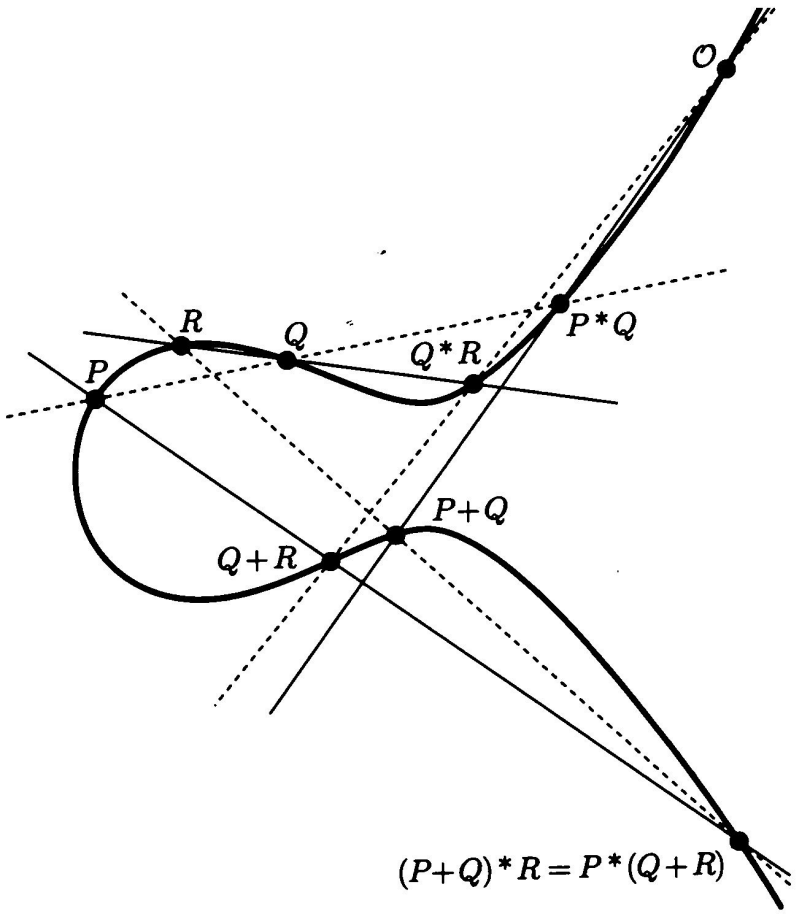


FIGURE 6.6 – Vérifier l'associativité : preuve par le dessin

Démonstration. Immédiat en appliquant le théorème 6. □

Abordons un changement d'origine.
Soient $\mathcal{O}_1$ et $\mathcal{O}_2$ deux origines accompagnées d'additions $+_1$ et $+_2$.

Ecrivons la symétrie σ_P déterminée par P, en liaison avec $+_1$ et $+_2$. Il vient

$$-_1 X -_1 P +_1 \mathcal{O}'_1 = -_2 X -_2 P +_2 \mathcal{O}'_2$$

pour tout $X \in C$.

En changeant de membre et donc de signe,

$$X +_2 P -_2 \mathcal{O}'_2 = X +_1 P -_1 \mathcal{O}'_1$$

Dès lors

$$X +_2 P = X +_1 P +_1 \text{constante}$$

De ce fait, les deux groupes $C, +_1$ et $C, +_2$ sont isomorphes.

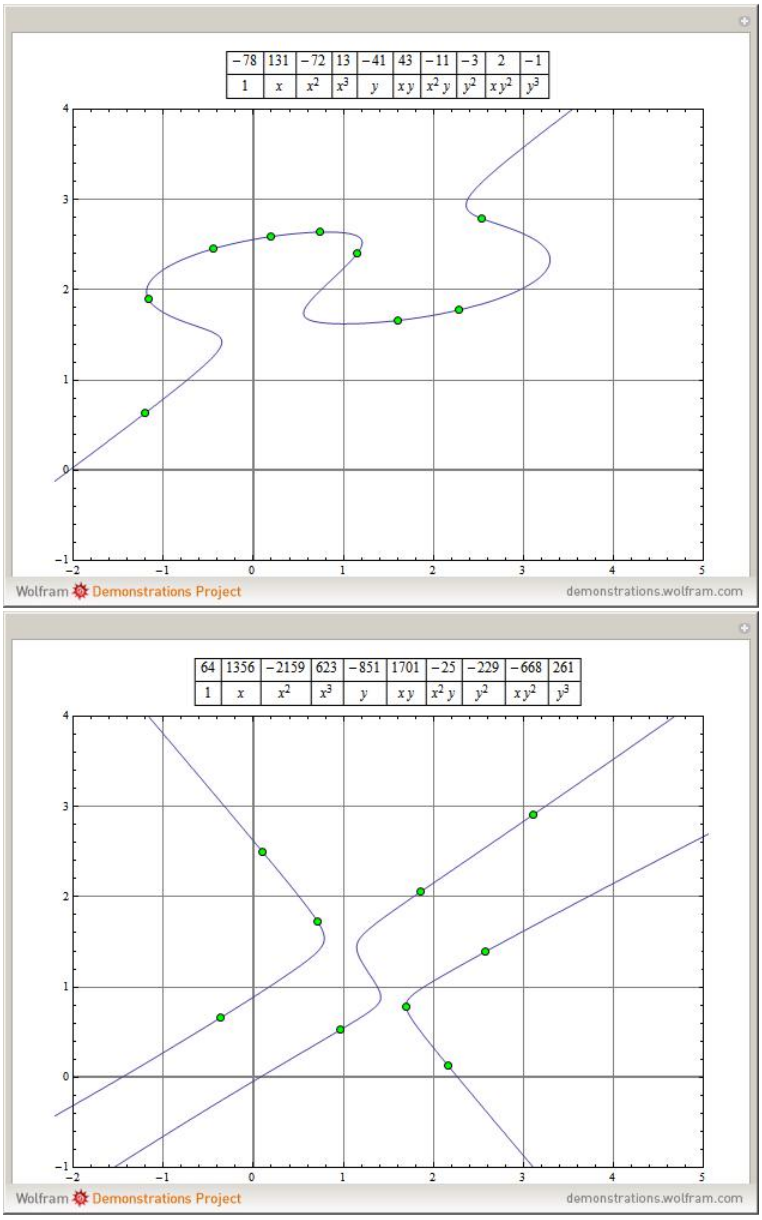
Théorème 8. *La loi de groupe abélien de C est indépendante du choix d'une origine $\mathcal{O} \in C$.*

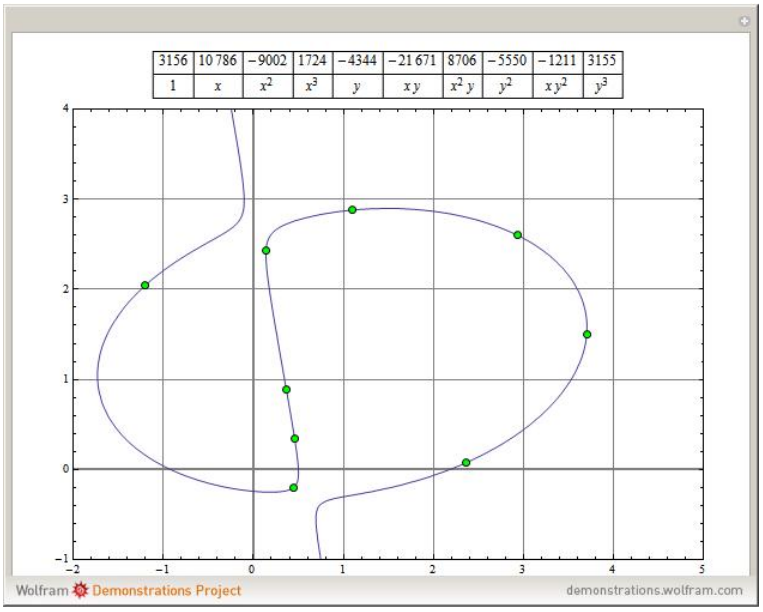
6.7.9 De neuf points à une cubique

Il existe une animation interactive qui dessine une cubique passant par neuf points WOLFRAM (2014). *Nine-Point Cubic*. Wolfram Demonstrations Project. URL : `http://demonstrations.wolfram.com/`

`NinePointCubic/` (visité le 11/04/2014) :

"This Demonstration plots a cubic equation of the form in the Cartesian plane to pass through any nine points. These cubic equations are often called elliptic curves. In this Demonstration, drag the points to see some of the many possible behaviors for a cubic equation. The coefficient values are rounded in the header, and should not be trusted when all values are low or zero. For some degenerate point configurations, such as the points marking the vertices and two points per side of a triangle, the matrix method used here may not work. A full method would employ special processing for degenerate lines and conics."





6.7.10 Formules explicites pour la loi de groupe

Dans cette section, nous travaillons sous l'hypothèse $\mathcal{O}$ = point d'inflexion. Cette hypothèse est toujours réalisée sur le corps des réels. Elle n'est pas toujours réalisée sur le corps des rationnels ou sur un corps fini. Alors C peut prendre la forme de Weierstrass

$$y^2 = ax^3 + bx^2 + cx + d \tag{6.3}$$

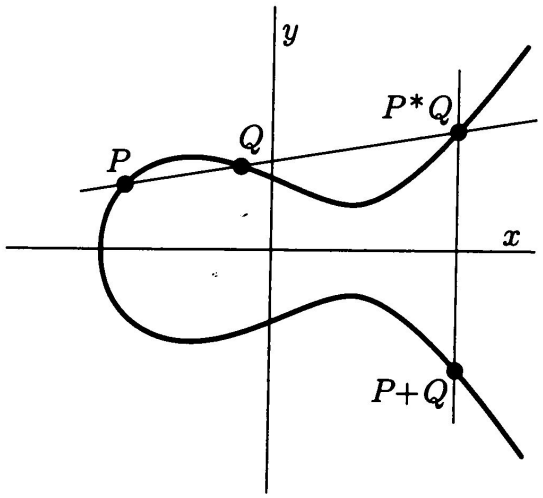


FIGURE 6.7 – Addition sur une cubique sous la forme de Weierstrass

Partons de

$$P = (x_1, y_1)$$
$$Q = (x_2, y_2)$$

Nous cherchons

$$P * Q = (x_3, y_3)$$
$$P + Q = (x_3, -y_3)$$

Alors PQ

$$\frac{y - y_1}{y_2 - y_1} = \frac{x - x_1}{x_2 - x_1} \tag{6.4}$$

Nous obtenons alors les expressions explicites

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2$$
$$y_3 = \frac{y_2 - y_1}{x_2 - x_1} x_3 + y_1 - \frac{y_2 - y_1}{x_2 - x_1} x_1$$

C'est la manière la plus efficace de calculer la somme de deux points distincts. Lorsqu'on veut calculer $2P = P + P$, il faut se servir de la tangente en P à la cubique C, dont le coefficient angulaire est égal à

$$\frac{f'(x)}{2y}.$$

Pour un point $P = (x, y)$, la formule explicite de la coordonnée en x de $2P$, appelée formule de duplication est :

$$x_{2P} = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

Sur base des outils que nous venons de mettre en place, il est possible de faire le calcul requis en vue de prouver l'associativité. Nous n'avons pas accompli ce calcul.

6.7.11 Exemples de somme de deux points (Lozano-Robledo 2011)

Nous reprenons des exemples tirés du livre de Lozano-Robledo 2011 :

Soit E la courbe elliptique $y^2 = x^3 - 25x$. Les points $P = (2, 5)$ et $Q = (-4, 6)$ appartiennent à $E(\mathbb{Q})$. Nous cherchons $P + Q$. Commençons par trouver l'équation de la droite PQ. La pente doit être

$$m = \frac{0 - 6}{5 - (-4)} = -\frac{6}{9} = -\frac{2}{3}$$

et l'équation est $y = -\frac{2}{3}(x - 5)$.

Pour trouver le troisième point d'intersection de cette droite avec la courbe elliptique, nous résolvons le système

$$\begin{cases} y & = -\frac{2}{3}(x - 5) \\ y^2 & = x^3 - 25x \end{cases}$$

Nous obtenons alors l'équation

$$x^3 - \frac{4}{9}x^2 - \frac{185}{9}x - \frac{100}{9} = 0$$

qui se factorise en $(x - 5)(x + 4)(9x + 5) = 0$. Le troisième point d'intersection de la droite PQ est $R = (-\frac{5}{9}, \frac{100}{27})$. Le point $P + Q$ et le symétrique de R par rapport à l'axe x. Donc $P + Q = (-\frac{5}{9}, -\frac{100}{27})$.

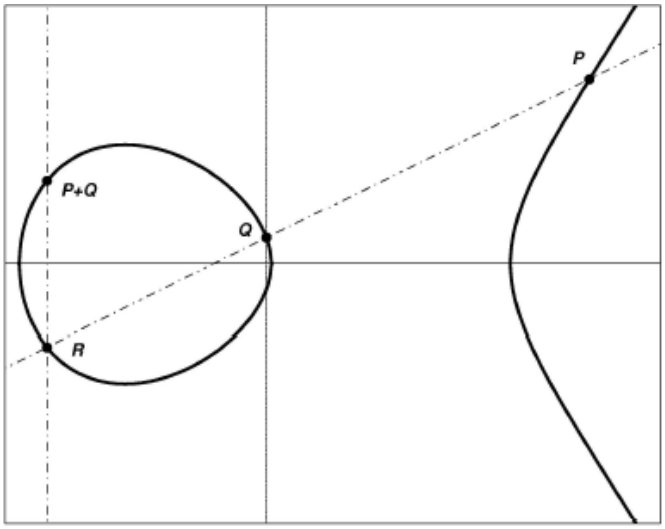


FIGURE 6.8 – Addition de points sur une courbe elliptique

Cherchons à présent $Q + Q = 2Q$. Cette fois, nous utilisons la tangente à E en Q. On trouve la pente de la tangente en dérivant implicitement $y^2 = x^3 - 25x$:

$$2y\frac{dy}{dx} = 3x^2 - 25, \text{ donc } \frac{dy}{dx} = \frac{3x^2 - 25}{2y}.$$

La pente de la tangente est $m = \frac{23}{12}$ et son équation $y = \frac{23}{12}(x + 4) + 6$.

Nous obtenons l'équation $x^3 - \frac{529}{144}x^2 - \frac{1393}{18}x - \frac{1681}{9} = 0$ qui se factorise en

$$(x + 4)^2(144x - 1681) = 0$$

La tangente coupe E en un point $R = (\frac{1681}{144}, \frac{62279}{1728})$, et donc

$$Q + Q = 2Q = (\frac{1681}{144}, -\frac{62279}{1728})$$

6.7.12 Points d'ordre fini chez SILVERMAN et TATE

Nous citons ici un extrait du chapitre 2 du livre de Silverman–Tate pour introduire les points d'ordre fini (SILVERMAN et TATE 1992, ch. 2) :

« Un élément P d'un groupe additif de neutre $\mathcal{O}$ est dit d'*ordre* m si

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ termes}} = \mathcal{O},$$

avec $m'P \neq \mathcal{O}$ pour tous les entiers $1 \leq m' \leq m$. Si un tel m existe, alors P est d'ordre fini ; sinon il est d'*ordre infini*. Nous commençons notre étude des points d'ordre fini sur des courbes cubiques en considérant des points d'ordre deux et d'ordre trois. Comme d'habitude, nous supposons que notre courbe cubique non singulière est donnée par une équation de Weierstrass

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

et que le point à l'infini $\mathcal{O}$ est l'élément neutre pour l'addition.

Quels sont les points dans notre groupe tels que $2P = \mathcal{O}$, mais $P \neq \mathcal{O}$? Au lieu de $2P = \mathcal{O}$, il est plus facile de considérer la condition $P = -P$. Comme $-(x, y)$ est juste $(x, -y)$, ce sont les points avec $y = 0$:

$$P_1 = (\alpha_1, 0), P_2 = (\alpha_2, 0), P_3 = (\alpha_3, 0)$$

où α_1, α_2 et α_3 sont les racines du polynôme cubique $f(x)$. Si nous autorisons les coordonnées complexes, alors il y a exactement trois points d'ordre deux, parce que la non-singularité de courbe garantit que $f(x)$ a trois racines distinctes.

Si nous prenons tous les points qui satisfont $2P = \mathcal{O}$ ainsi que $P = \mathcal{O}$, nous obtenons l'ensemble $\{\mathcal{O}, P_1, P_2, P_3\}$. On voit aisément que dans tout groupe abélien, l'ensemble des solutions de $2P = \mathcal{O}$ forme un sous-groupe. C'est un groupe d'ordre quatre dont chaque élément est d'ordre un ou deux. Il est évident que ce groupe est le produit direct de deux groupes d'ordre deux. Cela signifie que la somme de deux quelconques des points P_1, P_2, P_3 doit être égale au troisième, ce qui est évident du fait que les trois points sont colinéaires. Maintenant nous savons exactement à que ressemble le groupe des points tels que $2P = \mathcal{O}$: Si nous autorisons les coordonnées complexes, alors c'est le groupe d'ordre quatre, si nous nous restreignons aux coordonnées réelles, c'est soit le groupe d'ordre quatre, soit le groupe cyclique d'ordre deux, selon que $f(x)$ a trois ou une racine réelle, si nous nous restreignons aux coordonnées rationnelles, c'est soit le groupe d'ordre quatre, soit le groupe cyclique d'ordre deux, soit le groupe trivial, selon que $f(x)$ a trois, une ou zéro racines rationnelles. »

6.7.13 Exemples de points d'ordre fini (Lozano-Robledo 2011)

Soit $E : y^2 = x^3 + 1$ et $P = (2, 3)$. Nous cherchons la suite des points $P, 2P, 3P$, etc.

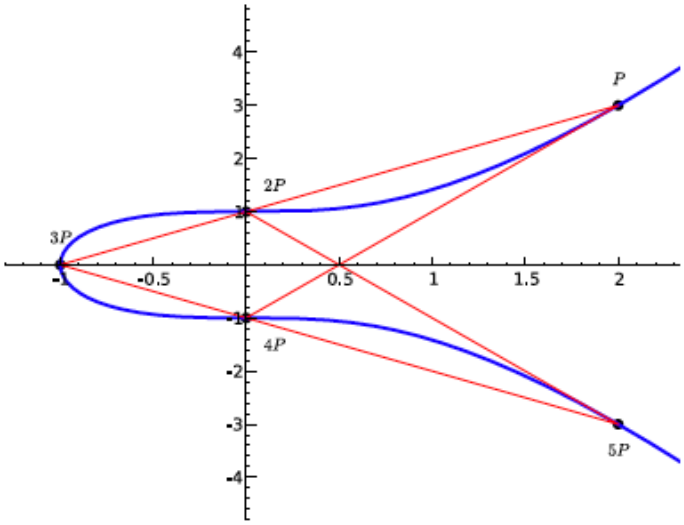


FIGURE 6.9 – les points rationnels sur $y^2 = x^3 + 1$, à l'exception du point à l'infini.

— Pour trouver $2P$, il faut d'abord trouver la tangente à E en P, qui a pour équation $y - 3 = 2(x - 2)$ ou y=2x-1. Le troisième point d'intersection est $R = (0, -1)$, donc $2P = (0, 1)$.
— Pour trouver $3P$, nous faisons la somme de P et de $2P$. Le troisième point d'intersection avec la droite qui joint P à $2P$ est $R' = (-1, 0)$ et donc $3P = (-1, 0)$.
— Le point $4P$ s'obtient en additionnant $3P$ à P. Le troisième point d'intersection de E avec la droite joignant P et $3P$ est $R'' = 2P = (0, 1)$ et donc $4P = P + 3P = (0, -1)$.
— Le point $5P$ s'obtient en additionnant $4P$ à P. Le troisième point d'intersection de E avec la droite joignant P et $4P$ est P et donc $5P = 4P + P = (2, 3)$.

— Pour finir, $6P = 5P + P$, mais $5P = (2, -3) = -P$, donc $6P = P + (-P) = \mathcal{O}$, le point à l'infini. Le point P est donc un point d'ordre fini et son ordre est égal à 6.

La courbe $E_n : y^2 = x^3 - n^2x = x(x - n)(x + n)$ a trois points rationnels : $P = (0, 0)$, $Q = (-n, 0)$, $T = (n, 0)$ qui sont chacun d'ordre deux, c'est-à-dire $2P = 2Q = 2T = \mathcal{O}$ et $P + Q = T$.

$$\{\mathcal{O}, P, Q, T\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$$

On peut voir dans le tableau qui suit des exemples de sous-groupes de torsion sur $\mathbb{Q}$

Courbe $E(\mathbb{Q})$	Groupe de torsion	générateurs
$y^2 = x^3 - 2$	trivial	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(2, 0)$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 1)$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, 3)$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$(-2, 10)$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(3, 1)$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$(0, 9)$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 212)$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(2, 0), (0, 0)$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(3, 6), (0, 0)$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(-3, 18), (2, -2)$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(30, -90), (-40, 400)$

6.7.14 Théorème de Nagell-Lutz

Ce théorème a été démontré indépendamment par le norvégien Trygve Nagell en 1935 et la Française Élisabeth Lutz en 1937.

Voici quelques informations biographiques concernant Trygve Nagell et Elisabeth Lutz

Trygve Nagell (Wikipedia 2011g)

Trygve Nagell (1895 – 1988) was a Norwegian mathematician, known for his works on the Diophantine equations within number theory. He received his doctorate at the University of Oslo in 1926, and lectured at the University until 1931. He was a professor at the University of Uppsala from 1931 to 1962. Nagell was appointed Commander of the Royal Norwegian Order of St. Olav in 1951, and of the Swedish Order of the Polar Star in 1952.

Elisabeth Lutz (Wikipedia 2011e)

Élisabeth Lutz est une mathématicienne française, née le 14 mai 1914 à Thann (Haut-Rhin) et morte le 31 juillet 2008 à Grenoble (Isère).

Elle a fait ses études secondaires à Colmar et ses études supérieures à Strasbourg. Elle a enseigné dans un collège à Poligny puis à Sarrebourg et Besançon.

Elle a soutenu sa thèse en 1951 sous la direction de Claude Chabauty et a été recrutée en 1953 à l'université comme maître de conférences, professeur sans chaire (1957), et professeur titulaire à titre personnel en 1960. E. Lutz a pris sa retraite en 1979 et s'est alors intéressée plus spécialement au patrimoine du Dauphiné.

Sa réputation internationale tient à son tout premier théorème obtenu dans son diplôme d'études supérieures soutenu en 1936 suivant un sujet donné par André Weil.

Sa thèse d'État, dirigée par C. Chabauty, concerne les approximations diophantiennes linéaires p-adiques : on se donne un système de p formes linéaires p-adiques avec n variables. Il s'agit de voir si des inégalités sur le maximum des valeurs absolues du système peuvent être vérifiées dans des boules définies à l'avance.

Elisabeth Lutz a été responsable de la licence de mathématiques de 1967 à sa retraite. À partir de 1960, Elisabeth Lutz a mis sur pied le système des échanges internationaux de la revue des Annales de l'Institut Fourier. Elle a rédigé un dizaine de séminaires en théorie des nombres et géométrie.

Le théorème de Nagell-Lutz chez Silverman et Tate 1992, ch. 2 :
"Our goal in this chapter is to prove a theorem, first proved by Nagell and Lutz, which tells us how to find all of the rational points of finite order. Their theorem says a rational point of finite order (x, y) must have integer coordinates, and either $y = 0$ (for points of order two) or else $y|D$, where D is the discriminant of the polynomial $f(x)$. In particular, a cubic curve has only a finite number of rational points of finite order.

The *discriminant* of $f(x)$ is the quantity

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

You may be familiar with this when $a = 0$, in which case $D = -4b^3 - 27c^2$. If we factor f over the complex numbers,

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

then one can check that

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2;$$

and so the non-vanishing of D tells us that the roots are distinct. Thus the question of finding the rational points of finite order can be settled in a finite number of steps. You take the integer D, and consider each of the finitely many integers y with $y|D$. You take all those values of y and subsitute them in the equation $y^2 = f(x)$. The polynomial $f(x)$ has integer coefficients and leading coefficient 1. If it has an integer root, that root will divide the constant term. Thus, there are a finite number of things to check, and in this way we will be sure to find all the points of finite order in a finite number of steps."

Théorème 9 (Théorème de Nagell-Lutz)**.** *Let*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c; and let D be the discriminant of the cubic polynomial f(x),

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers; and either $y = 0$, in which case P has order two, or else y devides D.

6.7.15 Le théorème de Mazur (1977)

Nous citons le livre de Silverman et Tate 1992, chap. 2, p. 57 :
"Many people worked on the problem of determining just which orders are possible, culminating in a very beautiful and very difficult theorem of Mazur."

Voici une notice biographique de Barry Mazur :

Barry Mazur (Wikipedia 2011a)

Barry Charles Mazur (born December 19, 1937) is a professor of mathematics at Harvard.

Born in New York City, Mazur attended the Bronx High School of Science and MIT, although he did not graduate from the latter on account of failing a then-present ROTC requirement. Regardless, he was accepted for graduate school and received his Ph.D. from Princeton University in 1959, becoming

a Junior Fellow at Harvard from 1961 to 1964. He is currently the Gerhard Gade University Professor and a Senior Fellow at Harvard. In 1982 he was elected a member of the National Academy of Sciences. Mazur has received the Veblen Prize in geometry, the Cole Prize in number theory, the Chauvenet Prize for exposition, and the Steele Prize for seminal contribution to research from the American Mathematical Society.

Théorème 10 (Théorème de Mazur)**.** *Let C be a non-singular rational cubic curve, and suppose that $C(\mathbb{Q})$ contains a point of finite order m. Then either*

$$1 \leq m \leq 10 \text{ or } m = 12.$$

More precisely, the set of all points of finite order in $C(\mathbb{Q})$ form a subgroup which has one of the following two forms :

(i) A cyclic group of order N with $1 \leq N \leq 10$ or $N = 12$.

(ii) The product of a cyclic group of order two and a cyclic group of order $2N$ with $1 \leq N \leq 4$.

Nous nous demandons si tous ces cas se réalisent.

Grâce à Zagier dans les Notices 1989, nous apprenons que les quinze cas se présentent effectivement et infiniment souvent.

6.8 Forme de Weierstrass

6.8.1 Forme de Weierstrass : notre version

Cubique générale dans $P_2(K)$

$$ax^3 + by^3 + cz^3 + dx^2y + exy^2 + fy^2z + gyz^2 + hx^2z + ixz^2 + kxyz = 0$$

— C passe par le point $O_1 = [1, 0, 0]$ ssi $a = 0$.
— C passe par le point $O_2 = [1, 0, 0]$ ssi $b = 0$.
— La droite $z = 0$ est tangente d'inflexion en O_2 ssi

$$ax^3 + dx^2y + exy^2 + by^3$$

se réduit à
ax^3
donc ssi

$$d = e = b = 0$$

Conique polaire de O_2

$$C_{O_2} \frac{\partial f}{\partial y} = 0$$

$$2fyz + gz^2 + kxz = 0$$

$$z(\underbrace{2fy + gz + kx}_{\text{droite } C_{O_1}}) = 0$$

Celle-ci se transforme projectivement en $y = 0$ (si $f = 0$ singularité) ce qui se ramène à

$$g = k = 0$$

Il vient

$$ax^3 + cz^4 + fy^2z + hx^2z + ixz^2 = 0, f \neq 0 \Rightarrow$$

$$y^2 = ax^3 + bx^2 + cx + d, a \neq 0$$

forme de Weierstrass avec axe de symétrie.

Tentons de simplifier davantage en effectuant la transformation linéaire

$$x \to x + \beta$$

Il vient

$$a(x+\beta)^3 + b(x+\beta)^2 + c(x+\beta) + d$$

terme an x^2

$$za\beta + b$$

s'annule par $\beta = \frac{-b}{3a}$

Ceci ramène C à

$$y^2 = ax^3 + cx + d$$

forme de Weierstrass.

Que faire si la cubique ne possède pas de point d'inflexion ? Supposons qu'il existe un point $p \in C$. Dans ce cas, le tangentiel $T(p)$ de p est un point de C distinct de p. Le tangentiel $T^2(p)$ de $T(p)$ est un troisième point sur C. Deux cas se présentent alors selon que $T^3(p)$ est égal à p ou $T^3(p)$ est distinct. Chacun de ces cas conduit à une réduction de l'équation de C après un choix judicieux du repère projectif. Nous laissons ce travail comme exercice au lecteur.

6.8.2 Forme de Weiertrass : Tate

Tate restreint l'attention à des cubiques données selon la forme de Weierstrass qui consiste classiquement en des équations comme

$$y^2 = 4x^3 - g_2x - g_3 \tag{6.5}$$

Il considère aussi la forme

$$y^2 = x^3 + ax^2 + bx + c \tag{6.6}$$

et l'appelle également forme de Weierstrass (Silverman et Tate 1992, p. 22).

Tate montre que toute cubique se ramène birationnellement à la forme de Weierstrass, ce que nous n'entrepenons pas ici.

La courbe (6.5) ou (6.6) est elliptique ssi l'équation $4x^3 - g_2x - g_3 = 0$ (ou $x^3 + ax^2 + bx + c = 0$) n'a pas de racine double.

S'il y a une racine double (voire triple), elle livre un point double de la courbe et celle-ci est rationnelle. Une cubique rationelle se traite aussi simplement qu'une conique.

Montrons sur un exemple qu'une cubique ayant un point double peut se paramétrer par des fonctions rationnelles. Adoptons $C : y^2 = x^2 + x^3$ (Fig. 6.10)

L'origine est un point double de C. Pour paramétrer, partons d'une droite $y = \lambda x$. L'unique point d'intersection en dehors de l'origine est livré par

$$\lambda^2 = x^2 + x^3$$

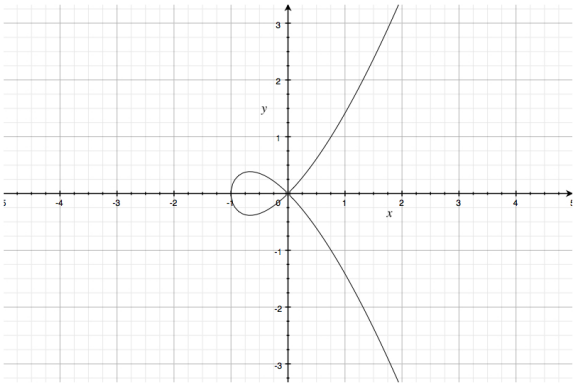


FIGURE 6.10 – Cubique à point double $C : y^2 = x^2 + x^3$

donc

$$\begin{cases} x &= \lambda^2 - 1 \\ y &= \lambda(\lambda^2 - 1) \end{cases}$$

Pour $\lambda = \infty$ on trouve le point à l'infini de C qui est donné par

$$\begin{cases} y^2 z &= x^2 z + x^3 \\ z &= 0 \end{cases}$$

donc c'est $[0, 1, 0]$.
Ceci était l'exemple promis.

Si on évite les singularités, la courbe elliptique est équipée d'une loi de groupe liée au choix d'un point qui sera l'élément neutre.

Loi de groupe pour cubique elliptique sous forme de Weierstrass munie de son point à l'infini (SILVERMAN et TATE 1992, p. 28).
Facile.
La preuve d'associativité est incomplète. Voir les calculs requis à la section 6.7.10

Dans la théorie des fonctions elliptiques de Weierstrass (SILVERMAN et TATE 1992, p. 43), on montre que dès qu'il y a deux racines complexes g_2, g_3 telles que le polynôme $4x^3 - g_2 x - g_3$ a deux racines distinctes (c'est-à-dire tel que $g_2^3 - 27 g_3^2 \neq 0$), alors on peut trouver deux nombres complexes ω_1, ω_2 (appelés *périodes*) dans le plan complexe u en évaluant certaines intégrales définies. Ces périodes sont $\mathbb{R}$-linéairement indépendantes et on s'intéresse au groupe obtenu en prenant toutes leurs combinaisons $\mathbb{Z}$-linéaires :

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}.$$

(Un tel groupe est appelé un *treillis*.) Malgré qu'il y ait de nombreux choix pour les générateurs ω_1 et ω_2 de L, il s'avère que les coefficients g_2 et g_3 déterminent le groupe L de manière unique. Inversement, le groupe L détermine les coefficients g_2 et g_3 de manière unique via les formules

$$g_2 = 60 \sum_{\omega \in L,\, \omega \neq 0} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega \in L,\, \omega \neq 0} \frac{1}{\omega^6}.$$

On utilise les périodes pour définir une fonction $\mathcal{P}(u)$ par la série

$$\mathcal{P}(u) = \frac{1}{u^2} + \sum_{\omega \in L,\, \omega \neq 0} \left(\frac{1}{(u - \omega)^2)} - \frac{1}{\omega^2} \right).$$

Cette fonction méromorphe est appelée la *fonction $\mathcal{P}$ Weierstrass*. Elle a visiblement des pôles aux points de L et n'a pas d'autres pôles dans le plan complexe u.

Il est moins évident de voir qu'elle est doublement périodique, c'est-à-dire que $\mathcal{P}(u+\omega_1) = \mathcal{P}(u)$ et $\mathcal{P}(u+\omega_2) = \mathcal{P}(u)$ pour tous les nombres complexes u.

Il en découle que $\mathcal{P}(u+\omega) = \mathcal{P}(u)$ pour tout $u \in \mathbb{C}$ et pour tout $\omega \in L$. Remarquez la ressemblance avec les fonctions trigonométriques et exponentielles qui sont simplement périodiques : $f(u) = \sin(u)$ a la période 2π, et $f(u) = \exp(u)$ a la période $2\pi i$.

La fonction doublement périodique $\mathcal{P}(u)$ satisfait l'équation différentielle

$$(\mathcal{P}')^2 = 4\mathcal{P}^3 - g_2\mathcal{P} - g_3, \text{ avec } \mathcal{P}' = \frac{d\mathcal{P}}{du}$$

Donc à tout nombre complexe u correspond un point

$$P(u) = (\mathcal{P}(u), \mathcal{P}'(u))$$

sur la courbe donnée, en général un point avec des coordonnées complexes. Nous obtenons ainsi une application du plan complexe u sur $C(\mathbb{C})$. (Bien entendu, nous envoyons les points dans L, qui sont les pôles de $\mathcal{P}$ sur $\mathcal{O}$.)

Les faits concernant cette application sont les suivants. L'application est surjective sur la courbe ; chaque couple de nombres complexes (x, y) satisfaisant $y^2 = 4x^3 - g_2x - g_3$ provient d'un certain u. Comme $\mathcal{P}$ est doublement périodique, l'application ne peut pas être bijective. Si u et v ont la propriété que leur différence $u - v$ est égale à $m_1\omega_1 + m_2\omega_2$ pour certains entiers m_1, m_2 (c'est-à-dire si $u - v \in L$), alors $P(u) = P(v)$.

6.9 Le théorème de Mordell

Si E est une courbe elliptique définie sur $\mathbb{Q}$, le groupe de E est finiment engendré.

Ce résultat surprenant avait été conjecturé par Poincaré vers 1900 comme nous pouvons le lire dans l'article de Norbert Schappacher 2005a, p. 12 :

« Dans la mesure où Poincaré n'envisage point la situation où aucun nombre fini de points fondamentaux ne suffit à engendrer tous les points rationnels on peut voir dans ce texte une façon de conjecturer le théorème de la base finie des points rationnels, démontré dans Mordell 1922. Il est aussi possible que, étant intéressé par une analyse plutôt constructive des points rationnels, il ait exclu tout de suite le cas d'un rang infini. Comme Poincaré ne dispose ni d'un élément neutre ni de l'inverse dans sa structure, sa notion de rang n'est pas bien calibrée de notre point de vue. En fait, le rang n'est pas un invariant birationnel pour la raison triviale que, de deux cubiques équivalentes, une, mais pas l'autre, peut avoir un point rationnel d'inflexion.

⋮

La formulation du jeune André Weil : "Il y a quelques années, Mordell a démontré un théorème remarquable, qui avait été entrevu déjà par Poincaré." (Weil 1929) »

Une démonstration complète du théorème est présentée par Silverman et Tate dans les chapitres II et III de leur livre (Silverman et Tate 1992, p. 121).

Théorème 11 (Mordell's Theorem for Curves with a Rational Point of order Two)**.** *Let C be a non-singular cubic curve given by an equation*

$$C : y^2 = x^3 + ax^2 + bx,$$

where a and b are integers. Then the group of rational points $C(\mathbb{Q})$ is a finitely generated abelian group.

Le théorème de Mordell ne donne pas une méthode permettant de construire des générateurs (Silverman et Tate 1992, p. 88).

6.10 Le rang de E

Grâce au théorème de Mordell pour E sur Q, le groupe est donc finiment engendré. Il a donc un nombre fini de générateurs. Il est tentant de croire que le plus petit nombre de générateurs est appelé rang de E, mais le rang r de E se définit de manière un peu plus subtile, comme nous allons le voir.

En présence d'une équation explicite de courbe elliptique, la détermination du rang est difficile.

Existe-t-il un algorithme général, à savoir s'appliquant à toute courbe pour déterminer son rang ? La réponse doit être nuancée. Nous nous référons à la réponse de Dr Vogler sur le site *Ask Dr Math* (Vogler 2007) :

"There are algorithms for determining the rank of an elliptic curve. There are even programs available that do just that. One is *mwrank* (as in Mordell-Weil Rank) by John Cremona (Cremona 2013).

This uses the method of descent to determine the rank, but while it works just fine for most curves, it is known to fail for some curves, which probably disqualifies it from being called a "general algorithm." That is, it works better in practice than it does in theory. There are other algorithms that work better in theory but which have very long runtimes in the sense that you have to perform large numbers of computations, sometimes more than is feasible.

Cette question est un objet de compétitions en vue de trouver des courbes elliptiques de rang plus élévé. En 2000 le record était 24 établi par Martin - McMillen, `http://web.math.hr/~duje/tors/rk24.html`, en 2006, il était de 28 établi par Elkies, `http://web.math.hr/~duje/tors/rk28.html`, (Réf. Dujela Dujella p.d.).

Voir l'équation établie par Elkies (2006) ci-dessous :

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x \quad + \\ 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

Independent points of infinite order :

$P_1 = [-212415009125438107329213746 3, 259854492051899599030515511070780628911531]$
$P_2 = [233450986603470175688475453 7, 188720041954944691808683165528036279315 31]$
$P_3 = [-167173605406236906387903866 3, 251709377261144287808506947241319126049131]$
$P_4 = [213913026013915666649298213 7, 366395091714397292024214596929412975275 31]$
$P_5 = [153470676446712072388547733 7, 854295853460176942890210328627810727995 31]$
$P_6 = [-273107948787567703334157506 3, 262521815484332191641284072623902143387531]$
$P_7 = [277572626684457164970545853 7, 128457554740140602488694876990826403699 31]$
$P_8 = [149438572932718895754183381 7, 884866055277334059861164945140492334114 51]$
$P_9 = [186843822862088735850906525 7, 592374032144377087127251403930593585891 31]$
$P_{10} = [200894510882574377486654253 7, 476906778801255528821517507815414247115 31]$
$P_{11} = [234836054091802516965163293 7, 174929300062005578573403324764488043635 31]$
$P_{12} = [-14720840070904811744700086 63, 24664345065350371419994744154975979846913 1]$
$P_{13} = [29241286077080612133632889 37, 28350264431488878501488356474767375899531]$
$P_{14} = [53749938910660618932939345 37, 28618890842726338645117503191647989373153 1]$
$P_{15} = [17096907682333545233340085 57, 71898834974686089466159700529215980921631]$
$P_{16} = [24509540113535931440725951 87, 44452281735326343570492625506107147365 31]$
$P_{17} = [29692547092735591674646749 37, 32766893075366270801333682543160469687531]$
$P_{18} = [27119149349416926013328829 37, 20684366127783816986504139815065906135 31]$
$P_{19} = [20078586077996854528778328 937, 27796085411378066046560517256246240300915 31]$
$P_{20} = [21580824502407347743178106 97, 34994373401964026809969662241800901254731]$
$P_{21} = [20046454582470590224032249 37, 48049329780704645522439866999888475467531]$
$P_{22} = [29757494509479962649470913 37, 33398989826075322320208934410104857869131]$
$P_{23} = [-21024904676862851501473478 63, 25957639145987578957167739317168720322753 1]$
$P_{24} = [31158317991506303490219453 7, 16810438522998060354010947291566015347393 1]$
$P_{25} = [27739310083418652314437718 17, 12632162834649921002414116273769275813451]$
$P_{26} = [21565811881437684093634613 87, 35125092964022908897004150516375178087331]$
$P_{27} = [38663304998724125088156591 37, 12119775565594422629303692671502584732253 1]$
$P_{28} = [22308682897735760237786787 37, 28558760030597485663387020600768640028531]$

Citons Ireland et Rosen 1990, p. 335 qui se réfèrent à Zagier 1984

"In an important survey of Zagier, it is stated that Mestre also found examples of curves of rank as large as 14. Whether or not the rank is bounded for curves defined over rational numbers is unsolved, although A. Néron in his annotations of Poincaré's paper states, 'L'existence de cette borne est considérée comme probable.' However, Zagier mentions in the survey that it is conjectured that all values can occur."

Voici comment Silverman et Tate 1992, p. 89 introduisent la notion de rang :

"In this section we are going to illustrate Mordell's theorem by working out some numerical examples. First we discuss some consequences of what we have already proven. We have shown that the group Γ of rational points on the curve

$$C : y^2 = x^3 + ax^2 + bx$$

is a finitely generated abelian group. It follows from the fundamental theorem on abelian groups that Γ is isomorphic, as an abstract group, to a direct sum of infinite cyclic groups and finite cyclic groups of prime order (section 11.1).

We will let $\mathbb{Z}$ denote the additive group of integers, and we will let $\mathbb{Z}_m$ denote the cyclic group $\mathbb{Z}/m\mathbb{Z}$ of integers mod m. Then the structure theorem tells us that Γ looks like

$$\Gamma \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ times}} \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}.$$

More naively, this says that there are generators

$$P_1, \ldots, P_r, Q_1, \ldots, Q_s \in \Gamma$$

such that every P in Γ can be written in the form

$$P = n_1 P_1 + \cdots + n_r P_r + m_1 Q_1 + \cdots + m_s Q_s.$$

Here the integers n_i are uniquely determined by P, whereas the integers m_j are determined modulo $p_j^{\nu_j}$.

The integer r is called the *rank* of Γ (*** r est le nombre de composantes cycliques infinies et est appelé le *rang*). The group Γ will be finite If and only if it has rank $r = 0$. The subgroup

$$\mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}$$

corresponds to the elements of finite order in Γ; it has order $p_1^{\nu_1} p_2^{\nu_2} \ldots p_s^{\nu_s}$.

Of course, the points $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ are not unique. There are many possible choices of generators for Γ."

6.11 Hauteur et rang moyen d'une courbe elliptique P

Poonen 2001 nous donne l'intuition de ce qu'est la hauteur d'une courbe elliptique :
"One calls $h(P)$ the *(logarithmic) height* of P. Roughly, $h(P)$ is the width of a sheet of paper needed to write down P."

Nous citons ici Brunault 2012 à propos des travaux de Bhargava et Shankar :
« Puisque le rang d'une courbe elliptique est un invariant mystérieux et en général difficile à calculer, il est naturel d'essayer de décrire son comportement en moyenne, c'est-à-dire lorsque l'on prend une courbe elliptique "au hasard". Voici par exemple une question naturelle :

Étant donnée une courbe elliptique prise au hasard, quelle est la probabilité qu'elle possède un nombre infini de points rationnels ?

En d'autres termes, avec quelle fréquence le rang d'une courbe elliptique est-il au moins égal à 1 ? Puisque l'ensemble des courbes elliptiques est infini, il est nécessaire, pour donner un sens précis à cette question, d'ordonner les courbes elliptiques par « taille ». Sans rentrer dans les détails, la taille ou hauteur d'une courbe elliptique est donnée par la taille des coefficients de l'équation qui la définit [16]. La probabilité qu'une courbe elliptique soit de rang ≥ 1 se définit alors comme la limite (si elle existe) de la quantité

$$\frac{\text{Nombre de courbes elliptiques de hauteur } \leq X \text{ et de rang } \geq 1}{\text{Nombre de courbes elliptiques de hauteur } \leq X}$$

lorsque X tend vers l'infini. Le quotient ci-dessus a bien un sens puisqu'il n'y a qu'un nombre fini de courbes elliptiques de hauteur $\leq X$. De même, le rang moyen des courbes elliptiques est la limite (si elle existe), lorsque X tend vers l'infini, de la moyenne des rangs des courbes elliptiques de hauteur $\leq X$.

Depuis des travaux de Dorian Goldfeld en 1979 précisés par Nicholas M. Katz, Peter Sarnak puis Mark Watkins, il est conjecturé que le rang moyen des courbes elliptiques vaut 12 : plus précisément, on s'attend à ce qu'en moyenne, 50% des courbes elliptiques soient de rang zéro et 50% des courbes elliptiques soient de rang un (par suite, la proportion des courbes elliptiques de rang ≥ 2 devrait être négligeable). Jusqu'à présent, les seuls résultats connus sur le rang moyen des courbes elliptiques utilisaient l'hypothèse

de Riemann généralisée et la conjecture de Birch et Swinnerton-Dyer, des conjectures hors d'atteinte aujourd'hui. En supposant ces conjectures, Armand Brumer a montré en 1992 que le rang moyen est $\leq 2,3$. Ce résultat a ensuite été amélioré par Roger Heath-Brown en 2004, qui obtient la borne supérieure 2, puis par Matthew P. Young en 2006, qui obtient la borne supérieure 25/14.

En 2010, Manjul Bhargava et Arul Shankar établissent le résultat spectaculaire suivant :

Théorème 12 (Bhargava et Shankar 2010)**.** *Lorsque les courbes elliptiques sont ordonnées par hauteur, leur rang moyen est au plus égal à 1,5.*

»

6.12 Le groupe des coniques

En étudiant le groupe d'une cubique et en ayant un regard pour une conique, on se demande si celle-ci ne peut pas être aménagée en groupe elle aussi.

Une idée naturelle est de compléter la conique (ovale) Γ par une droite de son plan, et d'en faire ainsi une cubique. A première vue, aucune droite ne s'impose, mais en fait, il y en a une tout de même, c'est la droite à l'infini. Le cas le plus simple est celui du cercle complété par la droite à l'infini.

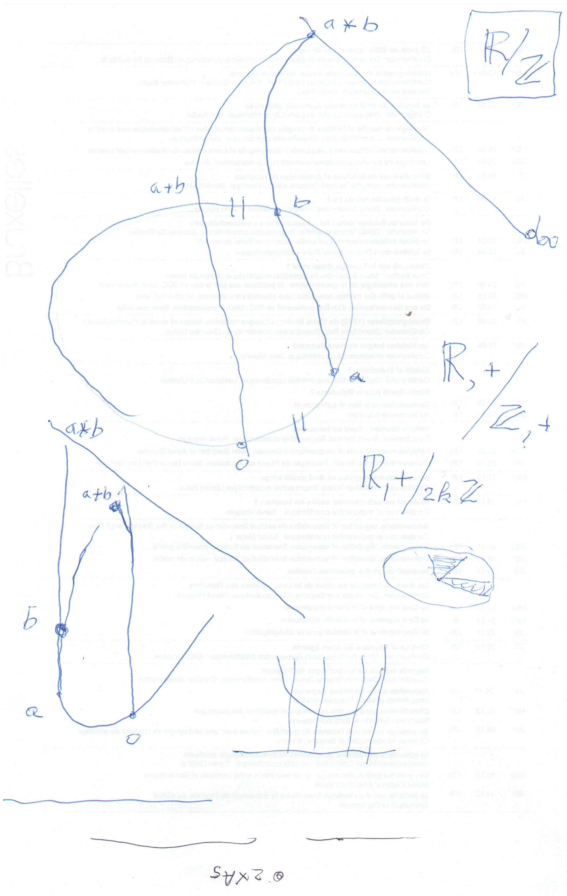


FIGURE 6.11 – Addition sur une conique complétée par la droite à l'infini

Tentons de répéter la construction sur une cubique (voir la section 6.7.5).

1. Fixons une origine O sur Γ.

2. Donnons deux points A et B de Γ.
3. La droite AB (ou la tangente en A, si $A = B$) coupe la droite à l'infini en un point $A * B$.
4. La droite par $A * B$ et O recoupe Γ en un point $A + B$.

Nous constatons sur le cercle que nous avons « redécouvert »le groupe des angles. La construction fonctionne bien évidemment pour toute ellipse.

Observons, à nouveau sur le cercle, que la somme n'est pas uniquement basée sur une addition d'arcs, mais sur une égalité de secteurs angulaires centrés à l'origine, donc sur la notion d'aire.

Comme l'aire est un invariant affin, cette considération s'étend aux ellipses. Elle a diverses applications, par exemple, dans les cadrans solaires, mais aussi dans le mouvement de rotation de la Terre autour du Soleil selon une ellipse.

La construction fonctionne pareillement sur une parabole et sur une hyperbole.

Exercice : vérifier que c'est bien un groupe de neutre O. Techniquement ce que l'on vient de dire relève de l'enseignement secondaire.

Rappelons que le groupe des angles du cercle (de l'ellipse) est le groupe quotient des groupes additifs $\mathbb{R}/\mathbb{Z}$ où l'unité de $\mathbb{Z}$ correspond à l'angle-tour.

Pour la parabole, le groupe est simplement $\mathbb{R}, +$.

Chapitre 7

Courbes hyperelliptiques

Revenons au parcours des courbes entamé par Zagier (Section 6) qui a rencontré successivement des courbes rationnelles et des courbes elliptiques.

Après la classe des courbes rationnelles et celle des courbes elliptiques toutes les autres courbes sont dites hyperelliptiques.
Exemple : $y^2 = (x-1)(x-2)(x-3)(x-4)$

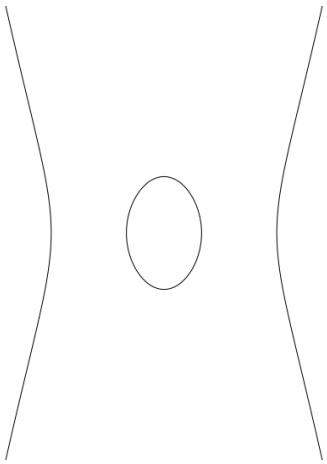


FIGURE 7.1 – Exemple de quartique hypelliptique en Grapher : $y^2 = (x-1)(x-2)(x-3)(x-4)$

Courbe hyperelliptique possédant un unique point double à l'infini.

Elles ont toujours un nombre fini de solutions. Nous comprenons ainsi la situation intermédiaire des courbes elliptiques.

Toute courbe projective algébrique irréductible possède un invariant birationnel qui est le *genre* g. Il prend les valeurs 0, 1, 2, ... Il ne sera pas défini ici.

Les courbes de genre 0 sont appelées *rationnelles*. Les courbes de genre 1 sont appelées *elliptiques*. Les courbes de genre $g \geq 2$ sont appelées *hyperelliptiques*. Cette terminologie prendra tout son sens quand nous aurons pris connaissance de divers résultats.

Si la courbe est considérée sur $\mathbb{C}$ elle a deux dimensions sur $\mathbb{R}$, elle est donc une surface. La théorie permet de prouver que celle-ci est compacte et orientable. Il s'agit d'un tore à g trous, une sphère si $g = 0$.

Le degré de la courbe est un invariant projectif mais pas birationnel. Une droite peut se transformer en cubique ayant un point double, en une quartique ayant deux point doubles, ..., en sextique ayant neuf points de rebroussement, etc.

Etant donné une quartique irréductible $F(X,Y,Z)=0$ (en coordonnées homogènes), ses points doubles et triples éventuels sont les solutions du système

$$\frac{\partial F}{\partial X}=0, \frac{\partial F}{\partial Y}=0, \frac{\partial F}{\partial Z}=0.$$

Ce sont donc les points communs à trois cubiques. On comprend que les points doubles et triples soient a priori peu fréquents.

A titre d'exemple, voici une quartique qui admette un point triple en $[0,1]$.

$$(X-Y)XYZ+(X+Y)^4=0$$

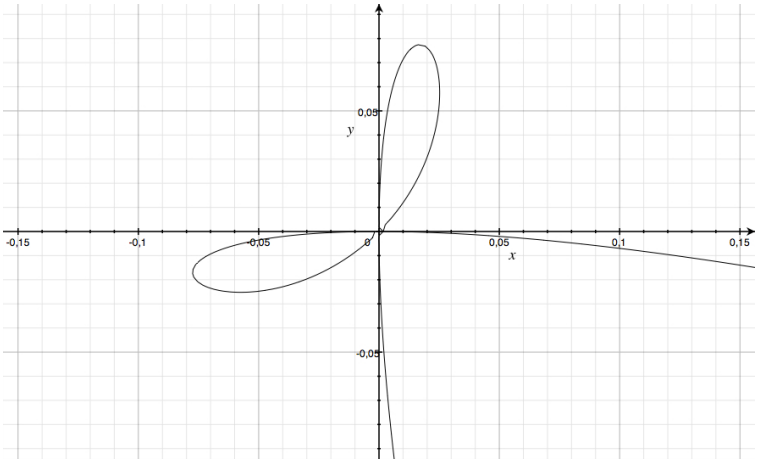


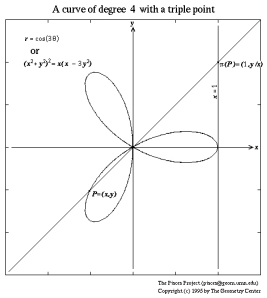
FIGURE 7.2 – Quartique hypelliptique à point triple $(X-Y)XYZ+(X+Y)^4=0$

En coordonnées cartésiennes, $Z=1$. Les termes du plus bas degré sont $(X-Y)XY=0$ qui livre trois droites tangentes en $(0,0)$.

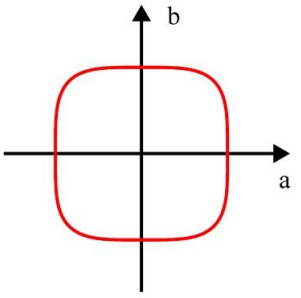
Autre exemple : quartique ayant deux point doubles en $[0,0,1]$ et $[0,1,0]$

$$XYZ^2+XY^2Z+(X+Y)^4$$

Voici quelques exemples de quartiques



Quartique à point triple



ovale

Voir aussi le site Mathcurve
`http://www.mathcurve.com/courbes2d/quarticrationnelle/quarticrationnelle.shtml`

Notons que la sextique à neuf points de rebroussement est la courbe duale d'une cubique.

Par un point extérieur à la cubique passent trois tangentes à la sextique.

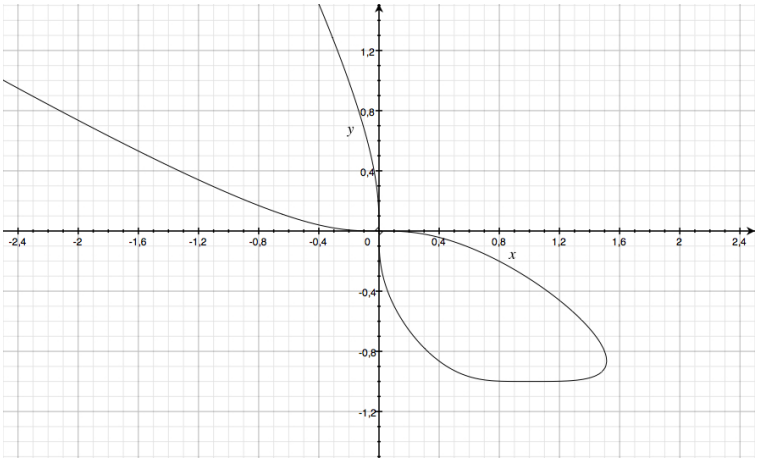


FIGURE 7.3 – Quartique hypelliptique à deux points doubles $(X-Y)XYZ+(X+Y)^4=0$

Chapitre 8

La conjecture de Birch et Swinnerton-Dyer

Zagier part de deux exemples simples d'équations du 3^{e} degré (Matthys 2009) :

a) $x^3 + y^3 = 5$

b) $x^3 + y^3 = 13$

La première admet la solution $(-1, 2)$ et $(2, -1)$ et pas d'autre.

(Zagier ou Matthys a écrit NON !)

(Il fallait OUI !)

La deuxième n'a pas de $\mathbb{Z}$-solution. Donc, ici c'est NON !

Zagier : « Quand cela marche-t-il ? »

« Birch et Swinnerton-Dyer ont une conjecture brillante en 1965

Ils associent un nombre S, "nombre magique" à chaque courbe elliptique. »

$S = 0$ ssi il y a un nombre infini de solutions (de points rationnels)

$S \neq 0$ ssi l'équation possède un nombre fini de solutions (de points rationnels).

Vers 1960 Birch et Swinnerton-Dyer ont formulé une conjecture qui détermine r et à certains égards la constante C (Nous n'avons pas expliqué C). Nous citons un paragraphe de la section 2 de l'article Zagier 1984 :

"Around 1960, Birch and Swinnerton-Dyer formulated a conjecture which determines r, and to some extend C. The idea is that a curve with a large value of (or, given r, with a large value of C) has an especially large number of rational points and should therefore have a relatively large number of solutions modulo a prime p on average as p varies."

Nous citons ici l'article Wikipedia (2011c). *Conjecture de Birch et Swinnerton-Dyer - Wikipédia*. URL : `https://fr.wikipedia.org/wiki/Conjecture_de_Birch_et_Swinnerton-Dyer`) (source Andrew Wiles 2006) :

« En mathématiques, la conjecture de Birch et Swinnerton-Dyer prédit que pour toute courbe elliptique sur le corps des rationnels, l'ordre d'annulation en 1 de la fonction L associée est égal au rang de la courbe. Elle prédit même la valeur du premier terme non nul dans le développement limité en 1 de cette fonction L.

Ouverte depuis plus de quarante ans, la conjecture n'a été démontrée que dans des cas particuliers. Largement reconnue comme un des problèmes mathématiques les plus difficiles et les plus profonds encore ouverts au début du XXI^{e} siècle, elle est un des sept problèmes du prix du millénaire.

Contexte

En 1922, Louis Mordell a démontré le théorème de Mordell : le groupe abélien des points rationnels de toute courbe elliptique définie sur le corps des rationnels est de type fini. Il est donc isomorphe au produit d'un nombre fini de groupes cycliques :

$$(\mathbb{Z}/a_1\mathbb{Z}) \times (\mathbb{Z}/a_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_k\mathbb{Z}) \times \mathbb{Z}^r,$$

où k et r sont deux entiers positifs ou nuls et les a_i sont des entiers strictement positifs.

L'entier r, appelé le rang de la courbe, est un invariant important de la courbe elliptique. Il est nul si et seulement si le groupe est fini (ce qui, d'après le théorème de Faltings (voir la section 6, théorème 1, p. 13), est toujours le cas si la courbe est de genre > 1.

Bien que le théorème de Mordell montre que ce rang est toujours fini, il ne donne pas de méthode effective pour calculer le rang de chaque courbe. Le rang de certaines courbes elliptiques peut être calculé en utilisant des méthodes numériques mais celles-ci ne peuvent pas être généralisées pour toutes les courbes.

Une fonction L, $L(E, s)$, peut être définie pour toute courbe elliptique E en construisant un produit eulérien à partir du nombre de points sur la courbe modulo chaque nombre premier p. Cette fonction L est analogue à la fonction zêta de Riemann et aux séries L de Dirichlet qui sont définies pour une forme quadratique à deux variables. C'est un cas particulier de fonction L de Hasse-Weil.

La définition naturelle de $L(E, s)$ converge seulement pour les valeurs de s dans le plan complexe telles que $Re(s) > 3/2$. Helmut Hasse a conjecturé que $L(E, s)$ pouvait être étendue par prolongement analytique au plan complexe entier. Cette conjecture fut d'abord démontrée par Max Deuring pour les courbes elliptiques avec multiplication complexe. Dans le cas général, elle résulte du théorème de modularité, qui établit que toute courbe elliptique est modulaire, c'est-à-dire que sa fonction L est la fonction L associée à une forme modulaire.

Trouver des points rationnels sur une courbe elliptique générale est un problème difficile. Trouver les points sur une courbe elliptique modulo un nombre premier donné p est conceptuellement direct, puisqu'il n'y a qu'un nombre fini de cas à vérifier. Néanmoins, pour des grands nombres premiers, cela requiert des calculs intensifs. »

Les protagonistes de la conjecture de Birch et Swinnerton-Dyer sont

Bryan Birch : Wikipedia 2011b

> Bryan John Birch F.R.S. (né le 25 septembre 1931) est un mathématicien britannique. Son nom est lié à la conjecture de Birch et Swinnerton-Dyer.
>
> Il a reçu son éducation à la Shrewsbury School et au prestigieux Trinity College, Cambridge.
>
> Doctorant à l'Université de Cambridge, sous la direction officielle de J. W. S. Cassels, il fut plus influencé par Harold Davenport. Il démontra le théorème de Birch, l'un des résultats les plus importants issu de la *circle method* de Hardy et Littlewood. Ce théorème démontre que les formes rationnelles de degré impair dans un ensemble suffisamment large de variables doivent avoir des zéros.
>
> Il travailla ensuite avec Peter Swinnerton-Dyer sur des calculs relatifs aux L-fonctions de Hasse-Weil des courbes elliptiques. La conjecture reliant le rang d'une courbe elliptique à l'ordre du zéro d'une L-fonction a eu une influence majeure sur le développement de la théorie des nombres depuis le milieu des années 1960 jusqu'à nos jours. En 2006, seuls des résultats partiels avaient été obtenus.
>
> Plus tard, il contribua à la K-théorie algébrique (conjecture de Birch–Tate). Il a émis des idées sur le rôle des points de Heegner (il fut l'un des premiers à réexaminer le travail de Kurt Heegner, qui n'avait pas été bien accepté à l'origine). Birch a rassemblé les éléments du contexte de la démonstration du théorème de Gross–Zagier ; la correspondance échangée est désormais publiée.
>
> Il a été élu Fellow of the Royal Society en 1972. Il a reçu le Senior Whitehead Prize en 1993 et la médaille De Morgan en 2007.

Peter Swinnerton-Dyer : Wikipedia 2011f

> Henry Peter Francis Swinnerton-Dyer KBE, FRS (né le 2 août 1927), 16$^{\text{e}}$ baronnet, plus connu sous le nom Peter Swinnerton-Dyer, est un mathématicien britannique spécialisé dans la théorie des nombres et œuvrant à l'université de Cambridge. Au début du XXIe siècle, il est surtout connu pour la conjecture de Birch et Swinnerton-Dyer qui relie les propriétés algébriques des courbes elliptiques aux valeurs spéciales des fonctions L. Cette conjecture fut mise au point avec Bryan Birch au début des années 1960, grâce à des calculs sur l'EDSAC, l'un des premiers ordinateurs britanniques.
>
> En 2006, il a reçu le prix Pólya et la médaille Sylvester.

Ses directeurs de thèse furent John Littlewood et André Weil, et lui-même a dirigé entre autres les thèses de Jean-Louis Colliot-Thélène et Miles Reid.

Reprenons maintenant la suite de l'article *Conjecture de Birch et Swinnerton-Dyer - Wikipédia* (WIKIPEDIA 2011c) :

« **Histoire**
Au début des années 1960, Bryan Birch et Peter Swinnerton-Dyer ont utilisé l'ordinateur EDSAC au laboratoire informatique de l'université de Cambridge pour calculer le nombre de points modulo p (désigné par N_p) pour un grand nombre de nombres premiers p sur des courbes elliptiques dont le rang était connu. À partir de ces résultats numériques, ils émirent la conjecture que N_p pour une courbe E de rang r suit la loi asymptotique

$$\prod_{p \leq x} \frac{N_p}{p} \approx C \log(x)^r \text{ quand } x \to \infty$$

pour une certaine constante C.

Initialement, ceci était basé sur la tendance ténue des points d'un graphique, ce qui induisait un certain scepticisme chez le directeur de thèse de Birch, J. W. S. Cassels.

Cela les conduisit à faire une conjecture sur le comportement de la fonction L d'une courbe elliptique L en $s = 1$, à savoir : qu'il y aurait un zéro d'ordre r en ce point. C'était une conjecture particulièrement spectaculaire car à cette époque, le prolongement analytique de $L(E, s)$ au point $s = 1$ était seulement établi pour les courbes avec multiplication complexe.

Une version plus précise de la conjecture fut ensuite proposée, décrivant le coefficient de Taylor principal de la fonction L en $s = 1$ en fonction d'invariants arithmétiques de la courbe étudiés par Cassels, Tate, Shafarevich et d'autres.

Exemple
Considérons un polynôme en deux variables $f(x, y)$ non nul dont les coefficients sont des nombres rationnels. Supposons que la courbe projective plane associée n'ait pas de singularités. Intéressons-nous aux solutions de l'équation $f(x, y) = 0$ en des nombres rationnels (x, y). Alors :

— Si le degré de f est égal à 1 ou 2 (le cas d'une droite ou d'une conique), soit cet ensemble est vide (par exemple $f(x, y) = x^2 + y^2 + 1$), soit il est infini, auquel cas la courbe projective associée est isomorphe à une droite projective.

— Si le degré de f est supérieur ou égal à 4, cet ensemble est fini d'après le théorème de Faltings (voir la section 6, théorème 1, p. 13).

— Si le degré de f est égal à 3, tous les cas sont possibles. Si cet ensemble est non vide, la courbe projective associée est une courbe elliptique. La conjecture de Birch et Swinnerton-Dyer prédit alors la « taille » (le rang) de l'ensemble des solutions en fonction du prolongement méromorphe d'une série génératrice formée à partir du nombre de solutions de $f(x, y) = 0$ modulo p pour tout nombre premier p. Elle prédit en particulier le fait de savoir si cet ensemble est fini ou infini.

État actuel
La conjecture de Birch et Swinnerton-Dyer a été démontrée seulement dans les cas particuliers suivants :

1. En 1976, John Coates et Andrew Wiles ont démontré que si E est une courbe sur un corps de nombres F avec multiplication complexe par un corps quadratique imaginaire K de nombre de classes 1, $F = K$ ou Q, et si $L(E, 1)$ n'est pas 0 alors E possède seulement un nombre fini de points rationnels. Ceci fut étendu par Nicole Artaud au cas où F est une extension abélienne finie de K.
2. En 1983, Benedict Gross et Don Zagier ont montré que si une courbe elliptique modulaire possède un zéro d'ordre 1 en $s = 1$ alors elle possède un point rationnel d'ordre infini.
3. En 1990, Victor Kolyvagin a montré qu'une courbe elliptique modulaire E pour laquelle $L(E, 1)$ n'est pas zéro est de rang 0, et une courbe elliptique modulaire E pour laquelle $L(E, 1)$ possède un zéro d'ordre 1 en $s = 1$ est de rang 1.

4. En 2001, Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor, étendant les travaux d'Andrew Wiles, ont démontré (théorème de modularité) que toutes les courbes elliptiques sur $\mathbb{Q}$ sont modulaires, ce qui étend les deux résultats précédents à toutes les courbes elliptiques sur $\mathbb{Q}$.
5. En 2010, Manjul Bhargava et Arul Shankar ont annoncé une preuve que le rang moyen du groupe de Mordell-Weil d'une courbe elliptique sur $\mathbb{Q}$ est majoré par 7/6. En combinant ceci avec la preuve annoncée de la conjecture principale de la théorie d'Iwasawa pour $GL(2)$ par Chris Skinner et Éric Urban, ils concluent qu'une proportion non nulle de courbes elliptiques sur $\mathbb{Q}$ sont de rang analytique nul (d'après le résultat de Kolyvagin, ces courbes vérifient la conjecture de Birch et Swinnerton-Dyer).

Rien n'a été démontré pour les courbes de rang supérieur à 1, bien que les calculs laissent à penser que la conjecture est vraie.

La conjecture de Birch et Swinnerton-Dyer est un des sept problèmes du prix du millénaire recensés et mis à prix en 2000 par l'Institut de mathématiques Clay. »

Chapitre 9

Conjecture de Mordell

9.1 La fonction L de Hasse-Weil d'une courbe elliptique

Nous nous référons au chapitre II du livre de Koblitz 1984 qui est incontournable.

La fonction de congruence zêta p. 51

La fonction zeta de E_n :p. 56, th p.59

Faire varier le nombre premier p . p. 64

Le prototype : la fonction zeta de Riemann p. 70

La fonction L de Hasse-Weil et son équation fonctionnelle p. 79, th p.84

La valeur critique Koblitz p. 90–91

La valeur de la fonction L de Hasse-Weil $L(E, s)$ d'une courbe elliptique E en $s = 1$ est appelée *valeur critique*.

Quand nous avons une équation fonctionnelle qui relie $L(E, s)$ à $L(E, 2 - s)$, le point $s = 1$ est le « centre » de l'équation fonctionnelle ; c'est le point fixe de la correspondance $s \leftrightarrow 2 - s$. Il y a une symétrie qui conserve l'équation fonctionnelle et qui est situé en $s = 1$.

L'importance de cette valeur critique provient de la célèbre conjecture de Birch et Swinnerton-Dyer

$$L(E, s) = 0 \text{ si et seulement si } E \text{ a un nombre fini de points rationnels.}$$

Voici un commentaire ci-dessous date de 1984 dont nous n'avons pas vérifié s'il est encore d'application aujourd'hui.

?Dans cette conjecture, E est toute courbe elliptique sur $\mathbb{Q}$. Dans le cas général, il n'a même pas été démontré qu'il y a un sens à parler de $L(E, 1)$ parce que personne n'a réussi à prouver le prolongement analytique de $L(E, s)$ à gauche de la droite Re $s = \frac{3}{2}$. Cependant, le prolongement analytique et une équation fonctionnelle ont été prouvés pour toute courbe elliptique avec multiplication complexe dont nos E_n sont des cas particuliers, ainsi que pour une classe plus grande de courbes elliptiques avec une « paramétrisation de Weil » par des courbes modulaires. **?**

Coates-Wiles :

Voici quelques extraits du chapitre II de Koblitz :

Koblitz, ch. II, p. 53 :

"This situation is a special case of a much more general fact concerning smooth projective algebraic varieties over finite fields.

Koblitz, ch. II, p. 56 : The zeta-function of E_n

We now return to our elliptic curve E_n, which is the curve $y^2 = x^3 - n^2x$, where n is a squarefree

positive integer. More precisely, E_n is the projective completion of this curve, i. E., we also include the point at infinity. E_n is an elliptic curve over any field K whose characteristic does not divide $2n$, and, as we have seen, it is sometimes useful to take $K = \mathbb{F}_p$, or more generally $K = \mathbb{F}_q$. The purpose of this section is to express the number of F_q-points on E_n in terms of "Jacobi sums".

To do this, we first transform the equation of E_n to a "diagonal form". We say that a hypersurface $f(x_1, \ldots, x_n) = 0$ in $\mathbb{A}_K^m$ is "diagonal" if each monomial in f involves at most one of the variables, and each variable occurs in at most one monomial. For example, the "Fermat curve" $x^d + y^d = 1$ is diagonal. It turns out that diagonal hypersurfaces lend themselves to easy computation of N_r (much in the same way that multiple integrals are much easier to evaluate when the variables are separate). We shall not treat the general case, but only the one we need to evaluate $N_r = \#E_n(\mathbb{F}_{q^r})$.

Koblitz, ch. II, p. 79 : The Hasse-Weil L-function and its functional equation:

Earlier in this chapter we studied the congruence zeta-function $Z(E/\mathbb{F}_p; T)$ for our elliptic curves $e_n : y^2 = x^3 - n^2x$. That function was defined by a generating series made up from the number $N_r = N_{r,p}$ of $\mathbb{F}_{q^r}$-points on the elliptic curve reduced $\mod p$. We now combine these functions for all p to obtain a function which incorporates the numbers $N_{r,p}$ for all possible prime powers p^r, i. e., the numbers of points on E_n over all finite fields.

Let s be a complex variable. We make the substitution $T = p^{-s}$ in $Z(E_n/\mathbb{F}_p; T)$, and define the Hasse-Weil L-function $L(E_n, s)$ as follows:

$$L(E_n, s) \underset{\text{def}}{=} \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n/\mathbb{F}_p; p^{-s})} \tag{9.1}$$

$$= \prod_{p \nmid 2n} \frac{1}{1 - 2a_{E_n,p}p^{-s} + p^{1-2s}} \tag{9.2}$$

$$= \prod_{P \nmid 2n} \frac{1}{1 - \alpha^{\deg P}(\mathbb{N}P)^{-s}} \tag{9.3}$$

We must first explain the meaning of these products, why they are equivalent, and what restriction on $s \in \mathbb{C}$ will ensure convergence."

Koblitz, ch. II, p. 84 :

Théorème 13. *The Hasse-Weil L-function $L(E_n, s)$ for the elliptic curve $E_n : y^2 = x^3 - n^2x$, which for $\Re s > \frac{3}{2}$ is defined by (9.2), extends analytically to an entire function on the whole complex s-plane. In addition let*

$$N = 4|n'|^2 = \begin{cases} 32n^2, n \text{ odd}; \\ 16n^2, n \text{ even}. \end{cases} \tag{9.4}$$

Let

$$\Lambda(s) \underset{def}{=} \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(E_n, s). \tag{9.5}$$

Then $L(E_n)$ satisfies the functional equation

$$\Lambda(s) = \pm\Lambda(2 - s), \tag{9.6}$$

where the "root number" ± 1 is equal to 1 if $n \equiv 1, 2, 3 (\mod 8)$ and is equal to -1 if $n \equiv 5, 6, 7 (\mod 8)$.

Koblitz, ch. II, p. 90-91 : §6 The critical value

Conjecture 1. (B. J. Birch and H. P. F. Swinnerton-Dyer). $L(E,s) = 0$ *if and only if* E *has infinitely many rational points.*

In this conjecture E is any elliptic curve defined over $\mathbb{Q}$. In the general case it has not even proved that it makes sense to speak of $L(E,1)$, because no one has been able to prove analytic continuation of $L(E,s)$ to the left of the line $\Re s = \frac{3}{2}$. However, analytic continuation and a functional equation have been proved for any any elliptic curve with complex multiplication, of which our E_n are special cases, and for a broader class of elliptic curves with a so-called "Weil parametrization" by modular curves. (It has been conjectured by Weil and Taniyama that the latter class actually consists of al elliptic curves defined over $\mathbb{Q}$).

We shall call the above conjecture the "weak Birch-Swinnerton-Dyer conjecture", because Birch and Swinnerton-Dyer made a much more detailed conjecture about the behavior of $L(E,s)$ at $s = 1$. Namely, they conjectured that the *order* of zero is equal to the *rank* r of the group of rational points on E. Moreover, they gave a conjectural description of the coefficient of the first nonvanishing term in the Taylor expansion at $s = 1$ in terms of various subtle arithmetic properties of E.

There is a simple heuristic argument – far from a proof – which shows why the weak Birch-Swinnerton-Dyer conjecture might be true. Let us pertend that the Euler product for $L(E,s)$ is a convergent infinite product when $s = 1$ (which it isn't). In that case we would have:

$$L(E,1) = \prod_p \frac{1}{1 - 2a_{E,p}p^{-s} + p^{1-2s}}\Big|_{s=1} = \prod_p \frac{p}{p + 1 - 2a_{E,p}} = \prod_p \frac{p}{N_p},$$

where $N_p = N_{1,p} = p+1-2a_{E,p}$ is the number of $\mathbb{F}$-points on the elliptic curve E considered modulo p. Now, as p varies, the N_p "straddle" p at a distance bounded by $2\sqrt{p}$. This is because $2a_{E,p} = \alpha_p + \bar{\alpha}_p$, and the reciprocal roots α_p have absolute value $\sqrt{p}$. Thus, roughly speaking, $N_p \approx p \pm \sqrt{p}$. If N_p spent an equal time on both sides of p as p varies, one could expect the infinite product of the p/N_p to converge to a nonzero limit. If, on the other hand, the N_p had a tendency to be on the large side: $N_p \approx p + \sqrt{p}$, then we would obtain $L(E,1) \approx \prod_p p/(p+\sqrt{p}) = \prod_p 1/(1+p^{-1/2}) = 0$. On the other hand, if there are only finitely many rational points, then their contribution to N_p woulf be negligible for large p, so that N_p would have "random" behavior $N_p \approx p \pm \sqrt{p}$. Needless to say, this heuristic argument is not of much help in trying to prove the weak Birch-Swinnerton-Dyer conjecture.

But there is considerable evidence, both computational and theoretical, to support the conjecture of Birch-Swinnerton-Dyer. The most dramatic partial result so far was the proof in 1977 by John Coates and Andrew Wiles that for a large class of elliptic curves, an infinite number of rational points implies that $L(E,1) = 0$.

9.2 Formes modulaires

Le chapitre III : Modular forms de Koblitz 1984 fait référence au livre de Serre 1970. Ce chapitre est une matière intéressante pour la culture générale.
$SL_2(\mathbb{Z})$: matrice 2×2 à coefficients entiers, fonctions homographiques.

Revenons à Silverman and Tate 1992 :

"**Mordell Conjecture**

The Mordell conjecture states that Diophantine equations that give rise to surfaces with two or more holes have only finite many solutions in Gaussian integers with no common factors (Mordell 1922). Fermat's equation has holes, so the Mordell conjecture implies that for each integer, the Fermat equation has at most a finite number of solutions.

This conjecture was proved by Faltings (1984) and hence is now also known as Falting's theorem."

Chapitre 10

Les conjectures de Weil

En 1990, Alain Valette a consacré un article de Math-Jeunes (Valette 1990) aux trois conjectures de Weil qui concernent le nombre de points d'une variété algébrique sur un corps fini. Ces conjectures avaient été formulées par André Weil en 1949 à la suite des résultats de Hasse-Weil concernant le nombre de points d'une courbe elliptique sur un corps fini.

Dans l'encadré de la page 84 de son article, Alain Valette énonce les trois conjectures de Weil :

« *Pour X une "bonne" variété algébrique de dimension r :*

(a) La fonction $Z_X(T)$ est une fonction rationnelle de T, c'est-à-dire un quotient de deux polynômes.

(b) De plus

$$Z_X(T) = \frac{Q_1(T)Q_3(T)\dots Q_{2r-1}(T)}{Q_0(T)Q_2(T)\dots Q_{2r}(T)}$$

où Q_i est un polynôme de degré b_i qui, sur $\mathbb{C}$, admet une factorisation

$$Q_i(T) = (1-\alpha_{i1}T)(1-\alpha_{i2}T)\dots(1-\alpha_{ib_i}T)$$

(c) Le degré b_i du polynôme Q_i peut se définir explicitement à partir de la topologie de l'ensemble $X(\mathbb{C})$ des points complexes de X.

»

A la page 85 du même article, on peut lire :

« Pour les variétés, la conjecture (a) a été démontrée en 1960 par Dwork (Voir à ce propos la référence Katz and Tate 1999, p. 339). De 1966 à 1972, Grothendieck a développé, dans le volume 4 de son "Séminaire de Géométrie algébrique" (1583 pages, 2810 grammes) la machinerie permettant de prouver simultanément les conjectures (a) et (c). Restait à démontrer la conjecture (b), ce qui fut fait par Deligne en 1973 en 34 pages "seulement". »

Chapitre 11

Groupes abéliens selon Fuchs et Bourbaki

Pour la théorie des groupes commutatifs, nous avons utilisé deux références classiques qui sont le livre de Fuchs 1960) et celui de N. Bourbaki Bourbaki 1962).

11.1 Groupes abéliens selon Fuchs

11.1.1 Génération et torsion

Soit G un groupe abélien de neutre o dont la loi ou opération se note $+$ et est appelée addition.

Il est clair que G est un $\mathbb{Z}$-module. Soit S une partie de G. Le sous-groupe *engendré* par S soit $\bar{S}$ est à la fois l'intersection de tous les sous-groupes contenant S et l'ensemble des $\mathbb{Z}$-combinaisons linéaires d'éléments de S.

Si $\bar{S} = G$ on dit que S est une *partie génératrice* de G.

Si S est une partie génératrice finie de G on dit que G est *finiment engendré*.

On dit que G est un *groupe de torsion* ssi tout élément de G est d'ordre fini.

Théorème 14. *Pour tout G, l'ensemble des éléments d'ordre fini de G est un sous-groupe. On l'appelle groupe de torsion de G et on le note $Tor(G)$. Le quotient $T/\,Tor(G)$ est sans torsion.*

11.1.2 Sommes directes

Si A, B sont des sous-groupes de G tels que :

1) A et B engendrent G

2) $A \cap B = 0$

on écrit $G = A + B$ et on dit que G est la somme directe de A et de B. Tout $g \in G$ s'écrit de manière unique $g = a + b$ où $a \in A$ et $b \in B$.

Théorème 15. *Tout groupe de torsion G est une somme directe de p-groupes G_p relatifs à des nombres premiers p distincts. Les G_p sont déterminés de manière unique par G.*

11.1.3 Indépendance linéaire et rang

Des éléments non nuls $a_1, \ldots, a_k$ de G sont appelés *linéairement indépendants* si toute *combinaison linéaire*

$$n_1 a_1 + \ldots n_k a_k = 0 \quad (a_i \in \mathbb{Z})$$

implique $n_1 a_1 = \cdots = n_k a_k = 0$.

Un ensemble L d'éléments de G est une *partie libre* si toute partie finie de L est linéairement indépendante.

Via le lemme de Zorn, toute partie libre est contenue dans au moins une partie libre maximale.

Une partie libre maximale est appelée *base* de G.

Une base B se décompose en parties B_0 et B_p, p premier où B_0 est l'ensemble des éléments de B d'ordre infini et B_p est l'ensemble des éléments de B dont l'ordre est une puissance de p.

Le *rang* de G est le cardinal de $|B_0| =: r_p(G)$ où p parcourt les nombres premiers.

Théorème 16. *Les rangs $r(G)$, $r_0(G)$, $r_p(G)$ sont des invariants de G : ils sont indépendants de la base.*

Parfois, c'est $r_0(G)$ qui est appelé *rang* de G. C'est le cas dans le livre de Kuroš. Et c'est le cas dans la tradition des courbes elliptiques.

11.1.4 Groupes finis et groupes finiment engendrés

Théorème 17. (Frobenius-Stickeleberger 1878) *Tout groupe abélien fini est la somme directe d'un nombre fini de groupes cycliques dont l'ordre est une puissance de nombre premier.*

Théorème 18. *Tout groupe abélien finiment engendré est une somme directe d'un nombre fini de groupes cycliques infinis et/ou finis.*

Question : Tout groupe abélien G de base B est-il le produit direct des sous-groupes cycliques $< b >$ où b parcourt B ? Ce n'est pas le cas. Il existe des conditions nécessaires et suffisantes pour qu'il en soit ainsi. Deux décompositions en somme directe de G sont isomorphes : il existe un automorphisme de G transformant l'une en l'autre.

11.2 Groupes abéliens selon Bourbaki

Contrairement à Nicolas Bourbaki, nous nous adressons à des lecteurs qui connaissent déjà les espaces vectoriels sur un corps K ou plutôt les espaces vectoriels à gauche sur K.

Chez Bourbaki, le corps est remplacé par une structure plus générale qui est celle d'anneau. L'analogue correspondant d'un espace vectoriel est un module à gauche sur A.

Nous reprenons la définition de *module à gauche* dans Bourbaki (Réf. Bourbaki 1962, p. 9–10) :

> **Définition 1.** Etant donné un anneau A, on appelle *module à gauche* sur A (ou *A-module à gauche*), un ensemble E muni d'une structure algébrique définie par la donnée :
>
> 1. d'une loi de groupe commutatif dans E (notée additivement dans ce qui suit) ;
> 2. d'une loi de composition externe partout définie $(\alpha, x) \to \alpha \tau x$, dont le domaine d'opérateurs est l'anneau A, et qui satisfait aux axiomes suivants :
>
> (I) $\alpha \tau (x + y) = (\alpha \tau x) + (\alpha \tau y)$ quels que soient $\alpha \in A$, $x \in E$, $y \in E$;
>
> (II) $(\alpha + \beta) \tau x = (\alpha \tau x) + (\beta \tau x)$ quels que soient $\alpha \in A$, $\beta \in A$, $x \in E$;
>
> (III) $\alpha \tau (\beta \tau x)$ quels que soient $\alpha \in A$, $\beta \in A$, $x \in E$;
>
> (IV) $1 \tau x = x$ pour tout $x \in E$.

Nous aimerons à dire $\mathbb{Z}$-module.

Tout groupe commutatif est un $\mathbb{Z}$-module de manière naturelle en posant

$$n \in \mathbb{N}, ng = \underbrace{g + g + \cdots + g}_{n \text{ fois}}$$

Dans le cas de $\mathbb{Z}$, il faut aussi les négatifs :

$$(-n)g = -(ng)$$

Nous reprenons la définition de *combinaison linéaire* dans Bourbaki (Réf. Bourbaki 1962, p. 13) :

Définition 3 : On dit qu'un élément x d'un A-module E est une *combinaison linéaire*, à coefficients dans A, d'une famille $(a_i)i \in I$ d'éléments de E, s'il existe une famille $(\lambda_i)\, i \in I$ d'éléments de A, de support fini, telle que $x \in \sum_{i \in I} \lambda_i a_i$.

Remerciements

Nos remerciements vont à Jean-Claude Matthys qui nous a confié ses notes manuscrites très soignées (Matthys 2009) et à Hugues Vermeiren qui a réalisé la figure 6.1.

Bibliographie

Amatheurs (2009). *Les problèmes du millénaire*. URL : http://maths.amatheurs.fr/index.php?page=millenaire.

Bashmakova, Isabella et Galina Smirnova (1999). *The Beginnings and Evolution of Algebra*. Abe Shenitzer, translator, 160 pages, ISBN 0-88385-329-9. Buekenhout possède un exemplaire de ce livre, Bouckaert possède une copie du chapitre 3. Mathematical Association of America.

Birch, B.J. et H.P.F. Swinnerton-Dyer (1963). « Notes on elliptic curves. I. » In : *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1963.212, p. 7–25. ISSN : 1435-5345. URL : http://www.reference-global.com/doi/abs/10.1515/crll.1963.212.7.

Bix, Robert (juil. 1998). *Conics and Cubics : A Concrete Introduction to Algebraic Curves*. en. Springer. ISBN : 9780387984018.

Bourbaki, N. C. (1962). *Elements De Mathematique-Algebre*. 3e éd. Livre II Algèbre, Chapitre 2 Algèbre linéaire. Hermann.

Bremner, Andrew (2011). « Positively Prodigious Powers or How Dudeney Done it ? » In : *Math. Mag.* 84, p. 120–125.

Brioist, Pascal (2002). « Les savoirs scientifiques ». In : *Revue d'histoire moderne et contemporaine* 5.49-4bis, p. 52–80. URL : http://www.cairn.info/revue-d-histoire-moderne-et-contemporaine-2002-5-page-52.htm#citation.

Brown, Ezra (mai 2000). « Three Fermat Trails to Elliptic Curves ». In : *The College Mathematics journal* 31.3. URL : http://www.math.vt.edu/people/brown/doc/ellip.pdf.

Brunault, François (16 janvier 2012). « Le rang des courbes elliptiques ». In : *Images des mathématiques*. URL : http://images.math.cnrs.fr/Le-rang-des-courbes-elliptiques.html.

Buekenhout, Francis (2008). « Courbes elliptiques et Pierre Deligne ».

Carlson, J., A. Jaffe et A. Wiles, éds. (2006). *The Millenium Prize Problems*. 169 pages, ISBN-13 :9780821836798, American Mathematical Society.

Chahal, Jasbir S. (avr. 2006). « Congruent Numbers and Elliptic Curves ». In : *The American Mathematical Monthly* 113.4, p. 308–317. ISSN : 00029890. DOI : 10.2307/27641916. URL : http://www.jstor.org/stable/27641916.

Chevanne, Philippe (2011). *Nombres congruents*. URL : http://mathafou.free.fr/themes/kcongnum.html.

Cipra, Barry et Paul Zorn (1994). *What's happening in the mathematical sciences*. American Mathematical Soc. ISBN : 9780821889985.

Coates, J., Z. Liang et R. Sujatha (août 2009). « The Tate–Shafarevich group for elliptic curves with complex multiplication ». In : *Journal of Algebra* 322 (3), p. 657–674.

Coates, John H. (2005). « Congruent Number Problem ». In : *Pure and Applied Mathematics Quarterly* 1.1, p. 14–27.

Colmez, Pierre (2005). *Le problème des nombres congruents*. URL : http://www.math.jussieu.fr/~colmez/congruents.pdf.

Conrad, Keith (2007). *The congruent number problem*. URL : http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/congnumber.pdf.

Cordonnier, Marie-Neige (2009). *Pour la Science - Actualité - Trois milliards de nombres congruents*. URL : http://www.pourlascience.fr/ewb_pages/a/actualite-trois-milliards-de-nombres-congruents-23522.php.

Cornelissen, Gunther L.M. (2010). *Elliptic Curves and their Moduli - Exam Material*. URL : http://www.staff.science.uu.nl/~corne102/elliptic-curves/ellmodcontents.pdf.

Cremona, John (26 mai 2013). *mwrank*. URL : http://homepages.warwick.ac.uk/~masgaj/mwrank/ (visité le 11/04/2014).

Dasgupta, Samit et John Voight (2009). « Heegner points and Sylvester's conjecture ». In : *Arithmetic geometry : Clay Mathematics Institute Summer School, Arithmetic Geometry, July 17-August 11, 2006, Mathematisches Institut, Georg-August-Universität, Göttingen, Germany*. T. 8, p. 89–91.

Dieudonné, (dir.) Jean et al. (1986). *Abrégé d'histoire des mathématiques*. 2e éd. Paris : Hermann.

Dujella, Andrej (p.d.). *History of elliptic curves rank records*. URL : http://web.math.hr/~duje/tors/rankhist.html.

Enriques, Federigo et Oscar Chisini (1915–1934). *Lezioni sulla teoria geometrica delle equazioni e delle funzioni algebriche*. Zanichelli.

Federico, Pasquale Joseph (1982). *Descartes on polyhedra : a study of the De solidorum elementis*. Springer. ISBN : 9780387907604.

Felgner, Ulrich (1984). « On Bachet's diophantine equation $x^3 = y^2 + k$ ». In : *Monatshefte für Mathematik* 98.3, p. 185–191. ISSN : 0026-9255. DOI : 10.1007/BF01507747. URL : http://www.springerlink.com/content/n2205w4k102m7788/.

Fuchs, László (1960). *Abelian groups*. Pergamon Press.

Funar, Louis (2009). *Images des mathématiques - Les nombres congruents*. URL : http://images.math.cnrs.fr/Les-nombres-congruents.html.

Gartner, Jérôme (20 avril 2010). *Quand la géométrie vient au secours de l'arithmétique*. URL : http://images.math.cnrs.fr/Quand-la-geometrie-vient-au.html.

Godefroy, Gilles (jan. 2011). *Mathématiques mode emploi*. Odile Jacob. ISBN : 2738123228.

Goldstein, C., N. Schappacher et J. Schwermer, éds. (2007). *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*. Springer.

Gray, Jeremy (nov. 2010). *Worlds Out of Nothing : A Course in the History of Geometry in the 19th Century*. Springer. ISBN : 9780857290595.

Gunning, Robert C. (déc. 2009). « The Millenium Prize Problems reviewed by Robert C. Gunning ». In : *Notices of the AMS* 56.11, p. 1438–1439. URL : http://www.ams.org/notices/200911/rtx091101438p.pdf.

Heath-Brown, Roger et Victor Flynn (2010). *Elliptic Curves : course material*. URL : http://www.maths.ox.ac.uk/courses/course/9505/synopsis.

Ireland, Kenneth et Michael Rosen (sept. 1990). *A Classical Introduction to Modern Number Theory*. en. Springer. ISBN : 9780387973296.

Katz, Nicholas M et John Tate (mar. 1999). « Bernard Dwork (1923–1998) ». In : *NOTICES OF THE AMS* 46.3, p. 338–343. URL : http://www.ams.org/notices/199903/index.html.

Koblitz, Neal I. (1984). *Introduction to Elliptic Curves and Modular Forms*. Springer. ISBN : 0387979662.

Kreussler, Bernd (2007). « Elliptic Curves – an Introduction ». In : *Irish Math. Soc. Bulletin* 60, p. 39–43. URL : http://www.maths.tcd.ie/pub/ims/bull60/R6001.pdf.

Kun, Jeremy (11 avr. 2014a). *Elliptic Curves as Python Objects | Math ∩ Programming*. February 24 2014. URL : http://jeremykun.com/2014/02/24/elliptic-curves-as-python-objects/ (visité le 11/04/2014).

— (19 mar. 2014b). *Connecting Elliptic Curves with Finite Fields | Math ∩ Programming*. URL : http://jeremykun.com/2014/03/19/connecting-elliptic-curves-with-finite-fields-a-reprise/ (visité le 11/04/2014).

— (31 mar. 2014c). *Elliptic Curve Diffie-Hellman | Math ∩ Programming*. URL : http://jeremykun.com/2014/03/31/elliptic-curve-diffie-hellman/ (visité le 11/04/2014).

Kun, Jeremy (16 fév. 2014d). *Elliptic Curves as Algebraic Structures | Math ∩Programming*. URL : http://jeremykun.com/2014/02/16/elliptic-curves-as-algebraic-structures/ (visité le 11/04/2014).

— (10 fév. 2014e). *Elliptic Curves as Elementary Equations | Math ∩ Programming*. URL : http://jeremykun.com/2014/02/10/elliptic-curves-as-elementary-equations/ (visité le 11/04/2014).

— (8 fév. 2014f). *Introducing Elliptic Curves | Math ∩ Programming*. URL : http://jeremykun.com/2014/02/08/introducing-elliptic-curves/ (visité le 11/04/2014).

— (14 avr. 2014g). *Sending and Authenticating Messages with Elliptic Curves*. Math ∩ Programming. URL : http://jeremykun.com/2014/04/14/sending-and-authenticating-messages-with-elliptic-curves/ (visité le 14/04/2014).

Lemmermeyer, Franz (2010). *Fermat's Bachet-Mordell Equation - MathOverflow*. URL : http://mathoverflow.net/questions/36800/fermats-bachet-mordell-equation.

Lozano-Robledo, Álvaro (2011). *Elliptic Curves, Modular Forms and their L-functions*. URL : http://www.math.uic.edu/~wgarci4/pcmi/PCMI_Lectures.pdf.

Lutz, Elisabeth (1955). *Sur les approximations diophantiennes linéaires p-adiques*. Hermann.

Machiavelo, Antonio (déc. 2009). « Pythagoras, Facts and Legends ». In : *EMS Newsletter*, p. 25–26. URL : http://www.ems-ph.org/journals/newsletter/pdf/2009-12-74.pdf.

Matthys, Jean-Claude (2009). « Notes manuscrites de la conférences de Don Zagier le 3 décembre 2009 ».

McKean, Henry et Victor Moll (1999). *Elliptic Curves : Function Theory, Geometry, Arithmetic*. Cambridge University Press.

Meier, Peter, Jörn Streuding et Rasa Streuding (sept. 2009). « Conjecture pour courbes elliptiques ». In : *Pour la Science* 383, p. 40–47.

Meskens, Ad. (2010). *Travelling Mathematics - The Fate of Diophantos' Arithmetic*. A Springer Basel book.

Moore, A.W. (22 July 2004). « The Seven Million Dollar Question ». In : *The London Review of Books* 26.14, p. 11–13. URL : http://www.lrb.co.uk/v26/n14/aw-moore/the-seven-million-dollar-question.

Mordell, L.J. (1922). « On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees ». In : *Proceedings of the Cambridge Philosophical Society*. T. XXI, p. 179–192.

Neale, Vicky (2009). *Theorem 9 : Bachet's duplication formula « Theorem of the week*. URL : http://theoremoftheweek.wordpress.com/2009/10/06/theorem-9-bachets-duplication-formula/.

Newton, Sir Isaac et Derek Thomas Whiteside (1981). *The Mathematical Papers of Isaac Newton : 1674-1684*. Cambridge University Press. ISBN : 9780521045834.

O'Connor, J. J. et E. F. Robertson (p.d.). *Johann Müller Regiomontanus*. URL : http://www-history.mcs.st-andrews.ac.uk/Biographies/Regiomontanus.html.

— (2010). *The development of group theory*. URL : http://www-history.mcs.st-andrews.ac.uk/HistTopics/Development_group_theory.html.

— (2014). *Diophantus of Alexandria*. URL : http://www-history.mcs.st-andrews.ac.uk/Biographies/Diophantus.html.

Perrin, Daniel (p.d.). *Autour de l'équation de Bachet*. URL : http://www.math.u-psud.fr/~perrin/Conferences/OlympiadeDP.pdf.

Pier, Jean-Paul (juil. 2003). *Development of Mathematics, 1900-1950*. 1ère. Birkhäuser Basel. ISBN : 3764328215.

Poonen, Bjorn (mar. 2001). « Elliptic curves ». In : *University of California, Berkeley*. URL : math.mit.edu/~poonen/papers/elliptic.pdf.

Raussen, Martin et Christian Skau (sept. 2010). « Interview with Abel laureate John Tate ». In : *EMS Newsletter*, p. 41–48.

Rice, Adrian (2010). « 'To a factor près' :Cayley's Partial Anticipation of the Weierstrass P-Function ». In : *The American Mathematical Monthly* 117, p. 291–302.

Rodríguez-Villegas, Fernando et Don Zagier (1994). « Which primes are sums of two cubes ? » In : *Number theory*, p. 295–306.

Schappacher, Norbert (2005a). *Développement de la loi de groupe sur une cubique*. URL : http://www-irma.u-strasbg.fr/~schappa/NSch/Publications_files/DPP.pdf.

— (avr. 2005b). *Diophantus of Alexandria : a Text and its History*. URL : http://www-irma.u-strasbg.fr/~schappa/NSch/Publications_files/Dioph.pdf.

Serre, Jean-Pierre (1970). *Cours d'arithmétique ...* Paris : Presses universitaires de France. URL : http://www.alsatica.eu/fr/alsatica/uha/Cours-d-arithmetique,00186369X.html.

— (Mai 2010). « Un amateur de courbes elliptiques ». In : *La Recherche* 441, p. 20–21. URL : http://www.larecherche.fr/actualite/mathematiques/amateur-courbes-elliptiques-01-05-2010-89262.

Silverman, Joseph H. et John Tate (1992). *Rational Points on Elliptic Curves*. Springer.

Steuding, Jörn, Rasa Steuding et Peter Meier (jan. 2012). « Conjecture pour courbes elliptiques ». In : *Dossier Pour la Science - Les grands problèmes mathématiques* 74, p. 26–30. URL : http://www.pourlascience.fr/ewb_pages/f/fiche-article-conjecture-pour-courbes-elliptiques-28625.php.

Stillwell, John (1989). *Mathematics and Its History*. Springer. ISBN : 0-387-96981-0.

Takasaki, Kanehisa (2012). *Elliptic Functions*. URL : http://www.math.h.kyoto-u.ac.jp/~takasaki/soliton-lab/chron/elliptic.html.

Tunnell, J. B. (1983). « A classical Diophantine problem and modular forms of weight 3/2 ». In : *Inventiones Mathematicae* 72.2, p. 323–334. ISSN : 0020-9910. DOI : 10.1007/BF01389327. URL : http://www.springerlink.com/content/r2l4v5302578x431/.

Valette, Alain (1990). « Les conjectures de Weil ». In : *Math-Jeunes* 47, p. 79–85.

Vogler (5 déc. 2007). *Diophantine equations*. Math Forum - Ask Dr. Math. URL : http://mathforum.org/library/drmath/view/71228.html (visité le 11/04/2014).

Weil, André (1929). « Sur un théorème de Mordell ». In : *Bull. Sc. Math.* 54, p. 182–191.

Weisstein, Eric W. (2010). *Modular Function*. URL : http://mathworld.wolfram.com/ModularFunction.html.

Weisstein, Eric W (2011). *Coates-Wiles Theorem – from Wolfram MathWorld*. URL : http://mathworld.wolfram.com/Coates-WilesTheorem.html.

Wikipedia (2009). *Don Zagier*. URL : http://fr.wikipedia.org/wiki/Don_Zagier.

— (2011a). *Barry Mazur - Wikipedia*. URL : http://en.wikipedia.org/wiki/Barry_Mazur.

— (2011b). *Bryan John Birch - Wikipedia, the free encyclopedia*. URL : https://en.wikipedia.org/wiki/Bryan_Birch.

— (2011c). *Conjecture de Birch et Swinnerton-Dyer - Wikipédia*. URL : https://fr.wikipedia.org/wiki/Conjecture_de_Birch_et_Swinnerton-Dyer.

— (25 juin 2011d). *Courbe elliptique - Wikipédia*. URL : http://fr.wikipedia.org/wiki/Courbes_elliptiques.

— (2011e). *Élisabeth Lutz - Wikipédia*. URL : http://fr.wikipedia.org/wiki/%C3%83%C2%89lisabeth_Lutz.

— (2011f). *Peter Swinnerton-Dyer - Wikipédia*. URL : https://fr.wikipedia.org/wiki/Peter_Swinnerton-Dyer.

— (2011g). *Trygve Nagell - Wikipedia*. URL : http://en.wikipedia.org/wiki/Trygve_Nagell.

— (2012). *Conjecture de Birch et Swinnerton-Dyer*. URL : http://fr.wikipedia.org/wiki/Conjecture_de_Birch_et_Swinnerton-Dyer.

Wiles, Andrew (2006). « The Birch and Swinnerton-Dyer conjecture ». In : *The Millennium prize problems*. [[American Mathematical Society]], p. 31–44. ISBN : 978-0-821-83679-8. URL : http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/birchswin.pdf.

Winterberger, Jean-Pierre (Juin 2010). « La conjecture de modularité de Serre démontrée ». In : *La Recherche* 442, p. 18–19.

Wolfram (2014). *Nine-Point Cubic*. Wolfram Demonstrations Project. URL : http://demonstrations.wolfram.com/NinePointCubic/ (visité le 11/04/2014).

Zagier, Don (nov. 1984). « L-Series of Elliptic Curves, the Birch-Swinnerton-Dyer Conjecture, and the Class Number Problem of Gauss ». In : *Notices of the AMS* 31.7, p. 739–743.

— (1996). *Problems posed at the St Andrews Colloquium, 1996*. URL : http://www-history.mcs.st-and.ac.uk/~john/Zagier/Problems.html.

— (2001). « Don Zagier, Staudt Prize ». In : *Max Planck Research* 3, p. 90–96. URL : http://www.mpim-bonn.mpg.de/digitalAssets/2676_mpforschung_2001_zagier.pdf.

— (2002). *Résumé de cours : Année 2001-2002, Formes modulaires et opérateurs différentiels (suite)*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/resumes.htm.

— (2003). *Résumé de cours : Année 2002-2003, Périodes des formes modulaires*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/resumes.htm.

— (2004). *Résumé de cours : Année 2003-2004, Périodes des formes modulaires (suite)*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/resumes.htm.

— (juillet 2005a). « Don Zagier à la BnF : Lettres d'un inconnu, de Ramanujan à Hardy ». In : *Gazette des mathématiciens* 105, p. 31–36. URL : http://smf4.emath.fr/Publications/Gazette/2005/105/smf_gazette_105_31-36.pdf.

— (2005b). *Résumé de cours : Année 2004-2005, Fonction Thêta*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/resumes.htm.

— (2006). *Résumé de cours : Année 2005-2006, Fonction Thêta (suite)*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/resumes.htm.

— (2007). *Résumé de cours : Année 2006-2007, Formes modulaires et structures algébriques*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/resumes.htm.

— (2008). *Résumé de cours : Année 2007-2008, Fonctions de Green et valeurs spéciales de fonctions L*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/resumes.htm.

— (2009a). *Résumé de cours : Année 2008-2009, Topologie, Combinatoire et Formes Modulaires*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/resumes.htm.

— (2009b). *Travaux*. URL : http://www.college-de-france.fr/default/EN/all/the_nom/travaux.htm.