Trois déguisements de la Grue blanche

La fonction zêta et deux analogues

Olivier Fouquet

Table des matières

Prélude

C'est un plaisir et un honneur d'être devant vous aujourd'hui pour cette rentrée des Masters. L'un des objectifs que je m'étais fixé pour ce mini-cours était d'illustrer l'unité des mathématiques : le sujet que nous allons aborder mélange, vous le verrez, combinatoire, analyse, arithmétique, algèbre, géométrie, topologie, histoire des mathématiques... Mais quand j'ai commencé à préparer, je me suis souvenu de ce que disait la romancière américaine Maya Angelou : "J'ai appris que les gens oublient ce que vous dites, oublient ce que vous faites mais n'oublient jamais comment vous les avez fait se sentir." Comme je veux que vous gardiez un bon souvenir de moi-et surtout de ce dont je vais vous parler-je veux que vous vous sentiez bien, et pour cela, je vais commencer par vous raconter une histoire.

Sans plus attendre, voici donc, dans une traduction personnelle, *Tsuru Nyobo monogatari* c'est-à-dire *La conte de la grue blanche changée en femme.*

Il y a longtemps-oh ! si longtemps-vivait un pauvre bucheron à la lisière d'une forêt. Un jour qu'il cherchait du bois dans les fourrés, il entendit une plainte d'une infinie tristesse : en s'approchant, il vit qu'il s'agissait d'une magnifique grue blanche prise dans un piège. Ému par la souffrance de l'animal, le bucheron la libéra. Plusieurs jours plus tard, une jeune femme d'une beauté exceptionnelle se présenta à lui et lui demanda humblement s'il accepterait de l'épouser. Sa beauté était grande ; le bucheron accepta donc et ils vécurent heureux pendant une saison. Mais la saison suivante, leur misère devint si critique qu'ils furent menacés de famine. "Va me chercher du fil au marché" dit alors l'épouse à son mari "puis laisse moi dans notre chambre la porte close pendant toute une journée et, surtout, n'entre pas avant que j'ai fini mon ouvrage." Le mari fit ce que son épouse lui demandait sans poser de questions et le soir, elle ressortit les yeux rougis de larmes mais portant un superbe kimono d'un blanc immaculé. Le bucheron le vendit à prix d'or et avec l'argent ainsi gagné, ils vécurent heureux pendant une saison. Mais la saison suivante, leur misère devint si critique qu'ils furent menacés de famine. "Va me chercher du fil au marché" dit alors l'épouse à son mari "puis laisse moi dans notre chambre la porte close pendant toute une journée et, surtout, n'entre pas avant que j'ai fini mon ouvrage." Le mari fit ce que son épouse lui demandait sans poser de questions et le soir, elle ressortit une nouvelle fois les yeux rougis de larmes mais avec un kimono d'un blanc immaculé. Mais la saison suivante... misère... fil... "surtout, n'entre pas avant que j'ai fini mon ouvrage." Cette fois-ci, cependant, la curiosité du bucheron fut plus grande. En fin de soirée, il entrouvrit la porte et jeta un regard dans la chambre. Ce qu'il vit le stupéfia : son épouse sous la forme d'une magnifique grue blanche tissait le kimono à partir de ses propres plumes, qu'elle s'arrachait au prix de grandes douleurs. "Hélas, mon époux, ne t'avais-je pas dit de ne pas m'interrompre avant la fin de mon ouvrage ?" lui dit la grue. "Une épouse oiselle ne convient pas à un homme. Je dois donc partir." Et, avec un dernier regard triste, elle s'envola et disparut dans le firmament.

Souvenez-vous bien de cette histoire, ne serait-ce que parce que dans vos deux années de Masters, à commencer par ce qui va se passer dans ce propre cours, il arrivera que votre misère devienne si critique que... Enfin bref, ne perdez pas espoir et n'oubliez pas qu'un superbe kimono vous attend.

1 Première saison

1.1 Combinatoire

1.1.1 Nombres de Bernoulli et sommes de puissances

Le point de départ de notre investigation est la célèbre équation

$$1+2+3+\cdots+(n-1)=\frac{(n-1)n}{2}=\frac{1}{2}(n^2-n)=\binom{n}{2} \tag{1.1.1.1}$$

qui se démontre immédiatement ou bien en calculant deux fois cette somme et en additionnant les termes extrêmes, ou bien par récurrence, ou bien de manière bijective en remarquant que les deux membres comptent le nombre de sous-ensemble à 2 éléments d'un ensemble ayant n éléments.

Au moins une fois que l'on connaît les formules, il est à peine plus difficile de démontrer par récurrence la formule calculant la somme des carrés

$$1^2+2^2+3^2+\cdots+(n-1)^2=\frac{(n-1)n(2n-1)}{6}=\frac{1}{3}\left(n^3-\frac{3}{2}n^2+\frac{1}{2}\right) \tag{1.1.1.2}$$

et celle calculant la somme des cubes

$$1^3+2^3+3^3+\cdots+(n-1)^3=(1+2+\cdots+(n-1))^2=\frac{1}{4}\left(n^4-2n^3+n^2\right). \tag{1.1.1.3}$$

Cette dernière formule ayant au moins l'avantage d'être presque une blague.

L'expérience de ces formules suggère que pour tout $r\in\mathbb{N}$, il existe un polynôme $S_r\in\mathbb{Q}[x]$ tel que

$$\forall\ x\in\mathbb{N}^*,\ \sum_{n=1}^{x-1}n^{r-1}=\frac{1}{r}S_r(x) \tag{1.1.1.4}$$

et une observation attentive suggère même que S_r pourrait être unitaire et de degré r. On peut aussi se convaincre du fait que si l'on parvient à deviner S_r, la formule (1.1.1.4) se démontrera facilement par récurrence.

Reste donc à déterminer les polynômes S_r. Ceci a été fait par Jakob Bernoulli, probablement vers 1680. En voici une présentation moderne. Commençons par rappeler que si

$$\sum_{n=0}^{\infty}a_n\frac{t^n}{n!}\ \text{et}\ \sum_{n=0}^{\infty}b_n\frac{t^n}{n!}$$

sont deux séries entières (vues ou bien comme objets formels, ou bien comme fonction analytique auquel cas on supposera qu'elles sont toutes deux de rayons convergence non-nul), alors leur produit vérifie

$$\left(\sum_{n=0}^{\infty}a_n\frac{t^n}{n!}\right)\left(\sum_{n=0}^{\infty}b_n\frac{t^n}{n!}\right)=\sum_{n=0}^{\infty}c_n\frac{t^n}{n!}$$

pour

$$c_n=\sum_{s=0}^{n}\binom{n}{s}a_{n-s}b_s.$$

En particulier, si pour $n \in \mathbb{N}$ on note $B_n \in \mathbb{Q}$ le nombre rationnel tel que

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

et $B_n(x) \in \mathbb{Q}[x]$ le polynôme tel que

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}, \tag{1.1.1.5}$$

alors

$$B_n(x) = \sum_{s=0}^{n} \binom{n}{s} B_s x^{n-s}. \tag{1.1.1.6}$$

Le membre de droite de l'équation (1.1.1.6) a une autre interprétation. En effet

$$\sum_{s=0}^{n} \binom{n}{s} B_s x^{n-s} = \sum_{s=0}^{n} \frac{B_s}{s!} \frac{n!}{(n-s)!} x^{n-s} = \sum_{s=0}^{n} \frac{B_s}{s!} D^s(x^n) = \sum_{s=0}^{\infty} B_s \frac{D^s}{s!}(x^n)$$

pour D l'opérateur de dérivation sur $\mathbb{C}[x]$. Le polynôme $B_r(x)$ est donc également l'image du polynôme x^r par l'application de $\mathbb{C}[x] \longrightarrow \mathbb{C}[x]$ définie par

$$P(x) \longmapsto \sum_{n=0}^{\infty} B_n \frac{D^n}{n!} \left(P(x)\right).$$

On obtient ainsi l'identité de polynômes suivante

$$B_r(x) = \left(\frac{D}{e^D - 1}\right)(x^r).$$

Ceci signifie que

$$\left(e^D - 1\right) B_r(x) = D(x^r) = r x^{r-1}. \tag{1.1.1.7}$$

Or, la formule de Taylor permet de calculer

$$e^D \left(P(x)\right) = \sum_{n=0}^{\infty} \frac{D^n}{n!} P(x) = P(x+1).$$

Donc (1.1.1.7) se reformule en

$$\frac{1}{r} \left(B_r(x+1) - B_r(x)\right) = x^{r-1}.$$

La somme des puissances $(r-1)$-unième devient alors simplement le calcul d'une somme télescopique. On obtient ainsi la formule clé

$$\sum_{n=0}^{x-1} n^{r-1} = \frac{1}{r} \left(B_r(x) - B_r(0)\right) \tag{1.1.1.8}$$

puis

$$\sum_{n=0}^{x-1} n^{r-1} = \frac{1}{r} \left(B_r(x) - B_r\right)$$

car poser $x = 0$ dans (1.1.1.5) montre que $B_r(0) = B_r$ pour tout r. Nous avons donc montré que le polynôme $S_r(x) = B_r(x) - B_r$ convient.

1.1.2 Calculs (Feel the Bern)

Reste à calculer les nombres B_n et les polynômes $B_n(x)$. Le calcul du développement limité (de préférence avec une machine) donne

$$B_0(x) = 1, B_1(x) = x - \frac{1}{2}, B_2(x) = x^3 - x + \frac{1}{6}, B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$$

et

$$B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30}.$$

Il est heureusement plus facile de calculer les B_n, que l'on appelle les nombres de Bernoulli. On trouve

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}$$

ce qui nous amènerait à conjecturer que tous les nombres de Bernoulli sont des inverses d'entiers ; auquel cas nous nous tromperions lourdement car

$$B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}, B_{14} = \frac{7}{6} \cdots$$

1.1.3 Sommes des puissances négatives

Maintenant que nous avons résolu le problème du calcul de

$$\sum_{n=0}^{x-1} n^{r-1} = \frac{1}{r} \left(B_r(x) - B_r \right),$$

nous voulons résoudre le même problème pour

$$\sum_{n=1}^{x-1} n^{-s}.$$

Comme souvent en mathématique, nous pouvons déclarer que nous avons résolu le problème en posant

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

et, pour $x > 0$,

$$\zeta(s, x) = \sum_{n=0}^{\infty} (x + n)^{-s}$$

(donc $\zeta(s, 1) = \zeta(s)$). Alors

$$\sum_{n=1}^{x-1} n^{-s} = -\zeta(s, x) + \zeta(s).$$

Imaginons maintenant que nous soyons Euler, en 1744. Alors nous remarquerions que nous avons maintenant deux formules pour la sommes des puissances *positives*, à savoir la formule correcte

$$\sum_{n=0}^{x-1} n^{r-1} = \frac{1}{r} \left(B_r(x) - B_r \right)$$

et l'absurde

$$\sum_{n=0}^{x-1} n^{r-1} = -\zeta(1-r,x) + \zeta(1-r).$$

La similitude entre ces deux formules nous amènerait alors à conjecturer

$$\zeta(1-r,x) = -\frac{B_r(x)}{r}$$

et donc (en posant $x=1$)

$$\zeta(1-r) = -\frac{B_r(1)}{r}.$$

L'identité télescopique

$$(B_r(x+1) - B_r(x)) = rx^{r-1}$$

montre que $B_r(1) = B_r(0) = B_r$ si $r > 1$ tandis que $B_1(1) = -1/2$. On aurait donc

$$1+1+1+\cdots = -\frac{1}{2},\ 1+2+3+\cdots = -\frac{1}{12}$$

ou (bien sûr)

$$1^{11}+2^{11}+3^{11}+\cdots = \frac{691}{2^3\cdot 3^2\cdot 5\cdot 7\cdot 13}.$$

1.2 Analyse

1.2.1 Deux lettres grecques

Oubliez π : les deux lettres grecques les plus importantes de la recherche mathématique sont Γ et sa grande soeur ζ.

Nous avons déjà rencontré les définitions de ζ et $\zeta(s,x)$

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s},\ \zeta(s,x) = \sum_{n=0}^{\infty} (x+n)^{-s}$$

dont il est aisé de voir qu'elles définissent des fonctions analytiques de s sur le demi-plan $\Re s > 1$.

La fonction Γ est définie par l'intégrale

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt$$

qui définit manifestement une fonction analytique sur le demi-plan $\Re s > 0$ vérifiant $\Gamma(1) = 1$, $\Gamma(s+1) = s\Gamma(s)$ et donc $\Gamma(n+1) = n!$ pour $n \in \mathbb{N}$.

On admet le lemme suivant.

Lemme 1.1. *La fonction Γ admet un prolongement méromorphe à $\mathbb{C}$ tout entier. Elle ne s'annule pas sur $\mathbb{C}$ et a des pôles simples aux entiers négatifs et son résidu en $-n$ est $(-1)^n/n!$. Plus précisément*

$$\frac{1}{\Gamma(z)} = z e^{\gamma z} \prod_{n=1}^{\infty} \left(\left(1 + \frac{z}{n}\right) e^{-z/n} \right).$$

Ici, γ désigne la constante d'Euler, c'est-à-dire la limite lorsque n tend vers l'infini de la différence

$$-\ln(n) + \sum_{k=1}^{n} \frac{1}{k}.$$

Soit s un nombre complexe de partie réelle strictement supérieur à 1. Alors

$$\begin{aligned}\Gamma(s)\zeta(s,x) &= \int_0^\infty e^{-t} t^s \frac{dt}{t} \sum_{n=0}^{\infty} \frac{1}{(x+n)^s} \\ &= \int_0^\infty \sum_{n=0}^{\infty} e^{-t} \left(\frac{t}{x+n}\right)^s \frac{dt}{t}.\end{aligned}$$

Posons $u = \frac{t}{x+n}$. On obtient alors l'expression intégrale

$$\begin{aligned}\Gamma(s)\zeta(s,x) &= \int_0^\infty \sum_{n=0}^{\infty} e^{-(x+n)u} u^s \frac{du}{u} \\ &= \int_0^\infty \frac{e^{-xu}}{1-e^{-u}} u^s \frac{du}{u}.\end{aligned}$$

1.2.2 Prolongement analytique de ζ

Pour étudier la convergence de cette intégrale, remarquons tout d'abord qu'en dehors de zéro, la décroissance rapide de e^{-xu} assure la convergence pour tout $s \in \mathbb{C}$. En zéro, nous utilisons le fait que

$$\sum_{n=0}^{\infty} \frac{B_n(x)}{n!} u^n = \frac{u e^{xu}}{e^u - 1}$$

et donc que

$$\sum_{n=0}^{\infty} \frac{B_n(x)}{n!} (-1)^n u^n = \frac{u e^{-xu}}{1-e^{-u}}$$

pour obtenir

$$\int_0^1 \frac{u e^{-xu}}{1-e^{-u}} u^{s-2} du = \int_0^1 \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} (-1)^n u^{s+n-2} du = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} \frac{(-1)^n}{s+n-1}.$$

Cette somme définit une fonction méromorphe de s avec des pôles simples en $1-n$ pour $n \in \mathbb{N}$ de résidu

$$(-1)^n \frac{B_n(x)}{n!}.$$

La fonction $\zeta(s,x)$ admet donc un plongement méromorphe à $\mathbb{C}$ tout entier avec un pôle simple en 1. Soit n un entier strictement positif. De

$$\lim_{s \to 1-n} (s+1-n)\Gamma(s) = \frac{(-1)^{n-1}}{(n-1)!}$$

et

$$\lim_{s \to 1-n} (s+1-n)\Gamma(s)\zeta(s,x) = \frac{(-1)^n B_n(x)}{n!},$$

on déduit que

$$\zeta(1-n,x) = -\frac{B_n(x)}{n}.$$

En particulier, on a bel et bien

$$\zeta(0) = -B_1(1) = -\frac{1}{2}.$$

1.3 Arithmétique

1.3.1 L'équation fonctionnelle

Soit $\hat{\zeta}$ la fonction

$$\hat{\zeta}(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

et, pour $x \in \mathbb{R}$ strictement positif, soit

$$\vartheta(x) = \sum_{n=1}^{\infty} e^{-\pi n^2 x}.$$

Si s est un nombre complexe vérifiant $\Re s > 1$, alors

$$\hat{\zeta}(s) = \int_0^\infty \vartheta(x)x^{s/2-1}dx = \int_0^1 \vartheta(x)x^{s/2-1}dx + \int_1^\infty \vartheta(x)x^{s/2-1}dx,$$

ce que l'on peut écrire de manière plus symétrique en faisant le changement de variable $x \mapsto 1/x$ dans la première intégrale

$$\hat{\zeta}(s) = \int_1^\infty \vartheta(1/x)x^{-s/2-1}dx + \int_1^\infty \vartheta(x)x^{s/2-1}dx.$$

Or, il se trouve que

$$2\vartheta\left(\frac{1}{x}\right) + 1 = x^{1/2}\left(\vartheta(x) + 1\right).$$

Donc

$$\begin{aligned}\hat{\zeta}(s) &= \int_1^\infty \vartheta(x)\left(x^{s/2} + x^{\frac{1-s}{2}}\right)\frac{dx}{x} + \frac{1}{2}\int_1^\infty \left(x^{1/2}-1\right)x^{-s/2-1}dx \\ &= \int_1^\infty \vartheta(x)\left(x^{s/2} + x^{\frac{1-s}{2}}\right)\frac{dx}{x} + \frac{1}{s(s-1)}.\end{aligned}$$

Un miracle a eu lieu. Dans la formule ci-dessus, les rôles de s et $1-s$ sont devenus exactement similaires. La fonction $\hat{\zeta}$ admet donc un plongement méromorphe à $\mathbb{C}$ tout entier avec un pôle simple en 0 et 1 et vérifie

$$\hat{\zeta}(1-s) = \hat{\zeta}(s).$$

1.3.2 Deux mystères plus épais que la nuit

A ce stade de notre histoire, faisons deux observations. Tout d'abord, regardons à nouveau la formule

$$\zeta(0) = -\frac{1}{2}.$$

Il se trouve que $\mathbb{Z}$ a exactement deux éléments inversibles et que dans $\mathbb{Z}$, un nombre admet une unique décomposition comme produit de nombres premiers. Les entiers 1 et 2 sont exactement ceux intervenant dans la formule. Est-ce une coïncidence ? Une des conjectures les plus importantes, peut-être la plus importante, de l'arithmétique actuelle prédit que non et que ce fait est la première manifestation d'un phénomène bien plus général.

Et puisque l'on parle de décomposition en facteurs premiers, l'existence et l'unicité de cette décomposition montre que pour $\Re s > 1$

$$\left(1 - p^{-s}\right) \zeta(s) = \sum_{n=1}^{\infty} n^{-s} - \sum_{n=1}^{\infty} (np)^{-s} = \sum_{p \nmid n} n^{-s}$$

donc que

$$\prod_{p} \left(1 - p^{-s}\right) \zeta(s) = 1$$

ou encore que

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

En particulier, $\zeta(s)$ est non-nul si $\Re s > 1$. Par ailleurs, de la formule

$$\pi^{s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{(1-s)/2} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s)$$

on déduit une équation fonctionnelle pour la fonction ζ elle-même ; à savoir

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s). \tag{1.3.2.1}$$

Cette relation montre que la fonction ζ s'annule en $s = -2k$ pour $k \in \mathbb{N}^*$ mais qu'elle ne s'annule pas pour $\Re s < 0$ si s n'est pas de cette forme. Il s'en suit qu'à part les zéros de ζ provenant de l'apparition de sin dans (1.3.2.1), tous les zéros de la fonction ζ sont dans la bande $0 \leq \Re s \leq 1$.

Où sont ces zéros ? Une des conjectures les plus importantes des mathématiques, peut-être la plus importante, que l'on appelle l'hypothèse de Riemann affirme qu'ils sont tous sur la bande $\Re s = 1/2$. Mais pourquoi ? Nous le verrons dans la prochaine saison.

2 Deuxième saison

2.1 Algèbre

2.1.1 Rappels d'algèbre

On rappelle les faits suivants sur les corps finis.

1. Un corps est un anneau dont tous les éléments non-nuls sont inversibles ; par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{Z}/2\mathbb{Z}$ sont des corps.

2. Il existe des corps de cardinal fini ; par exemple l'anneau $\mathbb{Z}/p\mathbb{Z}$ lorsque p est un nombre premier.

3. Plus généralement et plus précisément, il existe un corps fini $\mathbb{F}_q$ de cardinal q si et seulement si $q = p^s$ est une puissance d'un nombre premier et dans ce cas $\mathbb{F}_q$ est unique à isomorphisme près.

Le nombre premier p s'appelle la caractéristique du corps $\mathbb{F}_q$.

4. Le groupe multiplicatif $\mathbb{F}_q^\times$ d'un corps fini est cyclique (nécessairement de cardinal $q-1$).

5. En particulier, il existe un élément ζ d'ordre $q-1$ dans $\mathbb{F}_q^\times$ et tous les éléments de $\mathbb{F}_q$ vérifient $x^q = x$.

6. L'application $x \longmapsto x^p$ est un morphisme de corps.

7. Le corps $\mathbb{F}_{p^s}$ contient le corps $\mathbb{F}_{p^u}$ si et seulement si $u|s$.

8. Plus précisément, un élément $x \in \mathbb{F}_{p^s}$ appartient à $\mathbb{F}_{p^u}$ si et seulement si $u|s$ et $x^{p^u} = x$.

Soit k un corps fini de cardinal q. On appelle caractère de $k^\times$ un morphisme de groupes

$$\chi : k^\times \longrightarrow \mathbb{C}^\times.$$

Notons que l'image de χ est incluse dans le groupe $\mathbb{U}_{q-1}$ des racines $(q-1)$-unième de l'unité. L'ensemble $\widehat{k^\times}$ des caractères de $k^\times$ est fini et il est aisé de voir qu'il est en fait muni d'une structure de groupe multiplicatif commutatif qui le rend isomorphe à $k^\times$ (et donc à $\mathbb{Z}/(q-1)\mathbb{Z}$). En particulier, si $n|q-1$, alors il existe un caractère χ tel que les caractères vérifiant $\psi^n = \mathbb{1}$ soient exactement les caractères $\mathbb{1}, \chi, \chi^2, \cdots, \chi^{n-1}$.

Si χ est un caractère de $\mathbb{F}_q^\times$, on note également χ l'application de $\mathbb{F}_q$ dans $\mathbb{C}$ obtenu en posant

$$\chi(0) = \begin{cases} 1 & \text{si } \chi \text{ est le caractère } \mathbb{1} \text{ identiquement égal à 1,} \\ 0 & \text{sinon.} \end{cases}$$

2.1.2 Équations dans les corps finis

Nous allons utiliser les faits rappelés plus haut pour résoudre la question suivante : combien y a-t-il de solutions à l'équation

$$x^n = a$$

pour $a \in \mathbb{F}_q$ et $n|q-1$?

Lemme 2.1. *Soit $n|q-1$. Le nombre $N(x^n = a)$ de solutions de l'équation $x^n = a$ vérifie*

$$N(x^n = a) = \sum_{\psi^n = \mathbb{1}} \psi(a). \tag{2.1.2.1}$$

En effet, ou bien $a = 0$ auquel cas les deux membres (2.1.2.1) sont bien égaux à 1, ou bien $a = b^n$ pour $b \in \mathbb{F}_q$ auquel cas ils sont bien égaux tous les deux à n, ou bien $a \in \mathbb{F}_q^\times$ n'est pas une puissance n-ième (en particulier $a \neq 1$). Dans ce cas $N(x^n = a)$ est égal à zéro. Par ailleurs, il existe un caractère χ tel que $\chi^n = \mathbb{1}$ et $\chi(a) \neq 1$. Alors

$$\sum_{\psi^n=\mathbb{1}} \psi(a) = \sum_{(\chi\psi)^n=\mathbb{1}} (\chi\psi)(a) = \chi(a) \sum_{\psi^n=\mathbb{1}} \psi(a)$$

donc $\sum_{\psi^n=\mathbb{1}} \psi(a) = 0$.

2.2 Géométrie

2.2.1 Géométrie sur les corps finis

Un cercle de rayon 1 est l'ensemble des points satisfaisant l'équation $x^2+y^2 = 1$. Mais des points où ? S'agit-il des points rationnels ? réels ? complexes ? Pourquoi ne pas regarder les corps finis ?

Considérons à quoi ressemble un cercle pour un tel corps. Supposons que p (et donc q) soit impair. Alors $k^\times$ est de cardinal $q-1$ donc pair et l'application

$$\begin{array}{rcl} \chi : k^\times & \longrightarrow & \{\pm 1\} \\ x & \longmapsto & x^{\frac{q-1}{2}} \end{array}$$

est un caractère bien défini qui engendre le groupe des caractères d'ordre 2. D'après le lemme 2.1

$$N(x^2 = a) = 1 + \chi(a).$$

Donc

$$N\left(x^2+y^2=1\right) = \sum_{a+b=1} N(x^2 = a)N(y^2 = b) = \sum_{a+b=1} \left(1+\chi(a)\right)\left(1+\chi(b)\right)$$

et en développant on obtient

$$N\left(x^2+y^2=1\right) = q + \underbrace{\sum_{a+b=1} \chi(a)\chi(b)}_{\text{Somme de Jacobi}} = q - (-1)^{\frac{q-1}{2}}.$$

Que se passe-t-il maintenant si l'on considère plutôt la cubique $x^3+y^3 = 1$? Supposons cette fois que $q \equiv 1 \bmod 3$. Alors $\chi : x \longmapsto x^{(q-1)/3}$ est bien défini et le lemme 2.1 implique que

$$N(x^3 = a) = 1 + \chi(a) + \chi^2(a).$$

Donc

$$N(x^3+y^3=1) = \sum_{a+b=1} N(x^3 = a)N(y^3 = b) = \sum_{a+b=1} \left(1+\chi(a)+\chi^2(a)\right)\left(1+\chi(b)+\chi^2(b)\right).$$

SI l'on développe comme plus haut, on trouve

$$N(x^3+y^3=1) = q - \chi(-1) - \chi^2(-1) + \underbrace{\sum_{a+b=1} \chi(a)\chi(b)}_{J(\chi,\chi)} + \underbrace{\sum_{a+b=1} \chi^2(a)\chi^2(b)}_{J(\chi^2,\chi^2)}.$$

De $\chi(-1) = \chi^2(-1) = 1$ et de $\chi^2 = \bar{\chi}$, on déduit

$$N(x^3 + y^3 = 1) = q - 2 + 2\Re\left(\sum_{a+b=1} \chi(a)\chi(b)\right).$$

Or, il se trouve que

$$|\sum_{a+b=1} \chi(a)\chi(b)| = \sqrt{q}$$

et donc que

$$|N(x^3 + y^3 = 1) - q + 2| \leq 2\sqrt{q}.$$

Autrement dit, parmi les q^2 éléments de k^2, il y en a environ $q-2$ qui satisfont $x^3+y^3 = 1$ et le terme d'erreur est plus petit que $2\sqrt{q}$.

Nous sommes des mathématiciens, la généralité ne nous fait pas peur. Supposons donc que $q \equiv 1 \bmod n$. Alors $\chi : x \longmapsto x^{(q-1)/n}$ est bien défini et vérifie

$$N(x^n = a) = \sum_{s=0}^{n-1} \chi^s(a)$$

donc

$$N(x^n + y^n = 1) = \sum_{a+b=1} N(x^n = a)N(y^n = b) = \sum_{a+b=1} \sum_{s=0}^{n-1} \chi^s(a) \sum_{t=0}^{n-1} \chi^t(b).$$

Comme plus haut, on peut découper cette somme selon que $s = t = 0$, $s + t = n$, $s = 0$ et $t \neq 0$, $t = 0$ et $s \neq 0$ et finalement les $(n-1)(n-2)$ cas restants. On trouve le résultat remarquable suivant. Soit $\delta_n(-1)$ l'entier égal à 1 si -1 est une puissance n-ième dans k et égal à 0 sinon. Alors

$$|N(x^n + y^n = 1) + \delta_n(-1)n - (q+1)| \leq (n-1)(n-2)\sqrt{q}.$$

2.2.2 Espace projectif

Ce dernier calcul est remarquable car il suggère un lien intime entre nos calculs algébriques et l'espace projectif. Qu'est-ce que l'espace projectif ? Tout d'abord, définissons l'espace affine k^n, c'est-à-dire simplement l'ensemble des n-uplets à coefficients dans k (le cardinal de k^n est donc q^n). L'espace projectif $\mathbb{P}^n(k)$ est l'ensemble suivant

$$\mathbb{P}^n(k) = \{\mathbf{x} = (x_0, x_1, \cdots, x_n) \in k^n - \{0\}\}/\sim$$

où $\sim$ est la relation d'équivalence $\mathbf{x} \sim \mathbf{y}$ si et seulement s'il existe $\lambda \in k^\times$ tel que $\mathbf{x} = \lambda\mathbf{y}$. Remarquons que si $k = \mathbb{F}_q$, alors

$$|\mathbb{P}^n(k)| = \frac{q^n - 1}{q - 1} = 1 + q + \cdots + q^{n-1}.$$

Reprenons les calculs de la section précédente mais cette fois-ci en les interprétant dans l'espace projectif $\mathbb{P}^2(k)$ plutôt que dans l'espace affine $\mathbb{A}^2(k)$.

Autrement dit, au lieu de considérer

$$\{(x_1, x_2) \in \mathbb{A}^2(k) | x_1^2 + x_2^2 = 1\},$$

on considère

$$\{(x_0, x_1, x_2) \in \mathbb{P}^2(k) | x_1^2 + x_2^2 = x_0^2\}$$

et de même pour $x^3 + y^3 = 1$, $x^n + y^n = 1$. Notons que si l'on sait calculer

$$| \left\{ \mathbf{x} \in \mathbb{P}^2(k) | x_1^n + x_2^n = x_0^n \right\} |,$$

alors il est aisé de résoudre notre problème initial $N(x^n + y^n = 1)$; car l'ensemble

$$\left\{ \mathbf{x} \in \mathbb{P}^2(k) | x_1^n + x_2^n = x_0^n \right\}$$

est en bijection avec l'union disjointe

$$\{(x_1, x_2) \in \mathbb{A}^2(k) | x_1^n + x_2^n = 1\} \coprod \{x \in k | x^n = -1\}$$

par l'application qui envoie (x_0, x_1, x_2) sur $(x_1/x_0, x_2/x_0)$ dans le premier ensemble si $x_0 \neq 0$ et qui envoie $(0, x_1, x_2)$ sur x_2/x_1 dans le deuxième ensemble (remarquons que si $x_0 = 0$, alors $x_1 \neq 0$ car $x_1^n + x_2^n = 0$ et $(0, 0, 0) \notin \mathbb{P}^2(k)$). Or le cardinal de

$$\{x \in k | x^n = -1\}$$

est n si -1 est une puissance n-ième dans k et 0 sinon. C'est donc $\delta_n(-1)$. Le cardinal de

$$\left\{ \mathbf{x} \in \mathbb{P}^2(k) | x_1^n + x_2^n = x_0^n \right\}$$

est donc

$$N(x^n + y^n = 1) + \delta_n(-1).$$

Donc

$$-(n-1)(n-2)\sqrt{q} \leq | \left\{ \mathbf{x} \in \mathbb{P}^2(k) | x_1^n + x_2^n = x_0^n \right\} | - (q+1) | \leq (n-1)(n-2)\sqrt{q}.$$

ou encore

$$-(n-1)(n-2)\sqrt{q} \leq | \left\{ \mathbf{x} \in \mathbb{P}^2(k) | x_1^n + x_2^n = x_0^n \right\} | - | \mathbb{P}^1(k) | \leq (n-1)(n-2)\sqrt{q}.$$

Le nombre d'éléments de l'espace projectif $\mathbb{P}^2(k)$ sur la courbe $x_1^n + x_2^n = x_0^n$ est égal au nombre de points sur la droite projective $\mathbb{P}^1(k)$ à un terme d'erreur près en $\sqrt{q}$.

2.3 Percer le déguisement

2.3.1 La fonction Z

Quel est l'intérêt de tout cela ? Pour le percevoir, il faut revenir une seconde à la combinatoire. Fixons un nombre premier $p \equiv 1 \bmod n$ et posons

$$N_s = | \left\{ \mathbf{x} \in \mathbb{P}^2(\mathbb{F}_{p^s}) | x_1^n + x_2^n = x_0^n \right\} | .$$

Autrement dit, on s'intéresse non seulement aux solutions dans le corps $k = \mathbb{F}_p$ our $k = \mathbb{F}_{p^2}$ par exemple, mais dans tous les corps de la forme $\mathbb{F}_{p^s}$ à la fois. Plus généralement, soit f un polynôme homogène en $n+1$ variables. Alors l'ensemble

$$N_s = | \{ \mathbf{x} \in \mathbb{P}^n(\mathbb{F}_{p^s}) | f(\mathbf{x}) = 0 \} |$$

est bien défini et l'on peut se demander si le cardinal de cet ensemble vérifie des propriétés similaires à celles vérifiées dans le cas particulier $f(x_0, x_1, x_2) = x_1^n + x_2^n - x_0^n$.

Afin d'étudier les entiers N_s, on introduit la série génératrice

$$Z(u) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{u^s}{s}\right)$$

que l'on peut voir comme une série formelle en u, mais dont il est de toutes façons aisé de vérifier qu'elle converge pour $|u|$ suffisamment petit. Supposons ne serait-ce que pour un instant que cette fonction, *a priori* une série infinie assez générale, soit en fait une fraction rationnelle et plus précisément qu'elle soit de la forme

$$Z(u) = \frac{\prod_{i=1}^{m}(1-\alpha_i u)}{(1-u)(1-pu)} \in \mathbb{C}(u).$$

Supposons de plus-mais pourquoi ?-qu'il existe un entier g tel que

$$Z\left(\frac{1}{pu}\right) = p^{1-g}u^{2-2g}Z(u) = p^{1-g}u^{2-2g}\left(\frac{\prod_{i=1}^{m}(1-\alpha_i u)}{(1-u)(1-pu)}\right) \tag{2.3.1.1}$$

et que $|\alpha_i| \leq \sqrt{p}$ pour tout i. Observons alors que si α est l'un des α_i, alors $1/\alpha$ est un zéro de Z donc également de $u \mapsto Z(1/pu)$ d'après l'équation fonctionnelle (2.3.1.1). Donc $1/p\alpha$ est aussi un des α_i. Donc

$$|1/p\alpha| \leq \sqrt{p}$$

et donc $|\alpha| \geq \sqrt{p}$. Finalement, tous les zéros réciproques de $Z(u)$ seraient de module exactement $\sqrt{p}$.

Qui plus est, si l'on prend la dérivée logarithmique de

$$\exp\left(\sum_{s=1}^{\infty} N_s \frac{u^s}{s}\right) = Z(u) = \frac{\prod_{i=1}^{m}(1-\alpha_i u)}{(1-u)(1-pu)},$$

et si l'on multiplie par u, on obtient

$$\begin{aligned}\sum_{s=1}^{\infty} N_s u^s &= \frac{u}{1-u} + \frac{u}{1-pu} - \sum_{i=1}^{m}\frac{u}{1-\alpha_i u} \\ &= \sum_{s=1}^{\infty} u^s + \sum_{s=1}^{\infty} p^s u^s - \sum_{i=1}^{m}\sum_{s=1}^{\infty}\alpha_i^s u^s.\end{aligned}$$

En identifiant termes à terms les deux séries, on obtient donc

$$N_s = p^s + 1 - \left(\sum_{i=1}^{m}\alpha_i^s\right).$$

et donc

$$\mid N_s - \sharp\mathbb{P}^1(\mathbb{F}_{p^s}) \mid = \mid -\left(\sum_{i=1}^{m}\alpha_i^s\right) \mid \leq mp^{s/2}.$$

Sous nos étranges hypothèses, on retrouverait donc le phénomène que l'on a observé dans la section précédente : le nombre de points de l'espace projectif satisfaisant à une équation (une courbe projective) est égal au nombre de point de la droite projective à un terme d'erreur près qui est linéaire en $\sqrt{q} = p^{s/2}$.

2.3.2 Le kimono d'un blanc immaculé

Mais pourquoi nos hypothèses auraient-elles la moindre chance d'être vraies ?

Considérons tout d'abord un polynôme homogène f à coefficients dans $\mathbb{F}_p$ et observons que si $\mathbf{x} = (x_1, \cdots, x_n)$ est une solution affine de $f(\mathbf{x}) = 0$ telle que le plus petit corps contenant tous les x_i soit $\mathbb{F}_{p^s}$, alors les $(x_1^{p^i}, \cdots, x_n^{p^i})$ pour $0 \leq i \leq s-1$ sont aussi des solutions des $f(\mathbf{x}) = 0$. En effet, le morphisme $\sigma_i : x \longmapsto x^{p^i}$ est un morphisme de corps donc

$$f(\sigma_i(\mathbf{x})) = \sigma_i\left(f(x)\right) = \sigma_i(0) = 0.$$

De plus, ces solutions sont toutes distinctes car sinon $x_j^{p^i}$ serait égal à x_j pour tout j et cela impliquerait que la solution $\mathbf{x}$ est à coefficients dans un sous-corps strict de $\mathbb{F}_{p^s}$. Dans cette situation, on dira que la solution $\mathbf{x}$ est de degré s et les s solutions obtenues comme plus haut seront appelées les conjuguées de $\mathbf{x}$. On appelle zéro-cycle de degré s l'ensemble des conjuguées d'une solution de degré s. La partition de l'ensemble des solutions à coefficients dans $\mathbb{F}_{p^s}$ en zéro-cycles de degré d montre l'égalité

$$N_s = \sum_{d|s} d a_d$$

où a_d désigne le nombre de zéro-cycles de degré d. Donc

$$\begin{aligned}\left(\sum_{s=1}^{\infty} N_s \frac{u^s}{s}\right)' &= \frac{1}{u}\sum_{s=1}^{\infty} N_s u^s = \frac{1}{u}\sum_{s=1}^{\infty}\left(\sum_{d|s} d a_d\right) u^s = \frac{1}{u}\sum_{d=1}^{\infty}\left(\sum_{r=1}^{\infty} u^{dr}\right) d a_d \\ &= \frac{1}{u}\sum_{d=1}^{\infty}\frac{d a_d u^d}{1-u^d} = \sum_{d=1}^{\infty}\frac{d a_d u^{d-1}}{1-u^d} = \left(-\sum_{d=1}^{\infty} a_d \log\left(1-u^d\right)\right)' \\ &= \left(\log\left(\prod_{d=1}^{\infty}\left(\frac{1}{1-u^d}\right)^{a_d}\right)\right)'.\end{aligned}$$

En prenant la primitive de chaque côté, on obtient donc l'équation fondamentale

$$Z(u) = \prod_{d=1}^{\infty}\left(\frac{1}{1-u^d}\right)^{a_d}.$$

Or, a_d est par définition le nombre de zéro-cycles de degré d solution de f donc

$$\left(\frac{1}{1-u^d}\right)^{a_d} = \prod_{x \in ZC(d)} \frac{1}{1-u^{\deg(x)}}$$

et donc

$$Z(u) = \prod_{x \in ZC} \frac{1}{1 - u^{\deg(x)}}.$$

Si l'on définit enfin la fonction ζ d'une variable complexe s par

$$\zeta(s) = Z(p^{-s}),\ \hat{\zeta}(s) = p^{(s-1)(g-1)} Z(p^{-s}),$$

on remarque que

$$\zeta(s) = \prod_{x \in ZC} \frac{1}{1 - p^{-s \deg x}}$$

et que nos étranges hypothèses signifient que

$$\hat{\zeta}(1 - s) = \hat{\zeta}(s)$$

et que tous les zéros complexes de ζ vérifient $\Re s = 1/2$.

3 Troisième saison

Dans cette saison, nous découvrons le secret de la Grue blanche, mais le prix à payer est que, comme dans le conte, nous la perdons également de vue à tout jamais.

3.1 Où en sommes-nous ?

Résumons ce que nous avons vu jusqu'à présent. Nous avons d'une part rencontré la fonction ζ de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \frac{1}{1 - p^{-s}},$$

calculé ses valeurs aux entiers négatifs, montré qu'elle vérifiait une équation fonctionnelle reliant $\zeta(s)$ et $\zeta(1-s)$ et conjecturé que ses zéros complexes non-triviaux étaient de partie réelle $1/2$. Ensuite, nous avons introduit

$$\zeta(s) = \prod_{x \in ZC} \frac{1}{1 - p^{-s \deg x}}$$

où le produit est pris sur l'ensemble des zéro-cycles d'une équation $f(\mathbf{x}) = 0$. Nous avons conjecturé par analogie avec le premier cas et en observant le nombre de solutions de cette équation que $\zeta(s)$ était une fraction rationnelle en p^{-s} de la forme

$$\zeta(s) = \frac{\prod_{i=1}^{m} (1 - \alpha_i p^{-s})}{(1 - p^{-s})(1 - p^{1-s})}$$

satisfaisant une équation fonctionnelle reliant $\zeta(s)$ et $\zeta(1 - s)$ et dont les zéros sont de partie réelle $\Re s = 1/2$. Rappelons également que si $\zeta(s)$ vérifie bien ces propriétés, le nombre N_q de solutions de l'équation $f(\mathbf{x}) = 0$ dans $\mathbb{P}^2(\mathbb{F}_q)$ vérifie

$$\mid N_q - \sharp \mathbb{P}^1(\mathbb{F}_q) \mid \leq O(\sqrt{q}).$$

Or, nous avons vu par ailleurs que cette inégalité était vraie pour certains f très particulier. En conséquence, nous avons un faisceau de présomptions.

3.2 Histoire des mathématiques

Diophante d'Alexandrie est un mathématicien de l'Antiquité tardive. Très peu de choses certaines sont connues à son sujet mais on date en général sa vie au troisième siècle de l'ère commune. L'oeuvre principale qui nous soit parvenue de sa main est son *Artihmétique*.

L'*Arithmétique* de Diophante (ou du moins la partie qui a survécu jusqu'à nous, soit 10 des 13 livres annoncés dans la préface de l'ouvrage) est une collection de problèmes. Le problème 28 du livre I, par exemple, demande au lecteur de *trouver deux nombres dont la somme et la somme des carrés sont des nombres donnés*. Un autre problème demande au lecteur de trouver deux nombres tels que le cube de leur somme soit égal à la somme du cube du premier et du second. Autrement dit, le premier problème demande de résoudre

$$\begin{cases} x + y = a \\ x^2 + y^2 = b \end{cases}$$

et l'Arithmétique suggère de traiter le cas $a = 20$ et $b = 208$ tandis que le second demande de résoudre

$$(x + y)^3 = x^3 + y.$$

Dans l'*Arithmétique*, les solutions proposées sont respectivement 12 et 8 et 7/13 et 1/13.

Non seulement tous les problèmes de l'Arithmétique admettent-ils des solutions mais ils sont même tous résolus au sens où Diophante donne au moins une solution. La lecture des solutions proposées par le manuscrit montre que pour Diophante, nombre signifie nombre rationnel positif et l'on peut de plus inférer qu'il connaissait les nombres irrationnels : lorsque ses calculs l'amèneraient à une solution irrationnelle, il s'arrête et reprend en arrière en changeant les valeurs numériques qu'il considère. Pour ce que cela vaut, je vous conseille d'essayer de résoudre les deux problèmes ci-dessus par vous-mêmes.

Pour des raisons historiques, je ne peux pas résister à l'envie de mentionner encore le problème 8 du livre II de l'Arithmétique, qui énonce *Diviser un carré donné en une somme de deux carrés* et qui propose de traiter le cas de 16 (la solution offerte par l'*Arithmétique*est 256/25 et 144/25).

Vers 1630, un magistrat du Sud-Ouest célèbre surtout pour son excellente éducation classique et ses talents de polyglotte étudie soigneusement l'Arithmétique de Diophante. Profitant des innovations de l'algèbre, il s'attache à en résoudre le problèmes de manière générale (et non seulement en donnant une solution particulière comme le fait Diophante lui-même). Dans la marge de sa copie de l'Arithmétique, il écrit que l'aire d'un triangle rectangle dont les côtés sont des nombres rationnels n'est jamais un carré. Autrement dit, il n'existe pas de nombres rationnels a, b, c, n vérifiant

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2n^2. \end{cases}$$

Mais plus intéressant encore que l'énoncé est la preuve qui est inscrite. Tout d'abord, on remarque que si un tel triangle existe, alors en posant $2ab = (2n)^2$ est un carré. Donc

$$b^2 - 2ab + a^2 = (b - a)^2, a^2 + b^2 = c^2, b^2 + 2ab + a^2 = (b + a)^2$$

sont trois carrés α^2, β^2 et γ^2 formant une progression arithmétique dont la raison est un carré δ^2. Donc

$$\beta^4 - \delta^4 = (\beta^2 - \delta^2)(\beta^2 + \delta^2) = \alpha^2\gamma^2 = (\alpha\gamma)^2$$

et l'équation

$$u^4 - v^4 = w^2$$

admet une solution rationnelle (à savoir $u = \beta$, $v = \delta$ et $w = \alpha\gamma$). Il s'agit donc de montrer qu'il n'est pas possible d'écrire une puissance quatre comme la somme d'un carré et d'une puissance quatre non-nulle. Or, cette équation est équivalente à l'équation

$$\left(\frac{u}{v}\right)^6 - \left(\frac{u}{v}\right)^2 = \frac{u^2 w^2}{v^6}$$

en multipliant par u^4/v^6. Donc il suffit de montrer que l'équation

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

n'admet pas de solution rationnelle vérifiant $y \neq 0$.

Avant d'étudier cette équation, remarquons le fait suivant. S'il est bien exact que l'équation

$$u^4 - v^4 = w^2$$

n'admet pas de solutions rationnelles avec $v \neq 0$, alors *a fortiori* l'équation

$$z^4 - y^4 = x^4$$

n'en admet pas non plus, car si un carré n'est jamais la différence de deux puissances quatrièmes, une puissance quatrième non plus. Donc, si $xyz \neq 0$, alors

$$x^4 + y^4 = z^4$$

n'admet pas de solution rationnelles. A ce stade, vous avez peut-être deviné que le magistrat du Sud-Ouest s'appelait Pierre de Fermat. Dans la marge du problème 8 du livre II, il a écrit sur sa copie la deuxième observation la plus célèbre de l'histoire des mathématiques.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi.

C'est-à-dire

Il est impossible de diviser un cubes en deux cubes, ou deux bicarrés en deux bicarrés et généralement une puissance supérieure à la seconde en deux puissances semblables. J'ai découvert une preuve vraiment merveilleuse de ce fait.

La deuxième observation la plus célèbre, car la plus célèbre vient juste après.

Hanc marginis exiguitas non caperet.

C'est-à-dire

Cette marge est trop étroite pour la contenir.

Un fait amusant à ce sujet et que Fermat n'est pas la première personne à avoir écrit un commentaire dans la marge du problème 8 du livre II. Le grand bibliophile Jean Chortasménos, un moine byzantin qui vécut d'environ 1370 à 1431 a lui aussi laissé un commentaire. Même marge, même problème. Son commentaire à lui ? "Que ton âme aille à Satan, Diophante, à cause de la difficulté de tes théorèmes et en particulier de celui-là."

3.3 Courbe elliptique

3.3.1 Points rationnels sur les courbes elliptiques

Tout ceci est un long prétexte pour étudier l'équation

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

et la courbe qu'elle définit. D'après Fermat, il n'y a pas de points rationnels d'ordonnée non-nulle sur cette courbe. Une courbe lisse définie par une équation de la forme

$$E : y^2 = x^3 + ax + b$$

s'appelle une courbe elliptique. Voici trois exemples de courbes elliptiques.

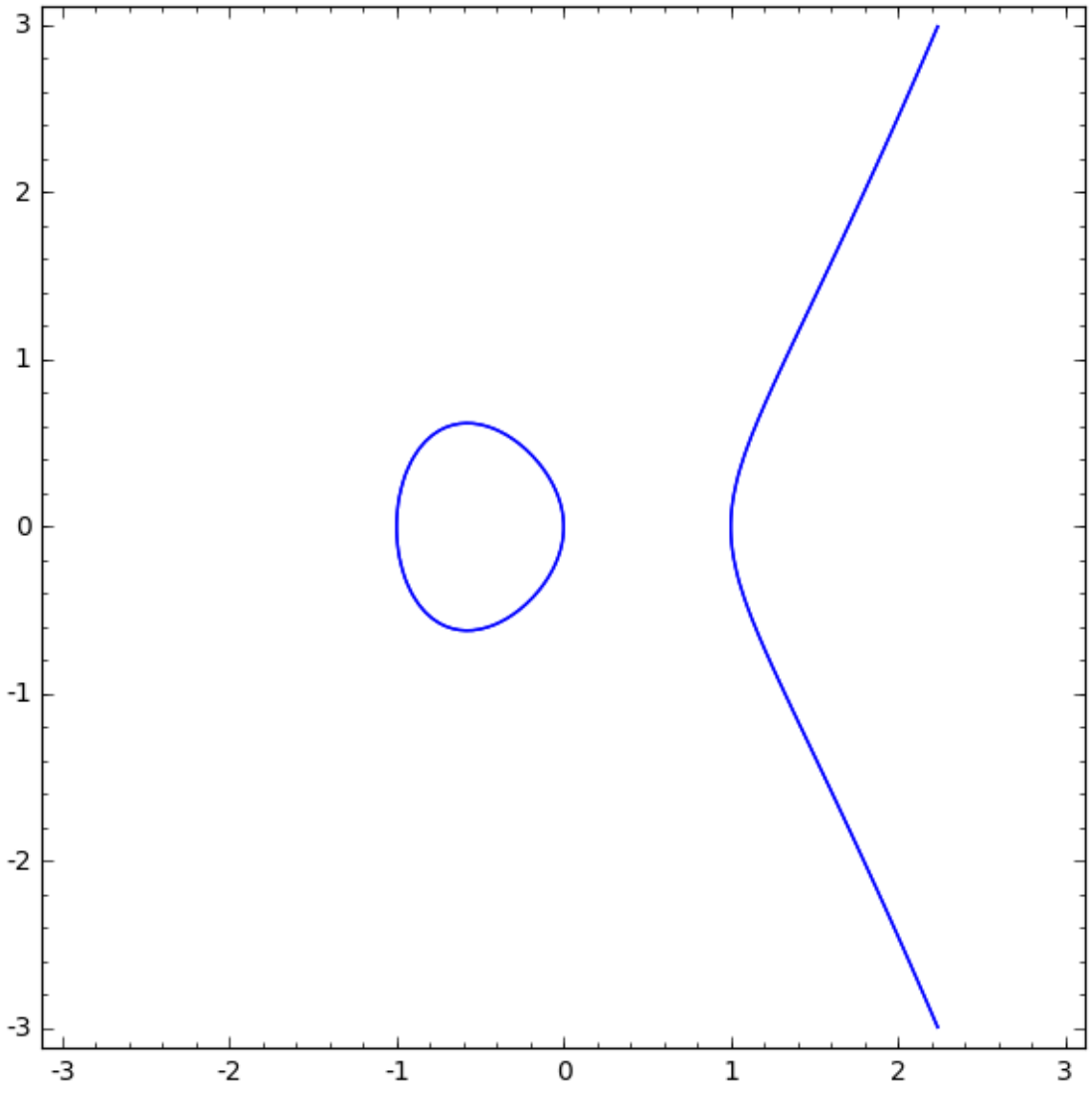

FIGURE 1 : $y^2 = x^3 - x$

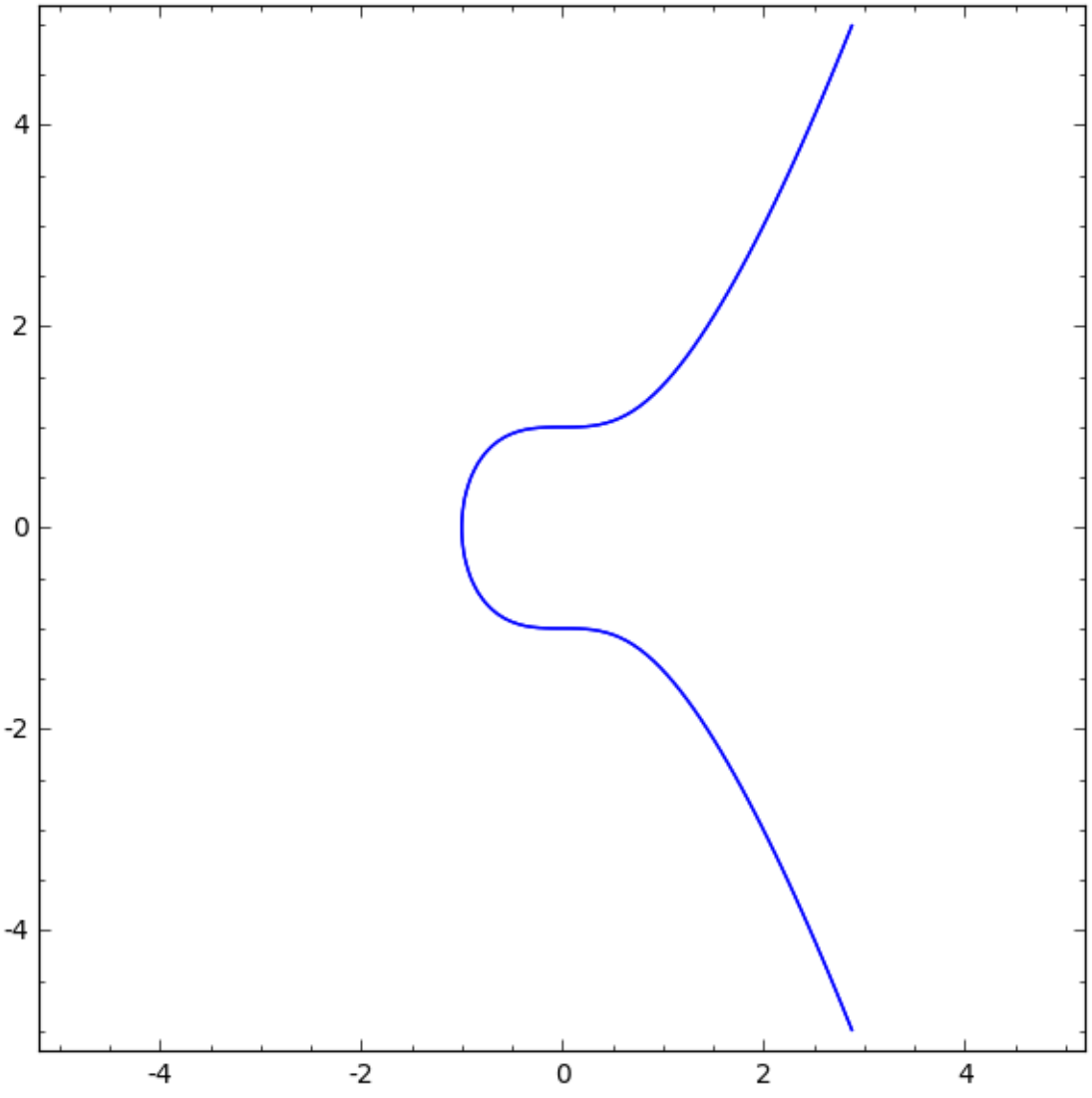

FIGURE 2 : $y^2 = x^3 + 1$

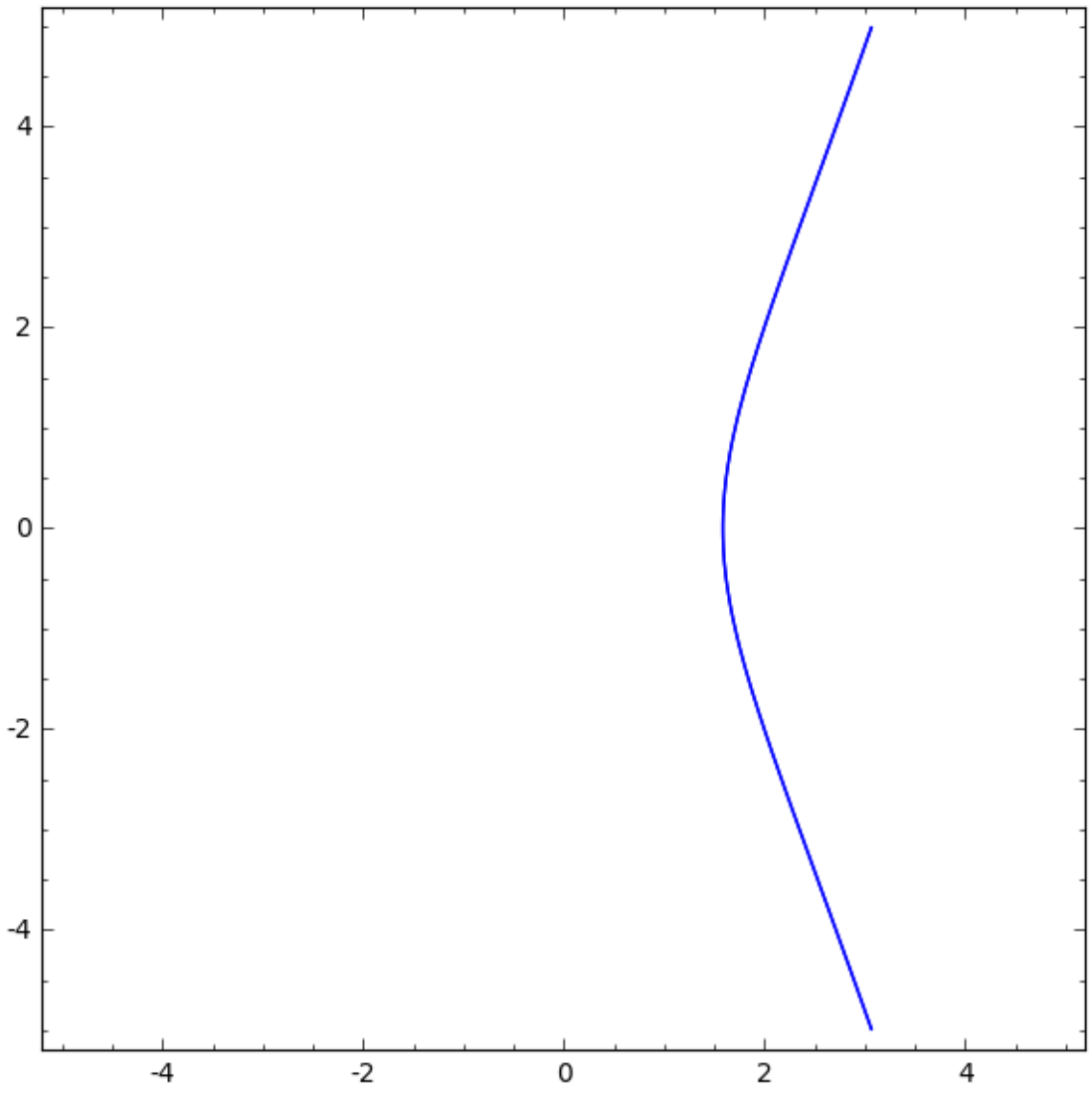

FIGURE 3 : $y^2 = x^3 - 4$

Dans la définition ci-dessus, l'adjectif lisse signifie que la courbe est... lisse. Les courbes suivantes, bien qu'elles soient définies par des équations de la forme $y^2 = x^3 + ax + b$, ne sont donc pas des courbes elliptiques.

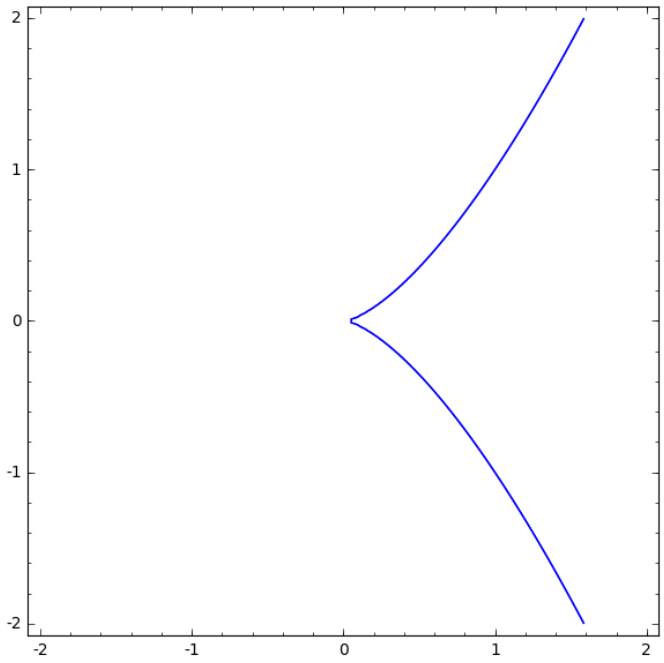

FIGURE 4 : $y^2 = x^3$

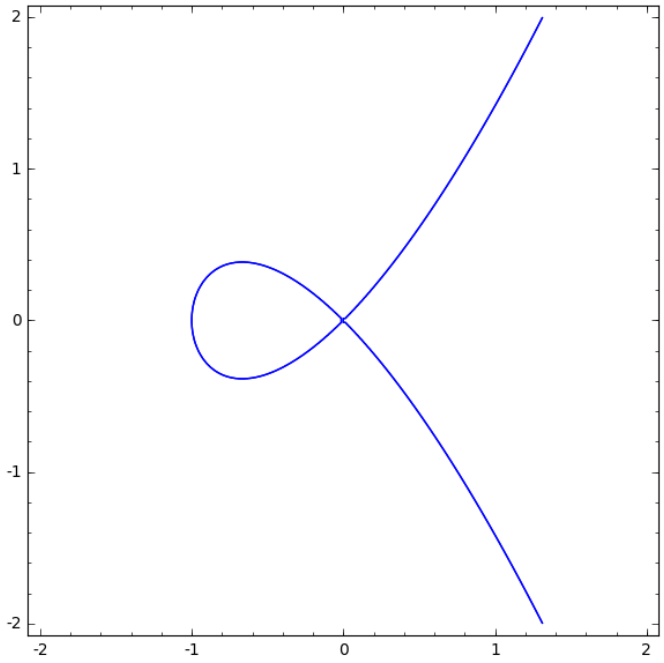

FIGURE 5 : $y^2 = x^2(x+1)$

Maintenant observons le fait suivant : si P_1 et P_2 sont deux points sur une courbe elliptique E, alors la droite (P_1P_2) recoupe la courbe en un troisième point et si P_1 et P_2 ont des coordonnées rationnelles, alors il en est de même du troisième point : en effet, l'équation que doit satisfaire l'abscisse de P_3 est de degré 3, à coefficients rationnels et

nous en connaissons déjà deux solutions rationnelles. Ceci est valable même si les deux points P_1, P_2 sont confondus ; auquel cas la droite (P_1P_2) est simplement la tangente en P_1. Nous avons vu que la droite (P_1P_2) recoupe la courbe en un troisième point, mais ce n'est pas tout à fait exact : un cas particulier est celui où les deux points sont symétriques l'un de l'autre par rapport à l'axe des abscisses, auquel cas on convient que la droite recoupe la courbe en un point à l'infini.

En 1922, Louis Mordell a démontré le théorème suivant.

Théorème 1. *Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique. Alors l'ensemble $E(\mathbb{Q})$ des points rationnels de E plus le point à l'infini et muni de la loi de composition interne décrite plus haut est un groupe commutatif de type fini.*

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}/n_i\mathbb{Z}$$

Par exemple, pour la courbe elliptique $E : y^2 = x^3 - x$, $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ (de générateurs $(0,1)$ et $(0,-1)$) ; pour $E : y^2 = x^3 + 1$, $E(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ (de générateur $(2,3)$) et pour $E : y^2 = x^3 - 4$, $E(\mathbb{Q}) \simeq \mathbb{Z}$ (de générateur $(2,2)$).

Se pose alors la question suivante : quelles sont les valeurs possibles de r et des n_i ci-dessus ?

3.3.2 Le dernier déguisement de la Grue blanche

Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique à coefficients dans $\mathbb{Z}$. On peut alors considérer l'équation définissant E comme définissant une courbe de $\mathbb{F}_q$ comme dans la deuxième saison et s'intéresser à

$$a_{p^s}(E) = p^s + 1 - \mid E(\mathbb{F}_{p^s}) \mid$$

qui est donc la différence entre le nombre de points de E et le nombre de point de la droite projective $\mathbb{P}^1(\mathbb{F}_{p^s})$. On pose

$$Z_{E,p}(u) = \exp\left(\sum_{n=1}^{\infty} a_{p^n} \frac{u^n}{n}\right).$$

Dans ce cas, on peut démontrer que

$$Z_{E,p}(u) = \begin{cases} \frac{1}{1-a_p(E)X+pX^2} & \text{pour presque tous les } p \\ \frac{1}{1-a_p(E)X} & \text{pour les autres.} \end{cases}$$

Enfin, on pose

$$L(E,s) = \prod_p Z_{E,p}(p^{-s}) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Il est facile de voir que ce produit infini converge pour $\Re s >> 0$ (par exemple $\Re s > 3/2$).

Bien entendu, on conjecture que nous avons affaire à un merveilleux kimono, c'est-à-dire que $L(E,s)$ admet un prolongement analytique à $\mathbb{C}$ tout entier satisfaisant une équation fonctionnelle, en l'occurrence une équation reliant $L(E,s)$ et $L(E,2-s)$.

L'une des conjectures les plus importantes de l'arithmétique contemporaine affirme que l'ordre d'annulation de $L(E,s)$ en $s = 1$ est exactement l'entier r tel que $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus G$.

3.4 L'envol de la Grue blanche ?

3.4.1 Le tableau des correspondances

	$\mathbb{Z}$	Courbes sur $\mathbb{F}_q$	$E/\mathbb{Q}$
Fonction	$\zeta(s)$	$Z(p^{-s})$	$L(E,s)$
Produit infini	$\prod_p \frac{1}{1-p^{-s}}$	$\prod_{x\in ZC} \frac{1}{1-p^{-s\deg x}}$	$\prod_p \frac{1}{1-a_p p^{-s}+p^{2-s}}$
Équation fonctionnelle	$\zeta(1-s)$	$\zeta(1-s)$	$L(E,2-s)$
Valeur spéciale	Unités et factorisation	Cycles	Points rationnels
Hypothèse de Riemann	$\Re s = 1/2$	$\Re s = 1/2$	$\Re s = 1$

Tous ces objets admettent un analogue dans un monde que l'on appelle le monde p-adique ; tout comme l'épouse admet un analogue dans le monde des oiseaux. Pour $\zeta_p(s)$ et $L_p(E,s)$, l'hypothèse de Riemann s'appelle la conjecture principale. Elle ne prend pas la forme "Tous les zéros de $\zeta_p(s)$ vérifie $\Re s = 1/2$" (bien sûr) mais "Les zéros de ζ_p et L_p sont exactement les zéros de $\mathscr{X}_p$ et $\mathscr{Y}_p$."

3.4.2 Chronologie partielle (et partiale)

1. En étudiant les points rationnels des courbes elliptiques $y^2 = x^3 - x$ et $y^2 = x^3 - 432$, Pierre de Fermat démontre vers 1637 que l'équation $x^n + y^n = z^n$ n'admet pas de solutions au sens de Diophante lorsque $n = 3$ ou 4.

2. En 1760, Leonhard Euler redémontre le cas $n = 3$ (première démonstration publiée).

3. En 1859, Bernhard Riemann montre le prolongement analytique et l'équation fonctionnelle de $\zeta(s)$.

4. Dans les années 1920 et 1930, Émile Artin, Helmut Hasse, Friedrich Karl Schmidt et André Weil formulent les premiers cas d'équation fonctionnelle et de prolongement analytique pour des fonctions zêtas provenant de la géométrie sur les corps finis.

5. Entre 1940 et 1948, André Weil démontre la conjecture concernant $Z(u)$ (la Grue blanche de la deuxième saison) pour les courbes et énonce des conjectures générales Il suggère aussi l'existence de ζ_p.

6. Entre 1960 et 1974, Bernard Dwork, Alexander Grothendieck et son école puis finalement Pierre Deligne démontrent toutes les conjectures de la deuxième saison. L'essentiel de ces travaux a été réalisé dans le bâtiment où vous vous trouvez. Ceci explique en particulier pourquoi vous vous trouvez actuellement dans le laboratoire Alexander Grothendieck.

7. En 1963, K.Iwasawa formule l'hypothèse de Riemann pour ζ_p.

8. En 1964, Tomio Kubota et Heinrich-Wolfgang Leopoldt construisent la fonction ζ_p.

9. En 1967, André Weil caractérise précisément l'équation fonctionnelle que doit vérifier $L(E,s)$ (dans la troisième saison) et fait remarquer que si cette conjecture est vraie, alors la fonction $L(E,s)$ est reliée à un objet appelé forme modulaire. On appelle courbe elliptique modulaire une courbe elliptique vérifiant les conditions de son travail.

10. En 1977, Barry Mazur a résolu le problème de la détermination des entiers n_i et m pouvant intervenir dans
$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}/n_i\mathbb{Z}.$$
L'essentiel de ce travail a eu lieu dans le bâtiment où vous vous trouvez.

11. En 1984, Barry Mazur et Andrew Wiles (pas André Weil) démontrent l'hypothèse de Riemann pour $\zeta_p(s)$.

12. En 1990, et en suivant des idées de Jean-Pierre Serre, Yves Hellegouarch et Gerhard Frey, Ken Ribet démontre que si $a^n + b^n = c^n$ est une solution de $x^n + y^n = z^n$ avec $n \geq 5$, alors la courbe elliptique
$$E : y^2 = x(x - a^n)(x + b^n)$$
n'est pas une courbe elliptique modulaire. L'essentiel de ce travail a été effectué ici.

13. En 1993, Kazuya Kato propose de représenter l'analogie entre ζ et ζ_p et $L(E, s)$ et $L_p(E, s)$ par le conte de la Grue blanche devenue femme.

14. En 1994, Andrew Wiles démontre que toutes les courbes elliptiques semi-stables sont modulaires. En particulier, leurs fonctions L admettent un prolongement analytique et vérifieent une équation fonctionnelle. Ceci termine la preuve du théorème de Fermat.

15. En 2001, Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor prouvent que toutes les courbes elliptiques sont modulaires. Christophe Breuil travaillait ici.

16. En 2004, Kazuya Kato démontrent que tous les zéros de $\mathscr{Y}_p$ sont des zéros de $L_p(f)$ si f est une forme modulaire (en particulier une courbe elliptique).

17. En 2014, Chris Skinner et Éric Urban démontrent que tous les zéros de $L_p(f)$ sont des zéros de $\mathscr{Y}_p$ si f est une forme modulaire ordinaire. Avec le résultat de Kato, ceci démontre l'hypothèse de Riemann p-adique pour les formes modulaires ordinaires.

18. En 2016, quelqu'un démontre l'hypothèse de Riemann p-adique pour les formes modulaires plates. Le travail n'a pas été effectué ici, mais au 425, et au moins la personne a l'avantage d'être dans la salle.

19. La conjecture prédisant que l'ordre d'annulation de $L(E, s)$ en $s = 0$ est le rang du groupe $E(\mathbb{Q})$ est encore ouverte ; elle a été choisie comme le problème 5 des 7 problèmes mathématiques les plus importants de ce millénaire.

20. La conjecture prédisant que les zéros de $\zeta(s)$ sont tous de parties réelles $1/2$ est encore ouverte ; elle a été choisie comme le premier problème des 7 problèmes mathématiques les plus importants de ce millénaire.

Au travail !

Olivier Fouquet
Département de Mathématiques, Bâtiment 425, Faculté des sciences d'Orsay Université Paris-Sud
E-mail address : olivier.fouquet@math.u-psud.fr
Telephone number : +33169155729
Fax number : +33169156019

Annexe

Transmission historique de l'*Arithmétique* :

1. Sur la pure base textuelle des références bibliographiques, l'*Arithmétique* est écrit au plus tôt juste avant l'ère commune, au plus tard au Vème siècle.

2. Le plus probable est que Diophante ait vécu au IIIème siècle ou avant mais les indices sont ténus. En particulier, le fait de le placer au IIIème siècle et non avant repose entièrement sur l'hypothèse qu'un livre est dédié à quelqu'un de vivant.

3. L'*Arithmétique* est connu et apparemment commentée par Theon et sa fille Hypatie (morte en 415EC).

4. L'*Arithmétique* est traduite du Grec à l'Arabe à Bagdad au Xème siècle dans le cadre du mouvement de traductions des sciences mondiales. Quatre des treize livres nous proviennent de cette traduction via une copie de la bibliothèque de Meshed, en Iran, datant de 1198EC.

5. D'autres copies sont étudiés à Byzance entre le XIème et le XIIIème siècle.

6. Une telle copie grecque de six des treize livres est découverte à Venise en 1463 par Regiomontanus.

7. Les premières traductions latines européennes répertoriées, due à Rafael Bombelli et Wilhelm Holzmann *Xylander*, datent de 1572 et 1575.

8. En 1621, Bachet de Méziriac traduit Diophante en Latin à Paris. C'est cette copie que Fermat acquiert vers 1630.