La conjecture de Fermat

La connaissance est le patrimoine de l'humanité, donc chaque être humain peut l'utiliser librement mais il a aussi le devoir de le protéger, partager, améliorer.

Morphocode CODE

Titre: La conjecture de Fermat

Auteur: Morphocode CODE

Site web: https://fan2cube.fr

Version: 15.12-23.9.13

ISBN **:** 979-8-4483-0839-0

Préface

L'histoire de la conjecture de Fermat est vraiment extraordinaire, poétique, passionnante ... tant de mathématiciens, et d'amateurs ... ont cherché pendant 358 ans !!!

Finalement la résolution ne se fait qu'en 1994 par Andrew Wiles.

1 INTRODUCTION

Vers 1636, Fermat émit l'énoncé suivante :

"L'équation :

L_n : $x^n + y^n = z^n$

n'a pas de solutions en entiers naturels non nuls x,y,z , dès que $n \geq 3$.

Et j'ai trouvé une merveilleuse démonstration mais cette marge est trop étroite pour en contenir ..."

Nous appelons cette assertion : "la conjecture de Fermat" puisqu'on n'a pas trouvé la démonstration de Fermat. Traditionnellement on l'appelle "le dernier théorème de Fermat".

Depuis ce jour, tout le monde essaie de démontrer cette conjecture ... mais il fallait attendre jusqu' au 1994 pour que cette conjecture soit démontrée par Andrew Wiles.

Avec les techniques que Wiles utilise pour démontrer cette conjecture, on pense que Fermat s'est trompé dans sa démonstration, autrement dit Fermat n'ai pas réellement démontré cette assertion, donc c'est une conjecture plutôt qu'un théorème, et puis depuis 358 ans personne n'a trouvé une démonstration "simple" pour cette conjecture alors probablement Fermat non plus.

2 LA GENÈSE DE LA CONJECTURE DE FERMAT

2.1 L'ARITHMÉTIQUE DANS UN ANNEAU

Soit A un anneau, pour nous c'est un anneau intègre, unitaire et commutatif.

On note A^x l'ensemble des éléments inversibles de A

$A^x = \{\alpha \in A \ / \ \exists \beta \in A \ \ \alpha\beta = 1\}$

on dit aussi les unités de A.

Définition divise : Soient $\alpha, \beta \in A$ on dit que α divise β et on note $\alpha | \beta$ s'il existe un $\kappa \in A$ tel que $\kappa\alpha = \beta$. On dit aussi :

→ α est un diviseur de β,

→ β est un multiple de α

→ β est divisible par α

On écrit aussi :

$\beta = 0 \pmod{\alpha}$

Propriétés :

¤ $\alpha|\beta \Rightarrow x\alpha|x\beta \quad ,x\in A$

¤ $\left.\begin{matrix}\alpha|\beta\\ \alpha|\gamma\end{matrix}\right\} \Rightarrow \alpha|(x\beta + y\gamma) \quad , x, y \in A$

Définition diviseur commun : Soient $\alpha,\beta \in A$ on dit que δ est un diviseur commun de α et β si :

$\delta|\alpha$ et $\delta|\beta$

Définition premiers entre eux : Soient $\alpha,\beta \in A$ on dit que α et β sont premiers entre eux si :

$\forall\delta\in A,\ \delta|\alpha$ et $\delta|\beta \ \Rightarrow \delta\in A^x$

autrement dit, les diviseurs communs de α et β sont des unités.

Définition pgcd : Soient $\alpha,\beta \in A$, le $\text{pgcd}(\alpha,\beta)=\delta$ est le plus grand diviseur commun de α et β, càd

$\delta|\alpha$ et $\delta|\beta$

et si $\delta'|\alpha$ et $\delta'|\beta \Rightarrow \delta'|\delta$

On note $\text{pgcd}(\alpha,\beta)=(\alpha,\beta)$

Définition ppcm : Soient $\alpha,\beta \in A$, le $\text{ppcm}(\alpha,\beta)=\mu$ est le plus petit commun multiple de α et β, càd

$\alpha|\mu$ et $\beta|\mu$

et si $\alpha|\mu'$ et $\beta|\mu' \Rightarrow \mu|\mu'$

Note : Le pgcd et le ppcm n'existent pas toujours, puisqu'il s'agit de l'existence d'un plus grand ou d'un plus petit élément d'un ensemble.

Définition associé : Soient $\alpha,\beta \in A$ on dit que α et β sont associés s'il existe un $\varepsilon \in A^x$ tel que $\alpha = \varepsilon\beta$.

¤ $\alpha|\beta$ et $\beta|\alpha \Rightarrow \alpha = \varepsilon\beta$, ε=unité

Définition irréductible : Soit $\eta \in A^*$ et $\eta \notin A^x$, on dit que η est irréductible si :

$\eta = \alpha\beta \Rightarrow \alpha \in A^x$ ou $\beta \in A^x$

autrement dit, les diviseurs de η sont des unités ou des associés de η.

Définition premier : Soit $\rho \in A^*$ et $\rho \notin A^x$, on dit que ρ est premier si :

$\rho|\alpha\beta \Rightarrow \rho|\alpha$ ou $\rho|\beta$ (lemme d'Euclide)

Propriété : premier ⇒ irréductible

Démonstration : On prend un ρ premier $\neq 0$, et on a:

$\rho=\alpha\beta$, il faut montrer que α ou β sont des unités.

allons-y:

$\rho=\alpha\beta \Rightarrow 1.\rho=\alpha\beta \Rightarrow \rho|\alpha\beta$ comme ρ est premier on a par ex $\rho|\alpha$. Or on a aussi $\alpha|\rho$ d'où

$\alpha=\varepsilon\rho$, ε=unité

$\rho=\alpha\beta=\varepsilon\rho\beta \Rightarrow \rho=\varepsilon\rho\beta \Rightarrow \rho(1-\varepsilon\beta)=0$ comme A est intègre $\Rightarrow$ $1-\varepsilon\beta = 0 \Rightarrow \varepsilon\beta=1 \Rightarrow \beta$ est une unité.

On fait de même pour $\rho|\beta \Rightarrow \alpha$ est une unité.

donc ρ est bien irréductible.

Définition anneau factoriel : Soit A un anneau, on dit que A est factoriel si :

Tout élément α non-nul de A se décompose de façon unique en produit des éléments irréductibles.

$\alpha = \varepsilon\eta_1\eta_2 \dots \eta_n$

ε=unité, η_i=irréductible.

Unique signifie:

$\alpha = \varepsilon\eta_1\eta_2 \dots \eta_n = \mu\eta_1\eta_2 \dots \eta_n$

ε,μ unités .

ou bien avec une deuxième décomposition

$\alpha = \mu\xi_1\xi_2\xi_3 \dots \xi_m$

alors on a:

1) m=n , même longueur

2) Les ξ_i sont des associés de η_i : $\xi_i = \mu_i\eta_i$, μ_i=unité.

Propriétés :

¤ Dans un anneau factoriel : irréductible $\Leftrightarrow$ premier.

On a déjà

premier ⇒ irréductible.

premier ⇐ irréductible ??

Soient :

$\alpha = \varepsilon\eta_1\eta_2$; ε=unité, η_i=irréductible

$\beta = \mu\xi_1\xi_2\xi_3$; μ=unité, ξ_i=irréductible

γ = irréductible

$\gamma|\alpha\beta \Rightarrow \gamma$ est l'un des η_i ou l'un des ξ_i donc

$\gamma|\alpha$ ou $\gamma|\beta$ càd γ est premier.

¤ Le pgcd existe : pgcd(α,β) existe

2.2 LES IDÉAUX

Définition idéal : Soit I⊂A , on dit que I est un idéal si :

1) 0∈I

2) ∀a,b ∈I ⇒ a+b ∈I , stabilité

3) ∀α∈A, ∀a ∈I ⇒ αa ∈I , propriété absorbante

On note 𝕀 l'ensemble des idéaux de A.

L'idéal engendré par un élément α∈A :

$\langle\alpha\rangle = \{x=\kappa\alpha$, avec $\kappa\in A\}$

$\langle\alpha\rangle$ se nomme idéal principal.

L'idéal engendré par n éléments $\alpha_1, \alpha_2, \dots, \alpha_n \in A$:

$\langle\alpha_1, \alpha_2, \dots, \alpha_n\rangle = \{x = \kappa_1\alpha_1 + \kappa_2\alpha_2 + \dots + \kappa_n\alpha_n \text{ , avec } \underline{\kappa_i \in A}\}$

Si $I = \langle\alpha_1, \alpha_2, \dots, \alpha_n\rangle$ on dira que I est de type fini. Dans un anneau A où tout idéal est de type fini, on dira que l'anneau A est noethérien.

et

$\langle\alpha\rangle = \langle\beta\rangle \Leftrightarrow \alpha = \varepsilon\beta$ où ε est une unité

<u>Le radical d'un idéal</u> :

Soit I un idéal, le radical $\sqrt{I}$ de I est défini par:

$\sqrt{I} = \{x \,/ \exists n \in \mathbb{N}\ x^n \in I\}$

En effet $\sqrt{I}$ c'est bien un idéal :

$0^1 = 0 \in I \Rightarrow 0 \in \sqrt{I}$

$\alpha \in \sqrt{I}$ et $\beta \in \sqrt{I} \Rightarrow \alpha + \beta \in \sqrt{I}$?

$\alpha \in \sqrt{I} \Rightarrow \alpha^n \in I$

$\beta \in \sqrt{I} \Rightarrow \beta^m \in I$

$$(\alpha + \beta)^{n+m} = \sum_{h=0}^{n+m} \binom{n+m}{h} \alpha^h \beta^{n+m-h}$$

$\rightarrow$ Si $n \leq h \Rightarrow \left(\alpha^{h-n}\beta^{n+m-h}\right)\alpha^n = \xi\alpha^n \in I$ (propriété absorbante)

$\rightarrow$ Si $n > h \Rightarrow \left(\alpha^n\beta^{n-h}\right)\beta^m = \xi\beta^n \in I$ (propriété absorbante)

$(\alpha+\beta)^{n+m} \in I \Rightarrow \alpha+\beta \in \sqrt{I}$

d'autre part:

$\alpha^n \in I \Rightarrow \xi^n\alpha^n \in I \Rightarrow (\xi\alpha)^n \in I \Rightarrow \xi\alpha \in \sqrt{I}$

$\sqrt{I}$ est bien un idéal.

Somme des idéaux :

$I+J = \{x=a+b \text{ avec } a \in I,\ b \in J\}$

Produit des idéaux :

$$IJ = \{x = \sum_i a_i b_i \quad \text{avec } a_i \in I,\ b_i \in J\}$$

en particulier

$I = \langle \alpha_1, \alpha_2 \rangle$

$J = \langle \beta_1, \beta_2 \rangle$

$I+J = \langle \alpha_1, \alpha_2, \beta_1, \beta_2 \rangle$

$IJ = \langle \alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2 \rangle$

$\langle \alpha \rangle + \langle \beta \rangle = \langle \alpha, \beta \rangle$

$\langle \alpha \rangle \langle \beta \rangle = \langle \alpha\beta \rangle$

Remarques importantes :

($\mathbb{I}$,+) n'est pas un groupe, c'est simplement un monoïde d'élément neutre $\langle 0\rangle$, seul l'idéal $\langle 0\rangle$ possède un opposé donc l'écriture -I n'a pas de sens ! par contre l'écriture $-\langle\alpha\rangle$ n'est rien d'autre que $\langle -\alpha\rangle = \langle\alpha\rangle$.

De même ($\mathbb{I}$, .) n'et pas un groupe non plus, lui aussi c'est un monoïde d'élément neutre $\langle 1\rangle$, l'écriture I^{-1} ni $\langle\alpha\rangle^{-1}$ elle non plus n'a pas de sens !!

Modulo par un élément γ ou par un idéal I :

Soit $\alpha, \beta, \gamma \in A$ et I un idéal,

$\rightarrow \alpha = \beta \pmod{\gamma} \overset{\text{déf}}{\Leftrightarrow} \exists \kappa \in A$ tel que $\alpha - \beta = \kappa\gamma$

$\rightarrow \alpha = \beta \pmod{I} \overset{\text{déf}}{\Leftrightarrow} (\alpha - \beta) \in I$

on note aussi :

$\alpha = \beta \pmod{\gamma} \Leftrightarrow \alpha = \beta \pmod{\gamma A} \Leftrightarrow \alpha = \beta \pmod{\langle\gamma\rangle}$

$\rightarrow \alpha | \beta$ (dans A) $\overset{\text{déf}}{\Leftrightarrow} \exists \kappa \in A$ tel que $\beta = \kappa\alpha$

$\Leftrightarrow \beta = 0 \pmod{\alpha}$

Définition anneau principal : Soit A un anneau, on dit que A est principal si tout idéal est principal.

$\forall$I idéal $\Rightarrow \exists \alpha \in A$ tel que $I = \langle\alpha\rangle$

Définition anneau euclidien : Soit A un anneau, on dit que A est euclidien si :

1) Il existe une division euclidienne $\psi: A \to \mathbb{N}$

2) $\forall(\alpha,\beta)\in AxA^*$, il existe $(\kappa,\varkappa)\in A^2$ tel que

$\alpha = \kappa\beta + \varkappa$, $\varkappa=0$ ou $\psi(\varkappa) < \psi(\beta)$

Si A est euclidienne alors on a l'identité de Bézout:

Si α et $\beta \in A$ premiers entre eux, alors il existe $\kappa,\varkappa \in A$ tels que

$\kappa\alpha + \varkappa\beta = 1$

Propriété : euclidien ⇒ principal ⇒ factoriel

Définition divise : Soient $I,J \in \mathbb{I}$ on dit que I divise J et on note I|J s'il existe un $K\in\mathbb{I}$ tel que $KI = J$.

Note on a: I|J ⇒ J⊂I

Définition pgcd : Soient $I,J \in \mathbb{I}$ on dit que D=pgcd(I,J)=(I,J) si:

1) D|I et D|J

2) D'|I et D'|J ⇒ D'|D

D=pgcd(I,J) = plus grand commun diviseur de I,J.

Propriété :

¤ pgcd(I,J) = I+J

On dit que I, J sont premiers entre eux si $D=pgcd(I,J)=\langle 1\rangle$

Soient $\alpha,\beta \in A$ et un idéal I, on définit la relation d'équivalence $\sim$ par :

$\alpha \sim \beta \Leftrightarrow \alpha-\beta \in I$ ou note encore $\alpha = \beta \pmod I$

On note $A/\sim$ ou A/I la classe d'équivalence de $\sim$.

Définition idéal premier : Soit $P \in \mathbb{I}^*$ et $P \neq A$, on dit que P est premier si :

¤ A/P est intègre. $\Leftrightarrow$

¤ $\alpha\beta \in P \Rightarrow \alpha \in P$ ou $\beta \in P$. $\Leftrightarrow$

¤ $\forall I, I|P \Rightarrow I=P$ ou $I=A$

2.3 ANNEAU DES ENTIERS

Soit $\mathbb{K}=\mathbb{Q}(\xi)$, un corps de nombres de degré d (ξ=nombre algébrique de degré d)

$$\mathbb{K} = \mathbb{Q}(\xi) = \{x = a_0 + a_1\xi + \cdots + a_{d-1}\xi^{d-1} \; ; \; a_i \in \mathbb{Q}\}$$

et $\overline{\mathbb{Z}}_{\mathbb{K}}$ l'anneau des entiers de $\mathbb{K}$ càd:

$$\overline{\mathbb{Z}}_{\mathbb{K}} = \overline{\mathbb{Z}} \cap \mathbb{K}$$

où $\overline{\mathbb{Z}}$ = les entiers algébriques.

Exemples :
¤ $\xi^2 = d \in \mathbb{Z}$ avec $d \neq 0,1$ et sans facteur carré.

$$\overline{\mathbb{Z}}_{\mathbb{K}} = \begin{cases} \mathbb{Z}[\sqrt{d}] \text{ si } d = 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \text{ si } d = 1 \pmod 4 \end{cases}$$

anneau quadratique.

¤ $\xi^3 = 1 \Rightarrow \overline{\mathbb{Z}}_{\mathbb{K}} = \mathbb{Z}[\xi]$ anneau d'Eisenstein

¤ $\xi^n = 1 \Rightarrow \overline{\mathbb{Z}}_{\mathbb{K}} = \mathbb{Z}[\xi]$ anneau cyclotomique

2.4 ANNEAU DES ENTIERS D'EISENSTEIN

On pose

$\varrho = e^{\frac{2\pi}{3}i} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ et on a: $\varrho^3 = 1$

le corps $\mathbb{K}$ engendré par $\mathbb{Q}$ et ϱ

$\mathbb{K} = \mathbb{Q}(\varrho) = \{\alpha = a + b\varrho \in \mathbb{C} \ / \ a,b \in \mathbb{Q}\}$

l'anneau des entiers de $\mathbb{K}=\mathbb{Q}(\varrho)$

$\overline{\mathbb{Z}}_{\mathbb{K}} = \mathbb{K} \cap \overline{\mathbb{Z}}$

$\overline{\mathbb{Z}}_{\mathbb{K}} = \mathbb{Z}[\varrho] = \{\alpha = a + b\varrho \in \mathbb{C} \ / \ a,b \in \mathbb{Z}\}$

Cet anneau s'appelle l'anneau des entiers d'Eisenstein, il contient l'anneau $\mathbb{Z}[i\sqrt{3}] \subset \overline{\mathbb{Z}}_{\mathbb{K}}$

$\mathbb{Z}[i\sqrt{3}] = \{\alpha = a + bi\sqrt{3} \in \mathbb{C} \ / \ a,b \in \mathbb{Z}\}$

$\mathbb{Z}[i\sqrt{3}] \subset \mathbb{Z}[\varrho]$

On va regarder les propriétés de cet anneau $\mathbb{Z}[\varrho]$.

Les corps $\mathbb{Q}(\zeta)$ avec $\zeta = e^{\frac{2\pi}{n}i}$, $\zeta^n = 1$, s'appelle les corps cyclotomiques, et l'anneau des entiers de $\mathbb{Q}(\zeta)$, les anneaux cyclotomiques $\mathbb{Z}[\zeta]$.

2.5 PROPRIÉTÉS DE $\mathbb{Z}[P]$

<u>La norme de $\mathbb{Z}[\varrho]$</u>

$N : \mathbb{Z}[\varrho] \to \mathbb{Z}$

$\alpha \to N(\alpha)$

$\alpha = a+b\varrho$ où $a,b \in \mathbb{Z}$

$$\alpha = a + b\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \left(a - \frac{b}{2}\right) + \frac{\sqrt{3}b}{2}i$$

$$\overline{\alpha} = \left(a - \frac{b}{2}\right) - \frac{\sqrt{3}b}{2}i$$

$N(\alpha) = \alpha\overline{\alpha}$

$N(a+b\varrho) = a^2 - ab + b^2 \in \mathbb{Z}$

on a :

$N(\alpha\beta) = N(\alpha)N(\beta)$

Avec cette norme, $\mathbb{Z}[\varrho]$ est euclidien ($\psi(\alpha) = |N(\alpha)|$), donc factoriel.

Les unités de $\mathbb{Z}[\varrho]$ sont :

$\mathbb{Z}[\varrho]^x = \{\pm 1, \pm\varrho, \pm\varrho^2\}$ et si μ est une unité alors $\mu^6 = 1$

Comme $\mathbb{Z}[\varrho]$ est factoriel, on a le théorème de décomposition suivante:

Théorème de décomposition unique :

$\forall\alpha$ non-nul, non-inversible $\in\mathbb{Z}[\varrho]$, il existe une décomposition unique de la forme :

$\alpha = \mu\rho_1\rho_2 \dots \rho_n$

où les ρ_i premiers (=irréductibles) et μ=une unité

Unique signifie :

Si α admet une deuxième décomposition, on aura :

$$\begin{cases} \alpha = \mu\rho_1\rho_2 \dots \rho_n \\ \alpha = \nu\tau_1\tau_2\tau_3 \dots \tau_m \end{cases}$$

n=m même longueur

$\tau_i = \nu_i\rho_i$ où ν_i=unité

ce qui donne donc

$\alpha = \mu\rho_1\rho_2 \dots \rho_n = \varepsilon\rho_1\rho_2 \dots \rho_n$; μ,ε unités

(2.5.1) Théorème :

$\alpha, \beta, \gamma \in \mathbb{Z}[\varrho]$

$$\begin{cases} \alpha\beta = \gamma^3 \\ (\alpha, \beta) = 1 \end{cases} \Rightarrow \begin{cases} \alpha = \mu\tau^3 \\ \beta = \nu\theta^3 \end{cases} \quad \text{où} \quad \begin{cases} \tau, \theta \in \mathbb{Z}[\varrho] \\ \mu, \nu \text{ unités } \in \mathbb{Z}[\varrho]^x \end{cases}$$

Démonstration :

La décomposition de α est de la forme:

$$\alpha = \varepsilon_1 \prod_i \rho_i^{k_i}$$

$$\beta = \varepsilon_2 \prod_i \tau_i^{m_i}$$

$$\gamma^3 = \varepsilon_3 \prod_i \eta_i^{3l_i}$$

$$\varepsilon_1\varepsilon_2 \prod_i \rho_i^{k_i}\tau_i^{m_i} = \varepsilon_3 \prod_i \eta_i^{3l_i}$$

Comme α et β sont premiers entre eux $(\alpha,\beta)=1$ les ρ_i et les τ_i sont différents (ils ne sont pas entremêlés) donc on retrouve les $\rho_i^{k_i}$ parmi les $\eta_i^{3l_i}$ autrement dit on a

$$\alpha = \mu \prod_i \eta_i^{3l_i} = \mu\tau^3$$

de même on retrouve les $\tau_i^{m_i}$ parmi les $\eta_i^{3l_i}$ restant :

$$\beta = \nu \prod_{j=\text{restant}} \eta_j^{3l_j} = \nu\theta^3$$

$\varepsilon_1, \varepsilon_2, \varepsilon_3, \mu, \nu$ les unités

(2.5.2) Théorème :

$\forall \alpha \in \mathbb{Z}[\varrho], \exists \mu = \text{unité} \in \mathbb{Z}[\varrho]^x , \exists \theta \in \mathbb{Z}[i\sqrt{3}]$ tels que

$\mu\alpha = \theta$

$\mu\alpha = u+vi\sqrt{3}$ où $u,v \in \mathbb{Z}$

Démonstration :

On pose

$$\xi = \frac{1 + i\sqrt{3}}{2}$$

$\varrho+1=\xi$

donc $\mathbb{Z}[\varrho] = \mathbb{Z}[\xi]$, et un élément de $\alpha \in \mathbb{Z}[\varrho]$ s'écrit :

$$\alpha = \frac{a + bi\sqrt{3}}{2}$$ avec a, b la même parité

Si a et b sont pairs , il n'y a aucun problème $\alpha = 1.\alpha \in \mathbb{Z}[i\sqrt{3}]$

Voyons ce qui se passe quand a et b sont impairs

$$a=2k+1 \Rightarrow \begin{cases} 2(2m) + 1 = 4m + 1 \\ 2(2m + 1) + 1 = 4m + 3 \end{cases}$$

$a = 1, -1 \pmod 4$

de même pour b

b = 1,-1 (mod 4)

il y a donc quatre cas à étudier :

→ cas1: a=1 (mod 4) , b=-1 (mod 4)

$$\left(\frac{1+i\sqrt{3}}{2}\right)\left(\frac{a+bi\sqrt{3}}{2}\right)=\frac{1}{4}\left((a-3b)+(a+b)i\sqrt{3}\right)$$

comme a=1 (mod 4) et b=-1 (mod 4) ça donne

a-3b=0 (mod 4)

a+b=0 (mod 4)

donc

$$\left(\frac{1+i\sqrt{3}}{2}\right)\left(\frac{a+bi\sqrt{3}}{2}\right)=\theta_1=u+vi\sqrt{3}\in\mathbb{Z}\left[i\sqrt{3}\right]\ ;u,v\in\mathbb{Z}$$

$$e^{\frac{\pi}{3}i}\left(\frac{a+bi\sqrt{3}}{2}\right)=\theta_1\in\mathbb{Z}\left[i\sqrt{3}\right]$$

→ cas2: a=-1 (mod 4) , b=1 (mod 4) ⇒

(-a)=1 (mod 4) , (-b)=-1 (mod 4)

$$e^{\frac{\pi}{3}i}\left(\frac{(-a)+(-b)i\sqrt{3}}{2}\right)=\theta_2\in\mathbb{Z}\left[i\sqrt{3}\right]$$

$$e^{\frac{\pi}{3}i}\left(\frac{(-a)+(-b)i\sqrt{3}}{2}\right)=e^{\frac{\pi}{3}i}\left(-\frac{a+bi\sqrt{3}}{2}\right)$$

$$=e^{\pi i}e^{\frac{\pi}{3}i}\left(\frac{a+bi\sqrt{3}}{2}\right)=e^{\frac{4\pi}{3}i}\left(\frac{a+bi\sqrt{3}}{2}\right)$$

$e^{\frac{4\pi}{3}i}\left(\frac{a+bi\sqrt{3}}{2}\right)=\theta_2\in\mathbb{Z}[i\sqrt{3}]\rightarrow$ cas3: a=-1 (mod 4) , b=-1 (mod 4) ⇒

(-a)=1 (mod 4) , b=-1 (mod 4)

$$e^{\frac{\pi}{3}i}\left(\frac{(-a)+bi\sqrt{3}}{2}\right)=\theta_3\in\mathbb{Z}[i\sqrt{3}]$$

$$e^{\frac{\pi}{3}i}\left(-\frac{a-bi\sqrt{3}}{2}\right)=e^{\pi i}e^{\frac{\pi}{3}i}\left(\frac{a-bi\sqrt{3}}{2}\right)=e^{-\frac{2\pi}{3}i}\left(\frac{a-bi\sqrt{3}}{2}\right)$$

$$e^{\frac{2\pi}{3}i}\left(\frac{a+bi\sqrt{3}}{2}\right)=\overline{\theta}_3\in\mathbb{Z}[i\sqrt{3}]$$

→ cas4: a=1 (mod 4) , b=1 (mod 4) ⇒

(-a)=-1 (mod 4) , (-b)=-1 (mod 4)

$$e^{\frac{2\pi}{3}i}\left(\frac{(-a)+(-b)i\sqrt{3}}{2}\right)=\theta_4\in\mathbb{Z}[i\sqrt{3}]$$

$$e^{\frac{2\pi}{3}i}\left(\frac{(-a)+(-b)i\sqrt{3}}{2}\right)=e^{\frac{5\pi}{3}i}\left(\frac{a+bi\sqrt{3}}{2}\right)$$

$$=e^{-\frac{\pi}{3}i}\left(\frac{a+bi\sqrt{3}}{2}\right)$$

$$e^{-\frac{\pi}{3}i}\left(\frac{a+bi\sqrt{3}}{2}\right)=\theta_4\in\mathbb{Z}[i\sqrt{3}]$$

(2.5.3) Théorème :

$$\begin{cases} a^2+3b^2=c^3 \\ abc\neq 0 \\ (a,b)=1 \\ a,b \text{ parités différentes} \end{cases}$$

alors il existe u,v $\in\mathbb{Z}$ et (u,v)=1 tels que :

$$a+bi\sqrt{3}=\left(u+vi\sqrt{3}\right)^3 \quad \text{où } u,v\in\mathbb{Z} \text{ et } (u,v)=1$$

Démonstration :

$a^2+3b^2=c^3$

On va se décomposer dans $\mathbb{Z}[\varrho]$

$$\left(a+bi\sqrt{3}\right)\left(a-bi\sqrt{3}\right)=c^3$$

Montrons que $\left(a+bi\sqrt{3}\right),\left(a-bi\sqrt{3}\right)$ sont premiers entre eux.

Soit τ un diviseur premier de $\left(a+bi\sqrt{3}\right)$ et $\left(a-bi\sqrt{3}\right)$ donc τ divise la somme

$\tau|2a \Rightarrow N(\tau)|4a^2$

$\tau|\left(a+bi\sqrt{3}\right) \Rightarrow N(\tau)|N\left(a+bi\sqrt{3}\right) \Rightarrow N(\tau)|(a^2+3b^2)$

$N(\tau)|(a^2+3b^2) \Rightarrow$ $N(\tau)$=impair car (a^2+3b^2)=impair (car a,b parités différentes)

$N(\tau)|4a^2$, $N(\tau)$=impair $\Rightarrow N(\tau)|a^2$

$$\left.\begin{matrix} N(\tau)|a^2 \\ N(\tau)|(a^2+3b^2) \end{matrix}\right\} \Rightarrow \text{impossible car } (a^2, a^2+3b^2) = 1$$

en effet, raisonnons à l'envers , Bézout donne :

$xa^2 + y(a^2 + 3b^2) = 1$

$(xa + ya)a + (3yb)b = 1$

$u = xa + ya$

$v = 3yb$

$y = v/3b$

$x = u/a - v/3b$

ainsi comme a,b premier entre eux on a

$ua + vb = 1$

il suffit de prendre

$x = u/a - v/3b$

$y = v/3b$

on aura

$xa^2 + y(a^2 + 3b^2) = 1$

Conclusion $(a + bi\sqrt{3}), (a - bi\sqrt{3})$ sont premiers entre eux.

D'après le théorème (2.5.1)

$\left(a + bi\sqrt{3}\right) = \varepsilon\tau^3$, $\varepsilon =$ unité, $\tau \in \mathbb{Z}[\varrho]$

Mais d'après le théorème (2.5.2) , il existe une unité ν telle que:

$\nu\tau = \theta \in \mathbb{Z}[i\sqrt{3}]$, ν=unité

comme $\nu^6=1$ (on a de la chance !) d'où

$\left(a + bi\sqrt{3}\right) = \varepsilon\nu^6\tau^3 = \varepsilon\nu^3(\nu\tau)^3 = \mu\theta^3$; μ=unité

Il faut maintenant examiner toutes les unités de $\mathbb{Z}[\varrho]$

$\mu \in \{\pm 1, \pm\varrho, \pm\varrho^2\}$

comme $-1 = (-1)^3$ il suffit de regarder seulement $\mu \in \{1, \varrho, \varrho^2\}$

allons-y :

$\rightarrow \mu = 1$

$\left(a + bi\sqrt{3}\right) = (u + vi\sqrt{3})^3$

OK pas de problème et on a:

$a = u(u - 3v)(u + 3v)$

$b = 3v(u - v)(u + v)$

et $(a,b) = 1 \Rightarrow (u,v) = 1$.

$\rightarrow \mu = \varrho$

$\left(a + bi\sqrt{3}\right) = \varrho(u + vi\sqrt{3})^3$

$$\overline{\varrho}\left(a + bi\sqrt{3}\right) = (u + vi\sqrt{3})^3$$

$$\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(a + bi\sqrt{3}\right) = (u + vi\sqrt{3})^3$$

$$\left(\frac{3b - a}{2}\right) - \left(\frac{a + b}{2}\right)i\sqrt{3} = (u + vi\sqrt{3})^3$$

ce qui montre que

-(a + b) = 6v(u - v)(u + v)

ce qui est impossible car a,b de parités différentes

$\rightarrow \mu = \varrho^2$

$$\left(a + bi\sqrt{3}\right) = \varrho^2(u + vi\sqrt{3})^3$$

$$\overline{\varrho}^2\left(a + bi\sqrt{3}\right) = (u + vi\sqrt{3})^3$$

$$\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\left(a + bi\sqrt{3}\right) = (u + vi\sqrt{3})^3$$

$$-\left(\frac{3b + a}{2}\right) + \left(\frac{a - b}{2}\right)i\sqrt{3} = \left(u + vi\sqrt{3}\right)^3$$

là aussi ça donne

(a - b) = 6v(u - v)(u + v)
ce qui est impossible car a,b sont de parités différentes
Finalement le seul cas valable est μ=1

2.6 LA DESCENTE INFINIE

La descente infinie est inventée par Fermat, elle sert à démontrer quelque chose qui n'existe pas !

Pennons par exemple, on a une équation à 2 variables f(x,y) = 0, et on veut montrer qu'il n'existe pas de solutions non-nulles dans $\mathbb{Z}$ par ex, càd il n'existe pas de couples $(a,b)\in\mathbb{Z}^2$, $ab\neq 0$ tels que f(a,b)=0.

à chaque solution (a,b) on associe un paramètre $\vartheta\in\mathbb{N}^*$, et on dit que la solution (a',b') est plus "petite" que la solution (a,b) ça signifie simplement $\vartheta'<\vartheta$.

¤ On suppose donc que l'équation f(x,y)=0 admet une solution non-nulle (a,b), et on se débrouille pour trouver une autre solution (a',b') qui est plus petite que (a,b), puis une autre (a'',b'') plus petite que (a',b') ... etc .... on aura donc

$\ldots < \vartheta'' < \vartheta' < \vartheta$

mais on ne peut pas descendre infiniment car il y a un nombre fini des entiers naturels entre 0 et ϑ. Donc la solution (a,b) n'existe pas !

Exemple :

$\sqrt{3}$ n'est pas rationnel, càd l'équation :

$x^2 - 3y^2 = 0$

n'a pas de solution non-nulle dans $\mathbb{N}^2$.

Supposons que l'équation admet une solution non-nulle $(a,b)\in\mathbb{N}^2$, on a alors :

$a^2 - 3b^2 = 0$

$a^2 = 3b^2 \Rightarrow$

$3|a^2 \Rightarrow 3|a$ (car 3=premier) $\Rightarrow a = 3a' \Rightarrow a^2 = 9a'^2$

$9a'^2 = 3b^2 \Rightarrow 3a'^2 = b^2 \Rightarrow 3|b^2 \Rightarrow 3|b \Rightarrow 3b' = b$

d'où

$a'^2 = 3b'^2$

$a'^2 - 3b'^2 = 0$

Ici on prend $\vartheta=a$

ça y est on a trouvé une autre solution (a',b') plus petite que (a,b), car $\vartheta'=a'<\vartheta=a$ et la descente infinie nous dit qu'une telle solution (a,b) n'existe pas, donc $\sqrt{3}$ n'est pas rationnel.

Remarque le même raisonnement peut être appliqué pour un nombre premier p, autrement dit $\sqrt{p}$ n'est pas rationnel.

On peut utiliser la descente infinie une autre façon.

¤ On suppose que l'équation f(x,y)=0 admet des solutions non-nulles dans $\mathbb{Z}^2$, parmi ces solutions on prend la plus petite (a,b) càd avec ϑ minimum et on se débrouille pour trouver une autre solution (a',b') qui est plus petite que (a,b), donc

$\vartheta' < \vartheta$

mais ceci contredit le fait que ϑ est minimum. Donc l'équation n'a pas de solution dans $\mathbb{Z}^2$.

3 L'ÉQUATION $X^3 + Y^3 = Z^3$

Soit l'équation de Fermat de degré 3 : $L_3 : x^3 + y^3 = z^3$

Supposons que l'équation admet une solution primitive (a,b,c) avec a,b,c $\in \mathbb{Z}$ càd :

$$\text{Solution primitive} = \begin{cases} a^3 + b^3 = c^3 \text{ ; solution} \\ abc \neq 0 \text{ ; non} - \text{nulle} \\ (a, b, c) = 1 \text{ ; premiers entre eux} \end{cases}$$

pgcd(a,b,c) = (a,b,c) = 1 , premiers entre eux (dans leur ensemble).

Remarque : En fait, ça signifie aussi premier entre eux 2à2.

En effet supposons que d=(a,b) on a donc

d|a et d|b ⇒ kd = a , md = b et soit ℓ un diviseur premier de d on a:

$\ell a' = a$ et $\ell b' = b$ (ℓ|a et ℓ|b)

$\ell^3 a'^3 + \ell^3 b'^3 = c^3$

$\ell(\dots) = c^3$

$\ell | c^3$ comme ℓ est premier ⇒ ℓ|c ceci contredit (a,b,c)=1 donc (a,b)=1 en permutant les lettres a, b, c on trouve (a,c)=(c,b)=1.

(a,b,c)=1 ⇔ (a,b)=(a,c)=(b,c)=1

Ce raisonnement est pour n=3, il est valable pour n=μ ≥5 premier.

(3.1.1) premiers entre eux ⇔ premiers entre eux 2à2

Voyons les propriétés de la solution primitive (a,b,c)

$a^3 + b^3 = c^3$

→ a,b,c ne peuvent pas tous être pairs car (a,b,c)=1 donc au moins un est impair , disons a.

→ b,c ne peuvent pas tous être impairs car a=impair donc au moins un est pair , disons c.

$$\begin{cases} a^3 + b^3 = c^3 \\ abc \neq 0 \\ (a, b) = 1 \\ c = \text{pair} \\ a, b = \text{impairs} \end{cases}$$

$a^3 + b^3 = c^3$

$(a+b)(a^2-ab+b^2) = c^3$

$(a+b)[(a-b)^2+ab] = c^3$

on pose

2p = a+b ; puisque (a+b) est pair

2q = a - b ; puisque (a-b) est pair

d'où

a = p+q

b = p-q

et (p,q)=1 car (a,b)=1

(p,q) de parités différentes car a=impair

le calcul donne

$2p(4q^2 + (p+q)(p-q)) = c^3$

$2p(p^2+3q^2) = c^3 \Rightarrow$ p=pair et q=impair , en effet

(p,q) de parités différentes $\Rightarrow (p^2+3q^2)$=pair, donc q=pair car c=pair

Résumons

$$\begin{cases} 2p(p^2 + 3q^2) = c^3 \\ (p, q) = 1 \\ p = \text{pair}, q = \text{impair} \end{cases}$$

Il nous reste maintenant de voir si 2p et (p^2+3q^2) sont premiers entre eux. Soit d leur diviseur commun

$$\begin{cases} d|2p \\ d|(p^2 + 3q^2) \end{cases}$$

$d|(p^2+3q^2) \Rightarrow md=(p^2+3q^2)=2h+1$ car (p,q) parités différentes donc (p^2+3q^2)=impair

donc d≠2.

d≠2 et d|2p ⇒ d|p ⇒ kd=p

$md=(p^2+3q^2) \Rightarrow md=(k^2d^2+3q^2) \Rightarrow md - k^2d^2=3q^2 \Rightarrow d|3q^2$

¤ $d|3q^2$

→ Supposons $d>3 \Rightarrow d|q^2$

Soit ℓ un diviseur premier de d: $\ell|d$, $d|q^2 \Rightarrow \ell|q^2 \Rightarrow \ell|q$ (car ℓ premier, lemme d'Euler : $\ell|ab \Rightarrow \ell|a$ ou $\ell|b$)

D'autre part : $\ell|d$, $d|p \Rightarrow \ell|p$

$\ell|p$ et $\ell|q$ ce qui est impossible car (q,p)=1

donc $d\leq 3 \Rightarrow d=1$ ou $d=3$ car $d\neq 2$

$pgcd(2p,(p^2+3q^2)) = d = 1$ ou 3

¤ Cas d=1

$$\begin{cases} 2p = r^3 \\ p^2 + 3q^2 = s^3 \end{cases}$$

on a:

$$\begin{cases} p^2 + 3q^2 = s^3 \\ (p,q) = 1 \\ (p,q) \text{ parités différentes} \end{cases}$$

Le théorème (2.5.3) nous dit qu' il existe u,v tels que:

$$p + qi\sqrt{3} = \left(u + vi\sqrt{3}\right)^3 \quad \text{où} \quad u,v \in \mathbb{Z} \text{ et } (u,v) = 1$$

après le calcul ça donne

$$\begin{cases} p = u(u-3v)(u+3v) \\ q = 3v(u-v)(u+v) \end{cases}$$

d'où

$2p = 2u(u-3v)(u+3v) = r^3$

On montre que 2u, (u-3v), (u+3v) sont premier entre eux donc ce sont des cubes

$$\begin{cases} 2u = c'^3 \\ u - 3v = a'^3 \\ u + 3v = b'^3 \end{cases}$$

$a'^3+b'^3 = c'^3$

or

$a^3 + b^3 = (a+b)(a^2-ab+b^2)$

$|a+b| \mid |a^3 + b^3| = |c|^3$

$|a+b| \mid |c|^3$

$|a'b'c'|^3 = |2p| = |a+b|$

$|a'b'c'|^3 \mid |c|^3$

$|a'b'c'|^3 \leq |c|^3$

$|a'b'c'| \leq |c| < |abc|$

$|a'b'c'| < |abc|$

Ici on prend $\vartheta = |abc|$

On a trouvé une solution (a',b',c') plus petite que (a,b,c) ($\vartheta' < \vartheta$) avec la descente infinie ce qui est impossible donc la solution primitive (a,b,c) n'existe pas dans le cas d=1.

¤ <u>Cas d=3</u>

d=3 , d|2p ⇒ 3|p ⇒ p=3t

$2p(p^2+3q^2) = 6t(9t^2+3q^2) = 18t(q^2+3t^2)$

$18t(q^2+3t^2) = c^3$

Ici aussi, c'est exactement le même travail.

(q,t)=1 car (p,q)=1

(q,t) parités différentes car (p,q) parités différentes

$$\begin{cases} 18t(q^2 + 3t^2) = c^3 \\ (q, t) = 1 \\ q, t \text{ parités différentes} \end{cases}$$

Il nous reste maintenant de voir si 18t et (q^2+3t^2) sont premiers entre eux. Soit δ leur diviseur commun

$$\begin{cases} \delta|18t \\ \delta|(q^2 + 3t^2) \end{cases}$$

$\delta|(q^2+3t^2) \Rightarrow m\delta=(q^2+3t^2)=2h+1$ car (q,t) parités différentes

donc δ≠2.

δ≠2 et δ|18t ⇒ δ|9p ⇒ δ=3,9,1 ou δ|t

<u>*a) Cas δ=3</u>

3k=18t

$3m=q^2+3t^2 \Rightarrow 3|q^2 \Rightarrow 3|q$ (car 3=nombre premier)

et 3|p (3t=p) donc c'est impossible car (p,q)=1

*b) Cas δ=9

9k=18t

$9m=q^2+3t^2 \Rightarrow 3|q^2 \Rightarrow 3|q$ (car 3=nombre premier)

et 3|p (3t=p) donc c'est impossible car (p,q)=1

*c) Cas δ|t

$$\left.\begin{array}{c} \delta|t \\ \delta|(q^2+3t^2) \\ (q,t)=1 \end{array}\right\}$$

kδ=t

mδ=(q^2+3t^2)

$m\delta=(q^2+3k^2\delta^2) \Rightarrow \delta|q^2$

Soit ℓ un diviseur premier de δ: $\ell|\delta$, $\delta|q^2 \Rightarrow \ell|q^2 \Rightarrow \ell|q$

D'autre part : $\ell|\delta$, $\delta|t \Rightarrow \ell|t$

c'est impossible car (q,t)=1

*d) Il nous reste donc le cas δ=1

$18t(q^2+3t^2) = c^3$

$$\begin{cases} 18t = r^3 \Rightarrow 3|r^3 \Rightarrow 3|r \Rightarrow 3\mathcal{k} = r \ ^{(*1)} \\ q^2+3t^2 = s^3 \end{cases}$$

$q^2+3t^2 = s^3$

Le théorème (2.5.3) nous dit:

$q + ti\sqrt{3} = \left(u + vi\sqrt{3}\right)^3$ où $u, v \in \mathbb{Z}$ et $(u, v) = 1$

après le calcul ça donne

$$\begin{cases} q = u(u-3v)(u+3v) \\ t = 3v(u-v)(u+v) \end{cases}$$

d'où

$18t = 3^3.2v(u-v)(u+v)$

$2v(u-v)(u+v) = \mathcal{k}^3$; d'après (*1)

On montre que 2v, (u-v), (u+v) sont premier entre eux donc ce sont des cubes

$$\begin{cases} 2v = a'^3 \\ u - v = b'^3 \\ u + v = c'^3 \end{cases}$$

$a'^3+b'^3=c'^3$

or

$a^3 + b^3 = (a+b)(a^2-ab+b^2)$

$|a+b| \mid |a^3 + b^3| = |c|^3$

$|a+b| \mid |c|^3$

$27|a'b'c'|^3 = |6p| = 3|a+b|$

$9|a'b'c'|^3 = |a+b|$

$9|a'b'c'|^3 \mid |c|^3$

$|a'b'c'|^3 \leq 9|a'b'c'|^3 \leq |c|^3$

$|a'b'c'|^3 \leq |c|^3$

$|a'b'c'| \leq |c| < |abc|$

$|a'b'c'| < |abc|$

Ici on prend $\vartheta = |abc|$

On a trouvé une solution (a',b',c') plus petite que (a,b,c) (Sol plus petite $\stackrel{def}{=} \vartheta' < \vartheta$) avec la descente infinie ce qui est impossible donc la solution primitive (a,b,c) n'existe pas dans le cas d=3 non plus.

Finalement l'équation

$x^3+y^3 = z^3$

n'a pas de solutions entiers non nuls.

4 L'ÉQUATION $X^2 + Y^2 = Z^2$

Soit l'équation: $x^2 + y^2 = z^2$,

On appelle une solution primitive dans $\mathbb{N}$, un triplet (a,b,c) avec a,b,c $\in \mathbb{N}$ tels que:

$$(a,b,c) \overset{\text{def}}{=} \begin{cases} a^2 + b^2 = c^2 \\ abc \neq 0 \\ (a,b,c) = 1 \end{cases}$$

Soit donc (a,b,c) une solution primitive et voyons alors ses propriétés:

$a^2 + b^2 = c^2$

on a

(a,b)=1 donc a,b ne peuvent pas être tous les deux pairs

ils ne peuvent pas être non plus tous les deux impairs

en effet, dans ce cas c serait pair et

$a^2 + b^2 = c^2 \pmod 4$

$2 = 0 \pmod 4$

donc a,b de parités différentes, et on suppose a=impair donc b=pair et finalement c=impair

Résumons

$$\begin{cases} a^2 + b^2 = c^2 \\ (a, b, c) = 1 \\ a, b \text{ parités différentes} \\ a = \text{impair}, b = \text{pair}, c = \text{impair} \end{cases}$$

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

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

on pose

$c+a=2p$; car c,a impairs

$c-a = 2q$; car c,a impairs

d'où

$c=p+q$

$a=p-q$

on voit que $(p,q)=1$ car $(c,a)=1$ (premier entre eux ⇒ premier 2à2)

$(c+a)(c-a) = 4t^2$ (car b=pair)

$pq = t^2$

comme $(p,q)=1$ p et q sont déjà des carrés

$p = u^2$

$q = v^2$

et on voit que $(u,v)=1$ car $(p,q)=1$

d'où

$c=p+q=u^2+v^2$

$a=p-q=u^2-v^2$

ici on voit que u>v car a>0 et u,v de parités différentes car c=impair

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

$u^4 + 2u^2v^2 + v^4 - u^4 + 2u^2v^2 - v^4 = b^2$

$b = 2uv$

les solutions de $x^2+y^2 = z^2$ sont donc

$$\begin{cases} x = u^2 - v^2 \\ y = 2uv \\ z = u^2 + v^2 \end{cases}$$

avec u>v>0, (u,v)=1, et u,v de parités différentes

Exemple, on peut prendre u=n+1, v=n avec $n\in\mathbb{N}^*$

$(2,1) \rightarrow 3^2 + 4^2 = 5^2$

$(3,2) \rightarrow 5^2 + 12^2 = 13^2$

$(4,3) \rightarrow 7^2 + 24^2 = 25^2$

.....

5 L'ÉQUATION $X^4 + Y^4 = Z^2$

L'équation : $x^4+y^4 = z^2$

Supposons que l'équation admet une solution (a,b,c) primitive dans $\mathbb{N}$ ($a,b,c \in \mathbb{N}$, $abc \neq 0$, $(a,b,c)=1$), voyons ses propriétés

$a^4 + b^4 = c^2$

$(a,b) = 1$

$(a^2)^2 + (b^2)^2 = c^2$

et a^2, b^2 premiers entre eux , donc on peut écrire

$a^2 = u^2 - v^2$

$b^2 = 2uv$

$c = u^2+v^2$

voyons l'égalité:

$a^2 + v^2 = u^2$

d'où de nouveau:

$a = p^2 - q^2$

$v = 2pq$

$u = p^2+q^2$

or

$b^2 = 2uv = 4upq$

$$\left(\frac{b}{2}\right)^2 = upq$$

car b^2=pair donc b=pair

donc u,p,q sont des carrés

$u = r^2$

$p = s^2$

$q = t^2$

$p^2+q^2=u \Rightarrow s^4+t^4=r^2$

et on a:

$0 < r=\sqrt{u} \leq u^2=c-v^2 < c$

Ici on prend $\vartheta=c$

On part de la solution (a,b,c) et on arrive à trouver une autre solution (s,t,r) plus "petite" ($\vartheta'=r<\vartheta=c$) donc avec la descente infinie, ce qui est impossible, la solution (a,b,c) n'existe pas donc l'équation $x^4+y^4 = z^2$ n'a pas de solutions non nulles dans $\mathbb{N}$, donc pas de solutions non nulles dans $\mathbb{Z}$ non plus :

En effet, si l'équation admet une solution primitive dans $\mathbb{Z}$

$a^4+b^4 = c^2$

par ex si $a<0$ alors on pose $a = -a'$ avec $a'>0$

et on aura :

$(-a')^4+b^4 = c^2$

$a'^4+b^4 = c^2$

(a',b,c) comme solution primitive dans $\mathbb{N}$, ce qui est impossible.

6 L'ÉQUATION $X^4 + Y^4 = Z^4$

D'après ce que nous avions dit, l'équation $x^4+y^4 = z^4$ n'a pas de solutions entiers non nuls.

En effet si elle admet une solution (a,b,c)

$a^4+b^4 = c^4 \Rightarrow a^4+b^4 = (c^2)^2$

alors (a,b,c^2) sera la solution de $x^4+y^4 = z^2$ ce qui est impossible.

Il y a une autre façon de montrer que l'équation $x^4+y^4 = z^4$ n'a pas de solutions entiers non nuls.

On commence par montrer la propriété suivante:

Propriété : L'aire d'un triangle rectangle à côtés entiers naturels (triangle pythagorique) ne peut pas être un carré, autrement dit

le système :

$$\begin{cases} x^2 + y^2 = z^2 \\ xy = 2t^2 \end{cases}$$

n'a pas de solution en entiers naturels non-nuls.

Démonstration :

Supposons que le système admet une solution (a,b,c,d) alors on a:

$a^2+b^2 = c^2$

$ab = 2d^2$

ce qui donne:

$a = u^2 - v^2$

$b = 2uv$

$c = u^2+v^2$

u,v premiers entre eux et de parités différentes, on peut supposer v=pair.

$ab = 2(u^2 - v^2)uv = 2d^2$

$(u - v)(u+v)uv = d^2$

les (u-v),(u+v),u,v sont premiers entre eux 2à2 , donc

$u - v = p^2$

$u + v = q^2$

$u = r^2$

$v = s^2$

d'où

$2v = q^2 - p^2$

$2u = q^2+p^2$

u,v de parités différentes $\Rightarrow$ p^2, q^2 impairs $\Rightarrow$ p,q impairs $\Rightarrow$ q - p, q+p pairs

$2h = q - p$

$2k = q+p$

$4h^2 = q^2 + p^2 - 2qp$

$4k^2 = q^2+p^2+2qp$

$4(h^2+k^2) = 2(q^2+p^2) = 4u$

$h^2+k^2 = u = r^2$

$h^2+k^2 = r^2$

et

$4hk = q^2 - p^2 = 2v = 2s^2$

$2hk = s^2$

$hk/2 = \frac{1}{4} s^2$

$hk = 2\left(\frac{s}{2}\right)^2 ; v = \text{pair} \Rightarrow s = \text{pair}, v = 2m$

$hk = 2m^2$

ça y est on a trouvé une autre solution :

$h^2+k^2 = r^2$

$hk = 2m^2$

c'est (h,k,r,m)

ici on prend ϑ=c

$c = u^2+v^2 = r^4 + s^4 > r$

$\vartheta'=r < \vartheta=c$

donc la solution (h,k,r,m) est plus petite que (a,b,c,d)

La descente infinie montre que ce n'est pas possible donc la solution (a,b,c,d) n'existe pas autrement dit il n'y a pas de triangle pythagorique dont l'aire est un carré.

L'équation L_4: $x^4+y^4 = z^4$ n'a pas de solution, en effet supposons qu'elle a une solution (a,b,c) on aura donc

$a^4 + b^4 = c^4$

d'où

$a^4 = c^4 - b^4$

$a^8 = c^8 + b^8 - 2c^4b^4$

$a^8 + 4c^4b^4 = c^8 + b^8 + 2c^4b^4$

$a^8 + 4c^4b^4 = (c^4 + b^4)^2$

et

$2a^4c^2b^2 = 2(a^2cb)^2$

On a trouvé un triangle pythagorique $(a^4,2c^2b^2,c^4+b^4)$ dont l'aire est un carré $(a^2cb)^2$, ce qui est impossible donc la solution (a,b,c) n'existe pas donc L_4 n'a pas de solution en entiers naturels non-nuls, comme on a des puissances paires, L_4 n'a pas non plus de solutions non-nulles dans $a,b,c \in \mathbb{Z}$, $abc \neq 0$.

7 SOPHIE GERMAIN

7.1 UNE FORMULE UTILE

Voici une formule utile :

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$$

On va la démontrer par récurrence.

¤ n=2

$$a^2 - b^2 = (a-b)\sum_{k=0}^{1} a^{1-k}b^k = (a-b)(a+b)$$

La formule est vraie pour n=2.

¤ Hypothèse de récurrence: supposons que la formule soit vraie pour n, puis montrons qu'elle reste encore vraie pour (n+1).

On a :

$$a^{n+1} - b^{n+1} = a^n(a-b) + b(a^n - b^n)$$

et d'après HR on a:

$$a^{n+1} - b^{n+1} = a^n(a-b) + b(a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$$

$$a^{n+1} - b^{n+1} = (a-b)\left[a^n + b\sum_{k=0}^{n-1} a^{n-1-k}b^k\right]$$

$$a^{n+1} - b^{n+1} = (a-b)\left[a^n + \sum_{k=0}^{n-1} a^{n-1-k}b^{k+1}\right]$$

changement des indices : k+1=m

$$a^{n+1} - b^{n+1} = (a-b)\left[a^n + \sum_{m=1}^{n} a^{n-m}b^m\right]$$

$$a^{n+1} - b^{n+1} = (a-b)\sum_{m=0}^{n} a^{n-m}b^m$$

Pour (n+1) la formule est encore vraie.

et pour la somme avec n=p=<u>impair</u> on a:

$$a^p + b^p = (a+b)\sum_{k=0}^{p-1} a^{p-1-k}(-b)^k$$

On ne peut pas parler de la conjecture de Fermat sans parler du théorème de Sophie Germain. On trouve des textes, des documents sur internet parlant du théorème mais pas du tout clair ... on ne sait même pas de quoi s'agit le théorème ... et on voit même des textes qui disent que le théorème de Sophie Germain démontre la conjecture de Fermat !!! bref un flou total , une pagaille pas possible ...

Et pour tant ce n'est pas bien compliqué.

Soit :

L_p : $x^p + y^p = z^p$ avec p premier ≥ 5

L'équation de Fermat, on divise l'ensemble des solutions (a,b,c) de L_p , en deux types:

type 1: (a,b,c) , $abc \neq 0 \pmod p$

type 2: (a,b,c) , $abc = 0 \pmod p$

Théorème de Sophie Germain : Soit p un nombre premier de Germain càd q=2p+1 est aussi un nombre premier.

Alors l'équation de Fermat L_p n'a pas de solution de type 1.

Démonstration : On va raisonner par absurde, càd on suppose une telle solution existe et on espère arriver à une contradiction.

Allons-y, on a donc

Solution de type 1

$$\begin{cases} a^p + b^p = c^p \\ abc \neq 0 \\ (a,b,c) = 1 \\ abc \neq 0 \pmod p \end{cases}$$

étape1:

(7.1.1) Lemme :

$\forall u \in \mathbb{Z}$, $u^p = 0,1,-1 \pmod q$

$\rightarrow q|u \Rightarrow u^p = 0 \pmod q$

$\rightarrow q \nmid u \Rightarrow u^q = u \pmod q$; petit th de Fermat

$u^{q-1} = 1 \pmod q$; car u est inversible dans $\mathbb{F}_q$, on simplifie u, c'est ici on a besoin q=premier.

$u^{2p} = 1 \pmod q$;

$u^p = \pm 1 \pmod q$; c'est ici on a besoin 2p (pair)

donc, on a bien.

$u^p = 0,1,-1 \pmod q$

étape2 : q|c (q∤a et q∤b)

Supposons qu'on aie : $abc \neq 0 \pmod q$

$a^q = a \pmod q$; petit th de Fermat

$a^{q-1} = 1 \pmod q$

$a^{2p} = 1 \pmod q$

$a^p = \pm 1 \pmod q$

de même pour b,c :

$b^p = \pm 1 \pmod q$, $c^p = \pm 1 \pmod q$

d'où

$a^p + b^p + (-c)^p = \pm 1 \pm 1 \pm 1 \pmod q$

$a^p + b^p + (-c)^p = \pm 1, \pm 3 \pmod q$

$a^p + b^p + (-c)^p \neq 0 \pmod q$, car q=2p+1 > 7

or on a :

$a^p + b^p = c^p \pmod q$

$a^p + b^p + (-c)^p = 0 \pmod q$

donc abc = 0 (mod q) càd q divise l'un des a,b,c . On peut supposer que c'est c, q|c (donc q∤a, q∤b car (a,b,c)=(a,b)=(a,c)=(b,c)=1)

étape3 :

$a^p + b^p = c^p$

$$(a+b)\sum_{k=0}^{p-1} a^{p-1-k}(-b)^k = c^p$$

posons

$$A = \sum_{k=0}^{p-1} a^{p-1-k}(-b)^k$$

on va montrer que (a+b) et A sont premiers entre eux. Supposons que r leur diviseur premier commun.

r|(a+b) et r|A

¤ $\Rightarrow r^2|c^p \Rightarrow$ r|c (car r=premier)

¤ r|(a+b) $\Rightarrow$ a+b = 0 (mod r) $\Rightarrow$ a = -b (mod r) $\Rightarrow$

$$A = \sum_{k=0}^{p-1} a^{p-1-k}(-b)^k = \sum_{k=0}^{p-1} a^{p-1-k}(a)^k \pmod r$$

$$A = \sum_{k=0}^{p-1} a^{p-1-k}(a)^k = \sum_{k=0}^{p-1} a^{p-1} = pa^{p-1} \pmod r$$

$A = pa^{p-1} \pmod r$

or $(r|A) \Leftrightarrow A=0 \pmod r$

$pa^{p-1} = 0 \pmod r$

$\rightarrow r|p \Rightarrow r=p$ (car r,p premiers) et $r|c \Rightarrow p|c$ contredit solution de type 1.

$\rightarrow r|a^{p-1} \Rightarrow r|a$ (car r=premier) et $r|c \Rightarrow$ contredit (a,c)=1

donc r=1 , (a+b) et A sont premiers entre eux.

il existe donc $\alpha,\alpha' \in \mathbb{Z}$ tels que :

$a + b = \alpha^p$ et $A = \alpha'^p$

En permutant les lettres a,b,c on trouve deux autres relations:

$$\begin{cases} a + b = \alpha^p \\ (-b) + c = \beta^p \\ (-a) + c = \gamma^p \end{cases} \qquad \begin{cases} A = \alpha'^p \\ B = \beta'^p \\ C = \gamma'^p \end{cases}$$

<u>étape4</u> :

$(-a) + c = \gamma^p$

$(-a) + c = \gamma^p \pmod q$

$\gamma^p = -a \pmod q$, car $q|c$

Or

$\gamma^p = 0,1,-1 \pmod q$, Lemme (7.1.1)

q∤a ⇒ q∤γ ⇒ γ inversible dans $\mathbb{F}_q$ donc γ≠0 (mod q) ⇒

$\gamma^p = \pm 1 \pmod q$

(-a) $= \pm 1 \pmod q$ ⇒ a=$\pm 1 \pmod q$ (3*)

de même pour b,

$\beta^p = \pm 1 \pmod q$, et b=$\pm 1 \pmod q$

$\alpha^p + \beta^p + \gamma^p = 2c$

$\alpha^p + \beta^p + \gamma^p = 0 \pmod q$

$\alpha^p \pm 1 \pm 1 = 0 \pmod q$

$\alpha^p = \pm 1 \pm 1 \pmod q$

$\alpha^p = 0, \pm 2 \pmod q$

mais d'après le Lemme (7.1.1) on a:

$\alpha^p = 0, \pm 1 \pmod q$;Lemme (7.1.1)

donc

$\alpha^p = 0 \pmod q$

càd

a+b = 0 (mod q)

a = -b (mod q)

or

$$A = \sum_{k=0}^{p-1} a^{p-1-k}(-b)^k$$

d'où

$$A = \sum_{k=0}^{p-1} a^{p-1-k}(a)^k \pmod q$$

$$A = pa^{p-1} \pmod q$$

$$\alpha'^p = pa^{p-1} \pmod q$$

Mais

$a = \pm 1 \pmod q$ (voir (3*))
et p-1 = pair donc
$a^{p-1} = 1 \pmod q$
d'où
$\alpha'^p = p \pmod q$
mais ça contredit

$$\alpha'^p = 0, \pm 1 \pmod q$$;Lemme (7.1.1)

car

$p \neq 0, \pm 1 \pmod q$; $p = \frac{q-1}{2} \rightarrow$ dans $\mathbb{F}_q$ on a: $p \neq 0,1,-1$

Ouuuoffff !!!

Remarque importante : Il y a des textes qui circulent sur l'internet qui disent que le théorème de Sophie Germain démontre la conjecture de Fermat !!! c'est faux et c'est n'importe quoi !!!

En effet si on observe bien la démonstration on voit que :

→ D'une part le théorème ne dit rien sur les solutions de type 2 . On ne sait pas si l'équation admet les solutions de types 2 ou non !!

→ D'autre part , on ne traite que des nombres premiers Germain, pas tous les nombres premiers !

Donc le théorème de Sophie de Germain ne démontre pas du tout la conjecture de Fermat.

Méfiez vous des informations sur le Net : "N'importe qui peut dire n'importe quoi et n'importe quoi peut être répété bêtement par n'importe qui !!"

Donc il faut trier, vérifier les informations sur le Net ....

8 L'OEUVRE DE KUMMER

On prend $\mathbb{K}=\mathbb{Q}(\zeta)$ avec $\zeta = e^{\frac{2\pi}{p}i}$, $\zeta^p = 1$, p=premier impair, on montre alors que

$$\overline{\mathbb{Z}}_{\mathbb{K}} = \mathbb{Z}[\zeta] = \{\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \; ; \; a_i \in \mathbb{Z}\}$$

On définit les $\mathbb{Z}$-morphismes σ_k de $\mathbb{Z}[\zeta]$ dans $\mathbb{C}$ de la façon suivante:

$1 \leq k \leq p-1$

$\sigma_k : \mathbb{Z}[\zeta] \to \mathbb{C}$

$\alpha \to \sigma_k(\alpha)$

$\alpha,\beta \in \mathbb{Z}[\zeta]$, $a \in \mathbb{Z}$

$\sigma_k(\alpha+\beta) = \sigma_k(\alpha)+\sigma_k(\beta)$

$\sigma_k(\alpha\beta) = \sigma_k(\alpha)\sigma_k(\beta)$

$\sigma_k(a) = a$

Et σ_k est identifié par :

$\sigma_k(\zeta) \stackrel{def}{=} \zeta^k$

Et une norme sur $\mathbb{Z}[\zeta]$

$N : \mathbb{Z}[\zeta] \to \mathbb{Z}$

$\alpha \to N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) \ldots \sigma_{p-1}(\alpha)$

On a alors les propriétés suivantes:

¤ $N(\alpha\beta) = N(\alpha)N(\beta)$

¤ $N(\alpha) = 0 \Leftrightarrow \alpha = 0$

¤ $N(\alpha) = \pm$premier $\Rightarrow \langle\alpha\rangle$ = premier

¤ $a \in \mathbb{Z} \Rightarrow N(a) = a^{p-1}$

Exemple

$\chi(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$; polynôme minimal de ζ

$X^{p-1} + X^{p-2} + \ldots + X + 1 = (X-\zeta)(X-\zeta^2) \ldots (X-\zeta^{p-1})$

$p = (1-\zeta)(1-\zeta^2) \ldots (1-\zeta^{p-1}) = (1-\sigma_1(\zeta))(1-\sigma_2(\zeta)) \ldots (1-\sigma_{p-1}(\zeta))$

$p = N(1-\zeta)$ (donc l'idéal $\langle 1-\zeta\rangle$ est premier)

On a:

$\zeta^{p-1} + \zeta^{p-2} + \ldots + \zeta + 1 = 0$

$\zeta(-\zeta^{p-2} - \zeta^{p-3} - \ldots - 1) = 1$

ce qui montre que ζ est une unité, $\zeta \in \mathbb{Z}[\zeta]^x$

¤ $\zeta\zeta^{p-1} = 1 \Rightarrow \zeta$ unité

¤ $\zeta^k\zeta^{p-k} = 1 \Rightarrow \zeta^k$ unité , pour $1 \leq k \leq p-1$

$\frac{1-\zeta^k}{1-\zeta^m} = \mu \in \mathbb{Z}[\zeta]^x$, $k \nmid p$ et $m \nmid p$

Autrement dit les $(1-\zeta^k)$ et $(1-\zeta^m)$ sont associés quand k∤p et m∤p

En particulier

¤ $1 - \zeta, 1 - \zeta^2, 1 - \zeta^3, \ldots, 1 - \zeta^{p-1}$ sont associés

¤ $\frac{1-\zeta^2}{1-\zeta} = 1 + \zeta = \varepsilon =$ unité

¤ $p = (1 - \zeta)(1 - \zeta^2) \ldots (1 - \zeta^{p-1})$

¤ $p = \omega(1 - \zeta)^{p-1}$, ω = unité

¤ $\langle p \rangle = \langle 1 - \zeta \rangle^{\,p-1}$

Quand on fait de l'arithmétique dans $\mathbb{Z}$, tout se passe bien et qu'on a la propriété suivante:

<u>Propriété-α</u> :

$a,b,c \in \mathbb{Z}$

$$\left.\begin{matrix} ab = c^n \\ (a,b) = 1 \end{matrix}\right\} \Rightarrow \begin{cases} a = \varepsilon u^n \\ b = \mu v^n \end{cases} \quad \text{où } u, v \in \mathbb{Z}, \varepsilon, \mu \text{ unités}$$

Cette propriété provient de la décomposition unique d'un nombre en facteurs premiers dans $\mathbb{Z}$, c'est parce que $\mathbb{Z}$ est factoriel.

Dans l'équation de Fermat

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

on factorise le membre de gauche ça donne

$(x+y)(x+y\zeta)(x+y\zeta^2) \ldots (x+y\zeta^{p-1}) = z^p$

On voit donc que les éléments $(x+y)$, $(x+y\zeta)$, $(x+y\zeta^2)$, ... $(x+y\zeta^{p-1})$ sont dans $\mathbb{Z}[\zeta]$, mais en général $\mathbb{Z}[\zeta]$ n'a aucune propriété particulier donc pas beaucoup de l'arithmétique...

Peut-on quand même utiliser la propriété-α dans $\mathbb{Z}[\zeta]$?

La réponse est non car $\mathbb{Z}[\zeta]$ n'est pas toujours factoriel, ni principal !! tout dépend de p .

Pour s'en sortir Kummer a l'idée suivante:

Au lieu de travailler dans $\mathbb{Z}[\zeta]$ on va "monter" travailler dans $\mathbb{I}$ l'ensemble des idéaux de $\mathbb{Z}[\zeta]$!! (ici $A=\mathbb{Z}[\zeta]$) . On démontre alors le théorème suivante très importante :

Théorème de décomposition unique :

Dans $\mathbb{I}$ tout idéal non nul I se décompose de façon unique en produit des idéaux premiers .

$\forall I \in \mathbb{I}^*$, $I = P_1 P_2 \ldots P_n$

$P_i =$ idéal premier

Note: On dira que $\mathbb{Z}[\zeta]$ est un anneau de Dedekind.

Une fois la décomposition est faite on "redescendre" sur $\mathbb{Z}[\zeta]$ par les règles suivantes:

1) $\langle\alpha\rangle \langle\beta\rangle = \langle\alpha\beta\rangle$

2) $\langle\alpha\rangle = \langle\beta\rangle \Rightarrow \alpha = \varepsilon\beta$ où ε est une unité.

En espérant qu'on pourrait s'en sortir. Mais il y a quand même 2 problèmes !!

→ Comment peut-on descendre de $\mathbb{I}$ à $\mathbb{Z}[\zeta]$?

→ Comment "débarrasser" l'unité ε ?

8.1 LES LEMMES

Définition nombre premier régulier :

On dit qu' un nombre premier p est régulier si

I^p principal ⇒ I principal.

où I est un idéal, $I \in \mathbb{I}$

Propriété 1 :

p est régulier s'il ne divise aucun des numérateurs N_k des nombres de Bernoulli $B_2, B_4, B_6, ..., B_{p-3}$

$p \nmid N_k$, pour k=2, 4, 6, ... , (p-3)

Rappel les nombres de Bernoulli : Les nombres de Bernoulli sont définis par récurrence :

$$B_0 = 1$$

$$1 + \binom{p+1}{1} B_1 + \binom{p+1}{2} B_2 + \cdots + \binom{p+1}{p} B_p = 0$$

$$\sum_{k=0}^{p} \binom{p+1}{k} B_k = 0$$

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

On a $B_{2k+1} = 0$ pour $k \geq 1$, les impairs B_3, B_5, B_7, B_9 , ... sont nuls et le signe de B_{2k} est alterné : $sig(B_{2k}) = (-1)^{k+1}$

B_2=+, B_4=-, B_6=+, B_8=-,....

Propriété 2 :

On pose

$S_k = 1^k + 2^k + ... + (p-1)^k$, pour k=2, 4, 6, ... , (p-3)

p est régulier si p^2 ne divise aucun des $S_2, S_4, S_6, ..., S_{p-3}$

$p^2 \nmid S_k$ pour k=2, 4, 6, ... (p-3)

Nombre de classes :

On définit la relation d'équivalence suivante sur $\mathbb{I}$:

$\forall I, J \in \mathbb{I}$

$I \sim J \Leftrightarrow \exists \alpha, \beta \in \mathbb{Z}[\zeta]$ tels que : $\langle\alpha\rangle I = \langle\beta\rangle J$

On montre que $\mathbb{I}/\sim$ est fini, on note h le nombre de classes càd le nombre d'éléments de $\mathbb{I}/\sim$

$\#(\mathbb{I}/\sim) = h$

¤ $\forall I \in \mathbb{I}, \quad I^h = \text{principal}$

h est donc le plus petit entier naturel m tel que

$\forall I \in \mathbb{I},\ I^m$ =principal

Propriété 3 (Kummer):

p est régulier s'il ne divise pas le nombre de classes h

p régulier $\Leftrightarrow p \nmid h$

exemples:

p=23, h = 3,

p=37, h = 37,

p=59, h = 3x59x233,

p=67, h = 67x12739

donc 23=régulier, 37=irrégulier, 59=irrégulier, 67=irrégulier

Voici le début de la liste des nombres premiers réguliers :

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, (37), 41, 43, 47, 53, (59), 61, (67), 71, 73, 79, 83, 89, 97, 107, 109, 113, 127, 137, 139, 151, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 239, 241, 251, 269, 277, 281, 313 ...

On voit qu'il y a trois nombres irréguliers 37, 59, 67 <100

Et le début de la liste des nombres premiers irréguliers :

37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293, 307, 311, 347, 353, 379, 389, 401, 409, 421, 433, 461, 463, 467, 491, 523, …

Note: On démontre qu'il y a une infinité des nombres premiers irréguliers (th de Jensen 1915), mais on ne sait pas si les nombres réguliers sont finis ou infinis.

Lemme :

soit

$$\sum_{i=0}^{p-2} a_i \zeta^i = 0 \pmod{p} \quad , a_i \in \mathbb{Z}$$

Si p divise l'un des a_i ($p|a_i$), alors $p|a_k \ \forall k$

$a_i = 0 \pmod{p} \Rightarrow a_k = 0 \pmod{p} \ \forall k$

Lemme :

L'idéal $\langle 1 - \zeta \rangle$ est premier

En effet : Soit

$\alpha\beta \in \langle 1 - \zeta \rangle$

$\alpha\beta = \kappa(1-\zeta) \quad , \kappa \in \mathbb{Z}[\zeta]$

$(1-\zeta)|\alpha\beta$

$\langle 1 - \zeta \rangle | \langle \alpha \rangle \langle \beta \rangle$

$N(\alpha)N(\beta) = N(\kappa)N(1-\zeta)$

$p|N(\alpha)N(\beta) \Rightarrow p|N(\alpha)$ par exemple car p est premier

$p|\sigma_1(\alpha)\sigma_2(\alpha)...\sigma_{p-1}(\alpha)$

donc p divise l'un des $\sigma_k(\alpha)$:

¤ si $k=1 \Rightarrow p|\alpha$

$\langle p\rangle|\langle\alpha\rangle$

$\langle 1-\zeta\rangle^{p-1}|\langle\alpha\rangle$

$\langle 1-\zeta\rangle|\langle\alpha\rangle \Rightarrow \langle\alpha\rangle \subset \langle 1-\zeta\rangle \Rightarrow \alpha\in\langle 1-\zeta\rangle$

¤ sinon $p|\sigma_k(\alpha)$ avec $k\neq 1$

$\langle p\rangle|\langle\sigma_k(\alpha)\rangle$

$\langle 1-\zeta\rangle^{p-1}|\langle\sigma_k(\alpha)\rangle$

$\langle 1-\zeta\rangle|\langle\sigma_k(\alpha)\rangle$

$(1\text{-}\zeta)|\sigma_k(\alpha) \Rightarrow \sigma_{p+1-k}(1\text{-}\zeta)|\sigma_{p+1}(\alpha) \Rightarrow (1\text{-}\zeta^{p+1-k})|\alpha$

Comme les $(1\text{-}\zeta^{p+1-k})$ sont associés à $(1\text{-}\zeta)$ ils auront le même idéal: $\langle 1-\zeta^{p+1-k}\rangle = \langle 1-\zeta\rangle$, càd:

$\langle 1-\zeta^{p+1-k}\rangle|\langle\alpha\rangle$

$\langle 1-\zeta\rangle|\langle\alpha\rangle \Rightarrow \langle\alpha\rangle \subset \langle 1-\zeta\rangle \Rightarrow \alpha\in\langle 1-\zeta\rangle$

Comme α et β jouent le même rôle (ils sont symétriques) on trouvera le même résultat pour β, autrement dit on a:

$\alpha\beta \in\langle 1-\zeta\rangle \Rightarrow \alpha\in\langle 1-\zeta\rangle$ ou $\beta\in\langle 1-\zeta\rangle$

ça signifie que $\langle 1-\zeta \rangle$ est premier.

Lemme :

Le nombre $\lambda = 1-\zeta$ est premier (dans $\mathbb{Z}[\zeta]$ bien sûr)

En effet :

Soit $(1-\zeta)|\alpha\beta$ il faut montrer que $(1-\zeta)|\alpha$ ou $(1-\zeta)|\beta$, allons-y

$(1-\zeta)|\alpha\beta \Rightarrow \alpha\beta = \kappa(1-\zeta)$, $\kappa \in \mathbb{Z}[\zeta]$

$N(\alpha)N(\beta) = N(\kappa)N(1-\zeta)$

$p|N(\alpha)N(\beta) \Rightarrow p|N(\alpha)$ par exemple car p est premier

$p|\sigma_1(\alpha)\sigma_2(\alpha)...\sigma_{p-1}(\alpha)$

donc p divise l'un des $\sigma_k(\alpha)$:

¤ si $k=1 \Rightarrow p|\alpha$

$(1-\zeta)|\alpha$, car $p = \omega(1-\zeta)^{p-1}$, ω = unité

¤ sinon $p|\sigma_k(\alpha)$ avec $k \neq 1$

$p|\sigma_k(\alpha)$

$(1-\zeta)|\sigma_k(\alpha) \Rightarrow \sigma_{p+1-k}(1-\zeta)|\sigma_{p+1}(\alpha) \Rightarrow (1-\zeta^{p+1-k})|\alpha$

Comme les $(1-\zeta^{p+1-k})$ sont associés à $(1-\zeta)$, on a :

$(1-\zeta)|\alpha$

Comme α et β jouent le même rôle (ils sont symétriques) on trouvera le même résultat pour β, autrement dit on a:

$(1-\zeta)|\alpha\beta \Rightarrow (1-\zeta)|\alpha$ ou $(1-\zeta)|\beta$, allons-y

ça signifie que $1-\zeta$ est premier.

(8.1.1) Lemme :

$\forall \alpha \in \mathbb{Z}[\zeta], \exists a \in \mathbb{Z}$ tel que

$\alpha^p = a \pmod p$

Démonstration :

comme α est un élément de $\mathbb{Z}[\zeta]$ il s'écrit

$$\alpha = \sum_{i=0}^{p-2} a_i \zeta^i \quad , a_i \in \mathbb{Z}$$

$$\alpha^p = \left(\sum_{i=0}^{p-2} a_i \zeta^i \right)^p = \sum_{i=0}^{p-2} \left(a_i \zeta^i \right)^p \pmod p$$

$$\alpha^p = \sum_{i=0}^{p-2} a_i^p \pmod p$$

$$\alpha^p = \sum_{i=0}^{p-2} a_i \pmod p$$

$$\alpha^p = a \pmod p \ , a \in \mathbb{Z}$$

Lemme des unités-1 :

$\forall \varepsilon \in \mathbb{Z}[\zeta]^x$,$\exists \mu$ unité réelle $\overline{\mu} = \mu$, et r entier ≥ 0 tels que

$\varepsilon = \mu\zeta^r$

Lemme des unités-2 (Kummer) :

Soit p=régulier et a∈ℤ

$\forall \varepsilon \in \mathbb{Z}[\zeta]^x$,

Si $\varepsilon = a \pmod p$

alors $\exists \mu \in \mathbb{Z}[\zeta]^x$ tel que $\varepsilon = \mu^p$

8.2 THÉORÈME DE KUMMER (1847)

Théorème de Kummer : La conjecture de Fermat est vraie pour les nombres premiers réguliers.

Démonstration :

On va traiter la résolution en deux cas.

Cas I : Solution de type 1

$$\begin{cases} a^p + b^p = c^p \\ (a, b, c) = 1 \\ abc \neq 0 \pmod p \end{cases}$$

On factorise le membre de gauche :

$(a+b)(a+b\zeta)(a+b\zeta^2) \ldots (a+b\zeta^{p-1}) = c^p$

puis on monte dans $\mathbb{I}$, on a donc des idéaux principaux

$\langle a + b\rangle\langle a + b\zeta\rangle\langle a + b\zeta^2\rangle \ \ldots \ \langle a + b\zeta^{p-1}\rangle = \langle c\rangle^p$

on va montrer que les idéaux à gauche sont premiers entre eux 2à2. On prend par ex les deux premier.

Soit P un idéal premier qui divise $\langle a + b\rangle$ et $\langle a + b\zeta\rangle$

$P|\langle a + b\rangle \Rightarrow \langle a + b\rangle \subset P \Rightarrow a+b \in P$

$P|\langle a + b\zeta\rangle \Rightarrow \langle a + b\zeta\rangle \subset P \Rightarrow a+b\zeta \in P$

d'où

$(1- \zeta)b \in P$

et

$a - a\zeta + b\zeta - b\zeta = (a + b\zeta) - \zeta(a+b) \in P$

$(1 - \zeta)a \in P$

$P|\langle 1 - \zeta\rangle\langle b\rangle$

$P|\langle 1 - \zeta\rangle\langle a\rangle$

comme a et b premiers entre eux $\Rightarrow \langle a\rangle$ et $\langle b\rangle$ premiers entre eux $\Rightarrow P|\langle 1 - \zeta\rangle \Rightarrow P = \langle 1 - \zeta\rangle$ car P est premier

$\langle 1 - \zeta\rangle|\langle a + b\rangle$

$\langle 1 - \zeta\rangle K \langle a + b\zeta\rangle\langle a + b\zeta^2\rangle \dots \langle a + b\zeta^{p-1}\rangle = \langle c\rangle^p$

$\langle 1 - \zeta\rangle|\langle c\rangle^p$

$\langle 1 - \zeta\rangle|\langle c\rangle$ car $\langle 1 - \zeta\rangle$ est premier

$(1-\zeta)|c$

$N(1-\zeta)|N(c)$

$p|c^{p-1} \Rightarrow p|c$ (car p=premier)

contradiction car p∤c.

Pour les autres couples on fait la même chose, donc les $\langle a + b\rangle\langle a + b\zeta\rangle\langle a + b\zeta^2\rangle$ … $\langle a + b\zeta^{p-1}\rangle$ sont premiers entre eux 2à2. ils sont donc en puissance p-ième par ex:

$\langle a + b\zeta\rangle = I^p$

On a I^p principal, et comme p est régulier I est principal :

$\langle a + b\zeta\rangle = \langle\tau\rangle^p$

$\langle a + b\zeta\rangle = \langle\tau^p\rangle$

on descend dans $\mathbb{Z}[\zeta]$

$a+b\zeta = \varepsilon\tau^p$; où ε=unité, $\tau\in\mathbb{Z}[\zeta]$

d'après le lemme des unités-1 ça donne

$a+b\zeta = \mu\zeta^r\tau^p$; où $\mu=\overline{\mu}$ unité réelle, r=entier ≥0

$a+b\zeta = \mu\zeta^r u \pmod p$; Lemme (8.1.1)

$a+b\overline{\zeta} = \mu\zeta^{-r}u \pmod p$

$a\zeta^{2r}+b\overline{\zeta}\zeta^{2r} = \mu\zeta^r u \pmod p$

finalement

$a+b\zeta - a\zeta^{2r} - b\zeta^{2r-1} = 0 \pmod p$

voyons les cas : $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$

on a: $1 \neq \zeta$, $\zeta \neq \zeta^{2r}$, $\zeta^{2r} \neq \zeta^{2r-1}$ il ne reste 3 cas:

$\rightarrow 1=\zeta^{2r} \Rightarrow b\zeta - b\zeta^{2r-1} = 0 \pmod p \Rightarrow$ d'après-(1) $p|b \Rightarrow$ impossible

$\rightarrow \zeta=\zeta^{2r-1} \Rightarrow a - a\zeta^{2r} = 0 \pmod p \Rightarrow$ d'après-(1) $p|a \Rightarrow$ impossible

$\rightarrow 1=\zeta^{2r-1} \Rightarrow (a-b) - (a-b)\zeta = 0 \pmod p \Rightarrow$ d'après-(1) $p|(a-b) \Leftrightarrow a = b \pmod p$

or

$a^p + b^p = c^p \pmod p$

$a + b = c \pmod p$

En permutant la solution $(a,b,c) \rightarrow (c,-a,b)$ on aura

$c = -a \pmod p$

d'où

$a + a = -a \pmod p$

$3a = 0 \pmod p$

$p|3a$

comme $p \nmid a \Rightarrow p|3$ impossible car $p \geq 5$

Donc l'équation de Fermat L_p n'a pas de solution de type 1.

Cas II: Solution de type 2

$$\begin{cases} a^p + b^p = c^p \\ (a,b,c) = 1 \\ abc = 0 \pmod p \end{cases}$$

On peut supposer que p|c.

Au lieu de résoudre L_p on va résoudre l'équation suivante: M_p avec les inconnues (x,y,z,u,v) :

M_p: $x^p + y^p = u\lambda^{vp} z^p$

où x,y,z $\in \mathbb{Z}[\zeta]$, x,y,z premiers entre eux 2à2,

u=unité, λ=1-ζ, v≥2 entier naturel

p premier régulier ≥5

Si M_p n'a pas de solution, L_p n'a pas de solution de type 2 non plus, en effet si L_p admet une solution (a,b,c) de type 2 on aura :

$a^p + b^p = c^p$, avec p|c

ce qui donne:

c = pc'

$c^p = p^p c'^p = \omega^p \lambda^{(p-1)p} c'^p$; ($p=\omega(1-\zeta)^{p-1}$, ω=unité)

$a^p + b^p = \omega^p \lambda^{(p-1)p} c'^p$

et $(a,b,c',\omega^p,p-1)$ serait une solution de M_p .

Résolution M_p :

Supposons que M_p admet une solution (a,b,c,μ,m)

$$a^p + b^p = \mu\lambda^{mp} c^p$$

En factorisant le membre de gauche, ça donne:

$$\prod_{i=0}^{p-1}\left(a + b\zeta^i\right) = \mu\lambda^{mp} c^p$$

en passant par les idéaux

$$\prod_{i=0}^{p-1}\langle a + b\zeta^i\rangle = \langle\lambda\rangle^{mp}\langle c\rangle^p$$

Note : L'arithmétique dans (𝕀,+,.) est exactement comme l'arithmétique dans (ℕ,+,.)

Contrairement au premier cas I, les facteurs $\langle a + b\zeta^i\rangle$ ne sont pas premiers entre eux 2à2. Le but est de savoir exactement que "contiennent" ces facteurs $\langle a + b\zeta^i\rangle$.

Pour bien comprendre ce qu'on veut, ce qu'on fait on va prendre un exemple :

On a p = trous, et np lamda λ à distribuer dans ces trous, pour fixer les idées on prend p=4 et n=2 on a donc 4 trous et 8 lamda λ, ex de distributions :

distribution1 : 1, 3, 2, 2

distribution2 : 3, 2, 0, 3

distribution3 : 2, 2, 2, 2

.....

On va démontrer qu'on a en réalité la distribution suivante:

distribution : 5,1,1,1

càd tout vaut 1 sauf le 1er qui a le reste des lambda λ .

Autrement dit on veut montrer que $\langle\lambda\rangle^t$ divise $\langle a + b\rangle$, avec $t\geq 2$ et $\langle\lambda\rangle$ divise <u>exactement</u> $\langle a + b\zeta^i\rangle$ pour $1\leq i\leq p-1$, et ça se fait en 4 étapes.

Allons-y:

<u>étape 1 ($\langle\lambda\rangle$M, $\langle\lambda\rangle$M, $\langle\lambda\rangle$M, ..., $\langle\lambda\rangle$M)</u> : $\langle\lambda\rangle$ divise tous les $\langle a + b\zeta^i\rangle$

on a:

$$\langle\lambda\rangle | \prod_{i=0}^{p-1} \langle a + b\zeta^i\rangle$$

$\langle\lambda\rangle$ est premier , il divise donc l'un des facteurs $\langle a + b\zeta^i\rangle$, disons $\langle a + b\rangle$,

$\langle\lambda\rangle | \langle a + b\rangle$ (1^*)

→ si $\langle\lambda\rangle$ divise $\langle a + b\zeta^h\rangle$ par ex, il suffit de prendre $b'=b\zeta^h$, celà revient à permuter les facteurs, par ex si on prend p=7 et h=4 ça donne:

$\langle a + b\zeta^4\rangle\langle a + b\zeta^5\rangle\langle a + b\zeta^6\rangle\langle a + b\rangle\langle a + b\zeta\rangle\langle a + b\zeta^2\rangle\langle a + b\zeta^3\rangle$

$\langle a + b' \rangle \langle a + b'\zeta \rangle \langle a + b'\zeta^2 \rangle \langle a + b'\zeta^3 \rangle \langle a + b'\zeta^4 \rangle \langle a + b'\zeta^5 \rangle \langle a + b'\zeta^6 \rangle$

on a l'identité :

$(a+b\zeta^i) - (a+b) = -b(1- \zeta^{i-1}) = -\varepsilon b(1-\zeta)$, ε=unité $1 \leq i \leq p-1$

$\lambda | [(a+b\zeta^i) - (a+b)]$

Avec (1^*) ce qui montre que $\langle \lambda \rangle$ divise tous les facteurs $\langle a + b\zeta^i \rangle$

$\langle \lambda \rangle | \langle a + b\zeta^i \rangle \, , 0 \leq i \leq p - 1$

étape 2 ($\langle \lambda \rangle^{t \geq 2} M, \langle \lambda \rangle M, \langle \lambda \rangle M, ..., \langle \lambda \rangle M$) : $\langle \lambda \rangle^t$ ($t \geq 2$) divise $\langle a + b\zeta^i \rangle$ et $\langle \lambda \rangle$ divise exactement $\langle a + b\zeta^i \rangle$ pour $1 \leq i \leq p-1$:

Comme $\{1, \lambda, \lambda^2, ..., \lambda^{p-1}\}$ est une base de $\mathbb{Z}[\zeta]$ (car les λ^i s'expriment en fonction de ζ^k) on peut écrire :

$$a = \sum_{i=0}^{p-1} a_i \lambda^i \, , a_i \in \mathbb{Z}$$

$$b = \sum_{i=0}^{p-1} b_i \lambda^i \, , b_i \in \mathbb{Z}$$

$$\lambda^i = (1 - \zeta)^i = \sum_{k=0}^{i} \binom{i}{k} (-\zeta)^k$$

$a = a_0 + a_1\lambda \pmod{\lambda^2}$

$b = b_0 + b_1\lambda \pmod{\lambda^2}$

$\lambda^i = 1 - i\zeta \pmod{\lambda^2}$

$a + b\zeta^i = (a_0 + b_0) + (a_1 + b_1 - ib_0)\lambda \pmod{\lambda^2}$

or

$a + b\zeta^i = 0 \pmod{\lambda}$

$a + b\zeta^i = (a_0 + b_0) \pmod{\lambda}$

$(a_0 + b_0) = 0 \pmod{\lambda}$

donc

$a + b\zeta^i = d\lambda + (a_1 + b_1 - ib_0)\lambda \pmod{\lambda^2}$

$a + b\zeta^i = \xi_i\lambda \pmod{\lambda^2}$

Les $\xi_i\lambda$ $(0 \leq i \leq p-1)$ sont tous distincts ça signifie qu'on a toutes les classes de $\mathbb{Z}[\zeta]/\lambda^2$ (il y en a p classes) donc parmi ces classes on a la classe zéro 0, et les autres $\neq 0$, autrement dit il existe un unique h tel que

$a + b\zeta^h = 0 \pmod{\lambda^2}$

et les autres

$a + b\zeta^i \neq 0 \pmod{\lambda^2}$, pour $i \neq h$

On peut supposer h=0, donc

$\lambda^2 | (a + b)$

et λ divise exactement $(a + b\zeta^i)$, $1 \leq i \leq p-1$, càd $(a + b\zeta^i)$ "contient" un seul λ.

$\lambda | (a + b\zeta^i)$ pour $1 \leq i \leq p-1$

ou encore en passant par les idéaux

$\langle\lambda\rangle^2 Q_0 = \langle a + b\rangle \, , Q_0 \in \mathbb{I}$

$\langle\lambda\rangle Q_i = \langle\lambda\rangle\langle a + b\zeta^i\rangle \quad , 1 \leq i \leq p - 1 \, , Q_i \in \mathbb{I}$

étape 3 ($\langle\lambda\rangle^{t\geq 2}$, $\langle\lambda\rangle$, $\langle\lambda\rangle$, ..., $\langle\lambda\rangle$) : Il n'y a que les $\langle\lambda\rangle$ qui divisent les $\langle a + b\zeta^i\rangle$.

Voyons si $\langle a + b\zeta^i\rangle$ contient autre chose $M \in \mathbb{I}$ que les $\langle\lambda\rangle$. Supposons que M divise $\langle a + b\zeta^i\rangle$ et $\langle a + b\zeta^j\rangle$, $0 \leq j < i \leq p-1$

$M|\langle a + b\zeta^i\rangle$ et $M|\langle a + b\zeta^j\rangle$

$(a+b\zeta^j) - (a+b\zeta^i) = b\zeta^j(1-\zeta^{i-j}) = \varepsilon b(1-\zeta)$,ε=unité

$(a+b\zeta^j) + [-(a+b\zeta^i)] = \varepsilon b(1-\zeta)$

$\langle a + b\zeta^i\rangle + \langle a + b\zeta^j\rangle = \langle b\rangle\langle\lambda\rangle$

d'où

$M|\langle b\rangle\langle\lambda\rangle$

Comme $\langle\lambda\rangle$ est premier on a

$M|\langle b\rangle$

On a l'identité:

$(a+b\zeta^j) - \zeta^{j-i}(a+b\zeta^i) = a(1-\zeta^{j-i}) = \varepsilon a(1-\zeta)$,ε=unité

$(a+b\zeta^j) + [-\zeta^{j-i}(a+b\zeta^i)] = \varepsilon a(1-\zeta)$

$\langle a + b\zeta^j\rangle + \langle a + b\zeta^i\rangle = \langle a\rangle\langle\lambda\rangle$

$M|\langle a\rangle\langle\lambda\rangle$

Comme $\langle\lambda\rangle$ est premier on a

$M|\langle a\rangle$

Mais par l'hypothèse $(a,b)=1 \Rightarrow (\langle a\rangle,\langle b\rangle)=\langle 1\rangle$, donc $\langle a + b\zeta^i\rangle$ ne contient que des $\langle\lambda\rangle$.

$\langle\lambda\rangle^2 Q_0 = \langle a + b\rangle$

$\langle\lambda\rangle Q_i = \langle a + b\zeta^i\rangle \quad , 1 \leq i \leq p-1$

étape 4 ($\langle\lambda\rangle^{mp-(p-1)}$, $\langle\lambda\rangle$, $\langle\lambda\rangle$, ..., $\langle\lambda\rangle$) : On $a\langle\lambda\rangle^{mp-(p-1)}|\langle a + b\rangle$ et $\langle\lambda\rangle|\langle a + b\zeta^i\rangle$, $1\leq i\leq p-1$

On a:

$$\prod_{i=0}^{p-1}\langle a + b\zeta^i\rangle = \langle\lambda\rangle^{mp}\langle c\rangle^p$$

Or dans le produit à gauche on a $\langle\lambda\rangle^{p+1}$ il manque disons $\langle\lambda\rangle^h$ (à cause de la décomposition unique des idéaux), on doit donc avoir:

$(p+1)+h = mp$

$h = mp - p - 1$

Comme chaque $\langle a + b\zeta^i\rangle$ $(1\leq i\leq p-1)$ contient exactement un $\langle\lambda\rangle$, $\langle a + b\rangle$ contient alors $\langle\lambda\rangle^{2+h}$:

$\langle\lambda\rangle^{mp-p+1} Q_0 \ \langle\lambda\rangle Q_1 \langle\lambda\rangle Q_2 \ldots \ \langle\lambda\rangle Q_{p-1}$

Soient:

$\langle\lambda\rangle^{mp-p+1}Q_0 = \langle a+b\rangle$

$\langle\lambda\rangle Q_i = \langle a+b\zeta^i\rangle \quad , 1\leq i\leq p-1$

En résumé:

$\langle\lambda\rangle^{mp-p+1}Q_0\,\langle\lambda\rangle^{p-1}Q_1\,Q_2 \ldots Q_{p-1} = \langle\lambda\rangle^{mp}\langle c\rangle^p$

$Q_0\,Q_1\,Q_2 \ldots Q_{p-1} = \langle c\rangle^p$

$$\prod_{i=0}^{p-1} Q_i = \langle c\rangle^p$$

On va montrer que les Q_i ($0\leq i\leq p-1$) sont premiers entre eux 2à2.

Supposons le contraire $Q\in\mathbb{I}$

$Q|Q_i$ et $Q|Q_j$

$\langle\lambda\rangle QK_i = \langle a+b\zeta^i\rangle \ , K_i \in \mathbb{I}$

$\langle\lambda\rangle QK_j = \langle a+b\zeta^j\rangle \ , K_j \in \mathbb{I}$

$\langle\lambda\rangle Q \mid \langle a+b\zeta^i\rangle$

$\langle\lambda\rangle Q \mid \langle a+b\zeta^j\rangle$

On a l'identité:

$(a+b\zeta^j) + [-(a+b\zeta^i)] = \varepsilon b(1-\zeta)$, ε=unité

$\langle a+b\zeta^j\rangle + \langle a+b\zeta^i\rangle = \langle b\rangle\langle\lambda\rangle$

$\langle\lambda\rangle Q \mid \langle b\rangle\langle\lambda\rangle$

$Q|\langle b\rangle$

Et

$(a+b\zeta^j) + [-\zeta^{j-i}(a+b\zeta^i)] = a(1-\zeta^{j-i}) = \varepsilon a(1-\zeta)$,ε=unité

$\langle a + b\zeta^j\rangle + \langle a + b\zeta^i\rangle = \langle a\rangle\langle\lambda\rangle$

$\langle\lambda\rangle Q|\langle a\rangle\langle\lambda\rangle$

$Q|\langle a\rangle$

ce qui contredit le pgcd($\langle a\rangle$,$\langle b\rangle$) = $\langle 1\rangle$.

Donc les Q_i sont premiers entre eux 2à2.

$Q_0\, Q_1\, Q_2 \ldots Q_{p-1} = \langle c\rangle^p$

Comme p est régulier, ce qui montre que les Q_i sont eux même une puissance de p.

$Q_i = T_i^p \quad (0\leq i\leq p-1)$

d'où

$\langle\lambda\rangle^{mp-p+1} T_0^p = \langle a + b\rangle$

$\langle\lambda\rangle T_i^p = \langle a + b\zeta^i\rangle\,, 1 \leq i \leq p-1$

On va maintenant montrer que T_0^p et T_i^p sont principaux :

$\lambda^2|(a + b)$

$\lambda|(a + b\zeta^i)$ pour $1\leq i\leq p-1$

$(a+b) = \lambda^2\theta_0$, $\theta_0\in\mathbb{Z}[\zeta]$

$(a+b\zeta^i) = \lambda\theta_i$, $\theta_i \in \mathbb{Z}[\zeta]$, $1 \leq i \leq p-1$

$\lambda^2\theta_0 \ \lambda\theta_1 \lambda\theta_2 \ldots \ \lambda\theta_{p-1} = \mu\lambda^{mp} c^p$

en passant par les idéaux

$\langle\lambda\rangle^2\langle\theta_0\rangle \langle\lambda\rangle\langle\theta_1\rangle\langle\lambda\rangle\langle\theta_2\rangle \ \ldots \ \langle\lambda\rangle\langle\theta_{p-1}\rangle = \langle\lambda\rangle^{mp}\langle c\rangle^p$

L'unicité de la décomposition oblige que le membre de gauche comporte autant de $\langle\lambda\rangle$ que le membre de droite. Et on sait que chaque $\langle a + b\zeta^i\rangle$ contient un seul $\langle\lambda\rangle$ sauf le premier $\langle a + b\rangle$ qui contient le reste des $\langle\lambda\rangle$

d'où

$\langle\lambda\rangle^{mp-p+1}\langle\theta_0\rangle \langle\lambda\rangle\langle\theta_1\rangle\langle\lambda\rangle\langle\theta_2\rangle \ \ldots \ \langle\lambda\rangle\langle\theta_{p-1}\rangle = \langle\lambda\rangle^{mp}\langle c\rangle^p$

on descend dans $\mathbb{Z}[\zeta]$

$$\lambda^{mp-p+1}\theta_0 \prod_{i=1}^{p-1}(\lambda\theta_i) = \ \mu\lambda^{mp} c^p$$

Soient

$a + b = \lambda^{mp-p+1}\theta_0 \ \ , \theta_0 \in \mathbb{Z}[\zeta]$

$a + b\zeta^i = \lambda\theta_i \ \ , \theta_i \in \mathbb{Z}[\zeta] \ , 1 \leq i \leq p-1$

finalement

$\langle\lambda\rangle^{mp-p+1} T_0^p = \langle\lambda\rangle^{mp-p+1}\langle\theta_0\rangle$

$\langle\lambda\rangle T_i^p = \langle\lambda\rangle\langle\theta_i\rangle \ , 1 \leq i \leq p-1$

$T_0^p = \langle \theta_0 \rangle$

$T_i^p = \langle \theta_i \rangle$, $1 \leq i \leq p-1$

T_0^p , T_i^p sont principaux et comme p est regulier T_0 et T_i sont eux même principaux.

$T_0 = \langle \alpha_0 \rangle$, $\alpha_0 \in \mathbb{Z}[\zeta]$

$T_i = \langle \alpha_i \rangle$, $1 \leq i \leq p-1$ et $\alpha_i \in \mathbb{Z}[\zeta]$

Montrons tout de suite que α_1 et α_2 sont premiers entre eux.

$\langle \lambda \rangle \langle \alpha_i \rangle^p = \langle a + b\zeta^i \rangle$

en descendant sur $\mathbb{Z}[\zeta]$, ça donne:

$\lambda \alpha_i^p \varepsilon_i = a + b\zeta^i$, $\varepsilon_i =$ unité

$$\begin{cases} \lambda \alpha_1^p \varepsilon_1 = a + b\zeta \\ \lambda \alpha_2^p \varepsilon_2 = a + b\zeta^2 \end{cases}$$

le calcul donne

$a = -\zeta \alpha_1^p \varepsilon_1 + \alpha_2^p \varepsilon_2$

$b = \alpha_1^p \varepsilon_1 \zeta^{p-1} - \alpha_2^p \varepsilon_2 \zeta^{p-1}$

d'où $(\alpha_1, \alpha_2)=1$ car $(a,b)=1$. On a bien α_1 et α_2 sont premiers entre eux (*2) .

Nous avions montré que :

$\langle a + b \rangle = \langle \lambda \rangle^{mp-p+1} \langle \alpha_0 \rangle^p$

$\langle a + b\zeta^i \rangle = \langle \lambda \rangle \langle \alpha_i \rangle^p$, $1 \leq i \leq p-1$

et on tire:

$\langle a + b \rangle \langle \alpha_i \rangle^p = \langle \lambda \rangle^{mp-p+1} \langle \alpha_i \rangle^p \langle \alpha_0 \rangle^p$

$\langle a + b \rangle \langle \alpha_i \rangle^p = \langle \lambda \rangle^{(m-1)p} \langle \lambda \rangle \langle \alpha_i \rangle^p \langle \alpha_0 \rangle^p$

$\langle a + b \rangle \langle \alpha_i \rangle^p = \langle \lambda \rangle^{(m-1)p} \langle a + b\zeta^i \rangle \langle \alpha_0 \rangle^p$

puis on descend dans $\mathbb{Z}[\zeta]$

$\mu_i (a + b) \alpha_i^p = \lambda^{(m-1)p} (a + b\zeta^i) \alpha_0^p$; $\mu_i =$ unité

or on a l'identité :

$(a+b\zeta)(1+\zeta) - (a+b\zeta^2) = (a+b)\zeta$

en multipliant par $\lambda^{(m-1)p} \alpha_0^p$

$\lambda^{(m-1)p}(a+b\zeta)\, \alpha_0^p\, (1+\zeta) - \lambda^{(m-1)p}(a+b\zeta^2)\, \alpha_0^p = (a+b)\zeta\, \lambda^{(m-1)p}\, \alpha_0^p$

d'où, en prenant i=1, 2 :

$\mu_1 (a + b) \alpha_1^p\, (1+\zeta) - \mu_2 (a + b) \alpha_2^p = \zeta\, \lambda^{(m-1)p}\, (a+b)\, \alpha_0^p$

$\mu_1 \alpha_1^p (1+\zeta) - \mu_2 \alpha_2^p = \zeta\, \lambda^{(m-1)p}\, \alpha_0^p$

$$\alpha_1^p - \frac{\mu_2}{\mu_1\,(1+\zeta)} \alpha_2^p = \frac{\zeta}{\mu_1\,(1+\zeta)} \lambda^{(m-1)p} \alpha_0^p$$

comme ζ et $(1+\zeta)$ sont des unités

$$\Rightarrow \frac{\mu_2}{\mu_1 (1+\zeta)} = \varepsilon \text{ unité}$$

$$\Rightarrow \frac{\zeta}{\mu_1\,(1+\zeta)} = \nu \text{ unité}$$

$\alpha_1^p - \varepsilon\,\alpha_2^p = \nu\,\lambda^{(m-1)p}\,\alpha_0^p$

Il faut maintenant faire entrer ε dans $(\alpha_2)^p$

$\alpha_1^p - \varepsilon\,\alpha_2^p = \nu\,\lambda^{(m-1)p}\,\alpha_0^p$

Comme $m\geq 2 \Rightarrow (m-1)p \geq p$, d'où

$\alpha_1^p - \varepsilon\,\alpha_2^p = 0 \pmod{\lambda^p}$

$\alpha_1^p - \varepsilon\,\alpha_2^p = 0 \pmod p$, car $p=\omega\lambda^{p-1}$,ω=unité

$h_1 - \varepsilon\,h_2 = 0 \pmod p$ avec $h_1,h_2 \in \mathbb{Z}$, Lemme (8.1.1)

on a: $h_2 \neq 0 \pmod p$ si non $h_1=0 \pmod p$ et (α_1, α_2) ne seront pas premiers entre eux (voit (*2)) :

$\alpha_1^p = h_1 \pmod p \Rightarrow \alpha_1^p = 0 \pmod p$

$\alpha_2^p = h_2 \pmod p \Rightarrow \alpha_2^p = 0 \pmod p$

$p \mid \alpha_1^p \Rightarrow p \mid \alpha_1$

$p \mid \alpha_2^p \Rightarrow p \mid \alpha_2$

donc il existe un h_2' entier tel que

$h_2'\,h_2 = 1 \pmod p$

$h_2'h_1 - \varepsilon\,h_2'h_2 = 0 \pmod p$

$h_2'h_1 - \varepsilon = 0 \pmod p$

$\varepsilon = h_2'h_1 \pmod p$ avec $h_2'h_1 \in \mathbb{Z}$

Donc , d'après le lemme des unités-2, ε est de la forme:

$\eta^p = \varepsilon$, où η=unité

$\alpha_1^p + (-\eta\alpha_2)^p = \nu\,\lambda^{(m-1)p}\,\alpha_0^p$

Si on pose:

$\alpha_1 = a'$, $-\eta\alpha_2 = b'$, $\alpha_0 = c'$, $\nu = \mu'$, $m-1 = m'$

alors l'équation devient

$(a')^p + (b')^p = \mu'\lambda^{m'p}(c')^p$

Ici on prend $\vartheta = m$

à partir de la solution (a,b,c,μ,m) on trouve une autre solution (a',b',c',μ',m') plus petite que (a,b,c,μ,m) : $\vartheta' = m' = m-1 < m = \vartheta$ donc avec la descente infinie ce n'est pas possible, autrement dit la solution (a,b,c,μ,m) n'existe pas donc l'équation M_p n'a pas de solutions, par conséquent l'équation L_p elle non plus n'a pas de solution de type 2 .

En résumé, la conjecture de Fermat est vraie pour les nombres premiers réguliers p.

Commentaire :

1) Il fallait attendre 211 ans (1847-1636=211) pour avoir une grande avancée dans la résolution de la conjecture de Fermat. C'est assez dommage que la méthode de Kummer ne permet pas de démontrer la conjecture. En effet il y a une infinité de cas où la méthode n'a pas traité: les

nombre premiers irréguliers. Et puis on ne sait pas si on a traité une infinité de cas réguliers ou non ? Bref la seule consolation c'est que la conjecture est vraie pour beaucoup de valeurs de n .... (voir la liste des nombres premiers réguliers)

Alors qu'avant Kummer on sait seulement que la conjecture est vraie pour :

n =3, 4, 5, 7, 14 c'est tout !!!

2) En examinant la démonstration, on pense que Fermat s'est trompé au niveau :

$\mathbb{Z}[\zeta]$ est principal $\forall p$!!

Alors que ceci n'est vrai que pour $p \leq 19$, pour $p \geq 23$, $\mathbb{Z}[\zeta]$ n'est pas principal !

9 FORME MODULAIRE

9.1 FORME MODULAIRE DE NIVEAU N

Définition une fonction modulaire :

On pose $\mathcal{H}$ = {τ=u+vi ∈ℂ / Im(τ)=v > 0} le demi-plan de Poincaré.

Soit f une fonction définie sur $\mathcal{H}\to\mathbb{C}$

f: $\mathcal{H} \to \mathbb{C}$

$\tau \to f(\tau)$

On dit que f est une fonction modulaire de niveau N (de poids k) si elle vérifie :

1. Holomorphe sur $\mathcal{H}$.

2. La modularité :

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau)$$

où

$\Gamma_0(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a,b,c,d ∈ℤ, ad-cb=1 et N|c }

3. Admet un q-développement :

$$F(q) = \sum_{n \geq -h}^{\infty} b_n q^n \text{ , convergeant pour } 0 < |q| < 1$$

tel que

$F(e^{2\pi i\tau}) = f(\tau)$.

Une forme modulaire est une série ayant des propriétés très symétriques ...

Définition une forme modulaire :

Soit F la série définie par :

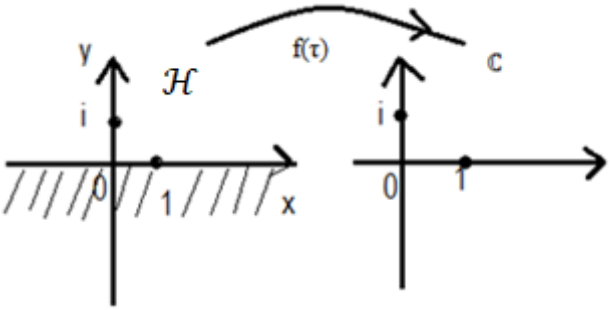
$$F = \sum_{n \geq -h}^{\infty} b_n q^n \text{ , convergeant pour } 0 < |q| < 1$$

F a un nombre fini d'indices n négatifs.

F = la série "en q", la série de "paramètre q" etc ...

et soit $f(\tau)$ la fonction définie par:
$f: \mathcal{H} \to \mathbb{C}$
$\tau \to f(\tau)$

$$f(\tau) = \sum_{n \geq -h}^{\infty} b_n e^{2\pi i \tau n} \text{ ; avec les même } b_n$$



Si la fonction f(τ) vérifie:

1. Holomorphe sur $\mathcal{H}$.

2. La modularité :

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau)$$

où

$$\Gamma_0(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ où } a,b,c,d \in \mathbb{Z}, \text{ ad-cb=1 et } N|c \}$$

On dit que F est une forme modulaire de niveau N (de poids k) .

Lorsque $n \geq 1$, et $b_1=1$ on dira que F est une forme parabolique ($b_0=0$, pas de terme constant) mais pour nous on gardera le mot "modulaire" pour ne pas introduire de nouveaux vocabulaires, donc on dit simplement que c'est une forme modulaire.

On dit que F est la q-série de $f(\tau)$, et que $f(\tau)$ est la fonction modulaire de F.

Remarque : Comme $f(\tau)$ est périodique de période 1, $f(\tau)$ admet un développement de Fourier

$f(\tau+1) = f(\tau)$

$$f(\tau) = \sum_{n\in\mathbb{Z}} b_n e^{2\pi i\tau n}$$

Pour retrouver F à partir de $f(\tau)$ il suffit de prendre les coefficients de Fourier b_n avec $b_n=0$ pour $n<-h$, et former la q-série :

$$F = \sum_{n\geq -h} b_n q^n \ ; 0 < |q| < 1, q = e^{2\tau i\tau}$$

Ne pas confondre F (une série) avec $f(\tau)$ qui est une fonction.

On note $S_2(N)$ l'ensemble des formes modulaires de niveau N (de poids 2 avec $n\geq 1$ et $b_1 = 1$), c'est un $\mathbb{C}$-esv, et $S_k(N)$ l'ensemble de formes modulaires de niveau N, de poids k .

On pose :

g = dim $S_2(N)$ et on démontre que:

$1 \leq N \leq 10$, g=0 (très important)

N=11 , g=1

N=12, 13 , g=0

et pour certaine valeur de N premier impair on a les formules suivantes:

$$g = \frac{N-13}{12} \text{ si } N = 1 \pmod{12}$$

$$g = \frac{N-5}{12} \text{ si } N = 5 \pmod{12}$$

$$g = \frac{N-7}{12} \text{ si } N = 7 \pmod{12}$$

$$g = \frac{N+1}{12} \text{ si } N = 11 \pmod{12}$$

exemple N=37

$$g = \frac{37-13}{12} = 2 \text{ car } 37 = 1 \pmod{12}$$

Exemples des formes modulaires:

Soit

$\tau \in \mathcal{H} = \{\tau = u+vi \text{ , } v>0\}$

$\Lambda = \mathbb{Z}+\mathbb{Z}\tau = \{\omega = a+b\tau \text{ avec } a,b \in \mathbb{Z}\} = \mathbb{Z}[\tau]$

$\Lambda^* = \Lambda - \{(0,0)\}$

On définit la fonction d'Eisenstein $\varphi_{2k}(\tau)$ par :

$$\varphi_{2k}(\tau) = \sum_{\omega \in \Lambda^*} \frac{1}{\omega^{2k}} = \sum_{(a,b) \neq (0,0) \in \mathbb{Z}^2} \frac{1}{(a+b\tau)^{2k}}$$

et

$$g_2(\tau) = 60 \sum_{\omega \in \Lambda^*} \frac{1}{\omega^4} = 60\varphi_4(\tau)$$

$$g_3(\tau) = 140 \sum_{\omega \in \Lambda^*} \frac{1}{\omega^6} = 140\varphi_6(\tau)$$

Voici les trois fonctions modulaires très connues:

$$\varphi_{2k}(\tau) = \sum_{(a,b)\neq(0,0)\in\mathbb{Z}^2} \frac{1}{(a+b\tau)^{2k}}$$

$$\delta(\tau) = \frac{g_2^3(\tau) - 27g_3^2(\tau)}{(2\pi)^{12}}$$

$$j(\tau) = 1728\frac{g_2^3(\tau)}{\delta(\tau)}$$

on a:

$$\varphi_{2k}\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{2k}\varphi_{2k}(\tau)$$

$$\delta\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{12}\delta(\tau)$$

$$j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau)$$

Leur q-séries (les formes modulaires correspondantes):

$$\rightarrow \Phi_{2k} = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!}\sum_{n\geq 1}\sigma_{2k-1}(n)q^n$$

où

$$\sigma_k(n) = \sum_{d|n} d^k$$

somme des k-puissances des diviseurs de n

Φ_{2k} = forme modulaire de poids 2k de niveau N=1.

$\Phi_{2k} \in S_{2k}(1)$

$$\rightarrow \Delta = q \sum_{n \geq 1} (1 - q^n)^{24}$$

$= q - 24q^2 + 252q^3 - 1472q^4 + \ldots$

Δ = forme modulaire de poids 12 de niveau 1.

$\Delta \in S_{12}(1)$

$$\rightarrow J = \frac{1}{q} + 744 + 196884q + \ldots$$

J = forme modulaire de poids 0 de niveau 1.

$J \in S_0(1)$

Rappel: $\zeta(2) = \frac{\pi^2}{6}$; $\zeta(4) = \frac{\pi^4}{90}$; $\zeta(6) = \frac{\pi^6}{945}$

$$\Phi_4 = \frac{4}{3}\pi^4 (1 + 240 \sum_{n \geq 1}^{\infty} \sigma_3(n) q^n)$$

$$= \frac{4}{3}\pi^4 (1 + 240q + \cdots)$$

$$\Phi_6 = \frac{8}{27}\pi^6(1 - 504\sum_{n\geq 1}^{\infty}\sigma_5(n)q^n)$$

$$= \frac{8}{27}\pi^6(1 - 504q + \cdots)$$

autres exemples :

$$F = q\prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2$$

$F = q-2q^2-q^3+2q^4+q^5+2q^6-2q^7-2q^9-2q^{10}+q^{11}-2q^{12}+\ldots$

$$F = \sum_{n\geq 1}^{\infty} b_n\, q^n$$

$F \in S_2(11)$ (remarque, on a : $b_0 = 0$, $b_1 = 1$)

10 COURBE ELLIPTIQUE SUR $\mathbb{Q}$

10.1 MODÈLE DE WEIERSTRASS

Une courbe elliptique $\mathcal{E}$ définie sur $\mathbb{Q}$, donnée par l'équation E:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ , a_i \in \mathbb{Q}$$

est une courbe algébrique, de degré 3, lisse et muni d'un point Θ nommé point à l'infini .

Note: par abus de langage, on confond parfois $\mathcal{E}$ et E : la courbe $\mathcal{E}$ et sa équation E, sa représentation .

Le point Θ n'est pas dans plan !! il est à l'extérieur du plan , quelque part ... on dit qu'il est à infini !!

Traditionnellement on note $\Theta = (0,1,0)$, pour voir pourquoi il faut passer par l'équation homogène de la courbe :

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \ , a_i \in \mathbb{Q}$$

(on complète Z pour avoir les monômes de degré 3)

dans cette écriture on doit avoir :

1) $(X,Y,Z) \neq (0,0,0)$

2) $(\alpha X,\alpha Y,\alpha Z) = (X,Y,Z)$ avec $\alpha \neq 0$ (*3)

¤ $Z \neq 0 \Longrightarrow (X,Y,Z) = (X/Z,Y/Z,1)$; d'après (*3)

on pose $x=X/Z$ et $y=Y/Z$ on a donc un correspondant

$(x, y,1) \longrightarrow (x, y)$

¤ $Z = 0 \Longrightarrow$ l'équation homogène montre que $X = 0$ donc

$(0,Y,0) = (0,1,0)$, d'après (*3)

le point (0,1,0) ne correspond à aucun point du plan on le nomme simplement le point à l'infini et on le note aussi $\Theta=(\infty,\infty)$

Attention !!

1) $\Theta \neq O = (0,0)$ l'origine car : $(0,0)\longrightarrow(0,0,1) \neq (0,1,0)$

2) $\Theta \neq (0,1)$ car : $(0,1)\longrightarrow(0,1,1) \neq (0,1,0)$.

On va noter $E(\mathbb{Q})$, $E(\mathbb{C})$: les points de $\mathcal{E}$ à coordonnées dans $\mathbb{Q}$, dans $\mathbb{C}$.

Les points de $\mathcal{E}$ sont les points à coordonnées algébriques $E(\overline{\mathbb{Q}})$

On verra que Θ joue le rôle d'élément neutre du groupe $(E(\overline{\mathbb{Q}}),+)$ de la courbe $\mathcal{E}$, sans lui on ne peut pas munir une structure de groupe sur $\mathcal{E}$.

Traditionnellement on utilise les modèles de Weierstrass comme équation pour la courbe $\mathcal{E}$:

Modèle 1 (standard):

E : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbb{Z}$ (°)

avec $\Delta \neq 0$ où

$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$

et les coefficients b_i sont donnés par :

$b_2 = a_1^2 + 4a_2$

$b_4 = a_1 a_3 + 2a_4$

$b_6 = a_3^2 + 4a_6$

$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2$

(on a aussi: $4b_8 = b_2 b_6 - b_4^2$)

les coefficients c_i sont aussi utiles

$c_4 = b_2^2 - 24b_4$

$c_6 = -b_2^3 + 36b_2 b_4 - 216b_6$

$\Delta = \dfrac{c_4^3 - c_6^2}{1728}$

On définit aussi le j-invariant de E

$j = \dfrac{c_4^3}{\Delta}$

$j = 1728 \dfrac{c_4^3}{c_4^3 - c_6^2}$

Le Δ se nomme le discriminant de E

($\Delta \neq 0$ signifie que la courbe est lisse $\Rightarrow$ courbe elliptique)

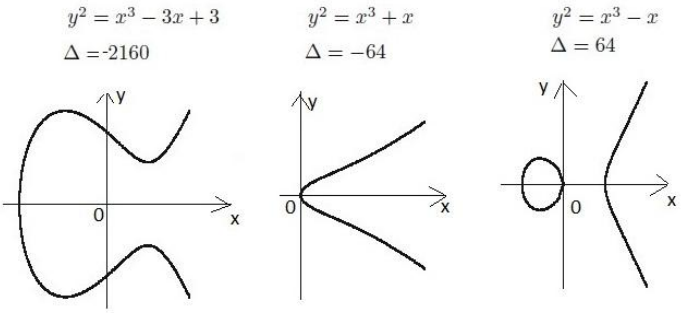
(°) Si les coefficients a_i sont dans $\mathbb{Q}$, pour passer dans $\mathbb{Z}$ on fait par un changement de variables par K :

$$K = \begin{cases} x = u^2 x' \\ y = u^3 y' \end{cases} \quad , \qquad K = \begin{cases} x \to u^2 x \\ y \to u^3 y \end{cases}$$

où u = produit des dénominateurs des a_i

Puis on multiplie l'équation par u^6, on aura alors une équation à coefficients entiers $\in \mathbb{Z}$.

Voici quelques courbes elliptiques



<u>Rappel</u> : Le discriminant d'un polynôme P(x) de degré n est défini par :

$P(x) = ax^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = a(x - e_1)(x - e_2) \ldots (x - e_n)$

$$\Delta(P) = a^{2n-2} \prod_{i<j} (e_i - e_j)^2$$

où a=le coefficient dominant de P(x) et les e_i sont des racines de P(x) dans $\mathbb{C}$.

En particulier pour un polynôme de degré deux ou trois

¤ $P(x) = ax^2+bx+c \Rightarrow \Delta(P) = a^2(e_1 - e_2)^2 = b^2 - 4ac$

¤ $P(x) = ax^3+bx^2+cx+d \Rightarrow \Delta(P) = a^4(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$

d'après un long, très très long calcul ... on trouve :

$\Delta(P) = b^2c^2 +18abcd - 4b^3d - 4ac^3 - 27a^2d^2$

Donc ne pas confondre le discriminant $\Delta = \Delta(E)$ de E et le discriminant $\Delta(P)$ du polynôme P(x).

$P(x) = x^3 + a_2x^2 + a_4x + a_6$

qui vaut :

$\Delta(P) = a_2^2a_4^2 + 18a_2a_4a_6 - 4a_2^3a_6 - 4a_4^3 - 27a_6^2$

ou

$\Delta(P) = (e_1 - e_2)^2 (e_1 - e_3)^2 (e_2 - e_3)^2$

où les e_i sont des racines de P(x) dans $\overline{\mathbb{Q}}$ (la clôture algébrique de $\mathbb{Q}$ = les nombres algébriques) ou simplement dans $\mathbb{C}$.

$\Delta(E) = 16\Delta(P)$

<u>Modèle 2 (court)</u> :

On a aussi le model court, pour passer en model court il suffit de remplacer :

$$y \to y + \frac{a_1 x + a_3}{2}$$

$$E: y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

Modèle 3 (simplifié) :

On peut aussi utiliser le modèle simplifié, pour passer en model simplifié il suffit de remplacer :

$$x \to x + \frac{b_2}{12}$$

$$E: y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

10.2 TRANSFORMATION ADMISSIBLE

Soit E une équation de la courbe, on se demande quelles sont les transformations qui font passer de E à E' une autre équation mais qui représente toujours la même courbe elliptique $\mathcal{E}$?

On démontre que la forme de ces transformations est:

$$T = \begin{cases} x = u^2 x' + r \\ y = u^3 y' + s u^2 x' + t \end{cases}$$

$$T = \begin{cases} x \to u^2 x + r \\ y \to u^3 y + s u^2 x + t \end{cases}$$

avec $u \neq 0, r, s, t \in \mathbb{Q}$ et on notera T(u,r,s,t) une telle transformation, et on l'appellera "transformation admissible".

Lorsqu'on transforme l'équation E par T, l'équation devient E' = T(E)

$E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6 \ , a'_i \in \mathbb{Q}^{(*)}$

Et on a les relations entre les coefficients:

$ua'_1 = a_1 + 2s$

$u^3a'_3 = a_3 + ra_1 + 2t$

$u^2a'_2 = a_2 - sa_1 + 3r - s^2$

$ua'_4 = a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st$

$u^6a'_6 = a_6 + ra_4 + r^2a_2 - rta_1 - ta_3 + r^3 - t^2$

et

$u^{12}\Delta' = \Delta$

$u^4c'_4 = c_4$

$u^6c'_6 = c_6$

$j' = j$

Remarque : Comme j est le seul invariant, il est intéressant de savoir quelle est l'équation qui correspond à un j donné, voici ce qu'on prend d'habitude :

$$\begin{cases} j = 0 \rightarrow y^2 = x^3 + 1 \\ j = 1728 \rightarrow y^2 = x^3 + x \\ j \neq 0, 1728 \rightarrow y^2 = x^3 - \dfrac{36}{j - 1728}x - \dfrac{1}{j - 1728} \end{cases}$$

Note : La seule transformation

$$T = \begin{cases} x = u^2 x' \\ y = u^3 y' \end{cases} \quad , \quad T = \begin{cases} x \rightarrow u^2 x \\ y \rightarrow u^3 y \end{cases}$$

préserve la forme simplifiée $y^2 = x^3 + a_4x + a_6$ et on a les relations

$$u^4 a_4' = a_4$$

$$u^6 a_6' = a_6$$

(°) **Note:** Après la transformation les a_i' ne sont pas forcement des entiers ils sont en général des rationnels.

Mais on démontre le théorème suivant:

<u>Théorème:</u> Il existe des u,r,s,t $\in \mathbb{Q}$ tels que la transformation T(u,r,s,t) donne des a_i' entiers, $a_i' \in \mathbb{Z}$

On notera T*(u,r,s,t) qui donne des a_i' entiers, $a_i' \in \mathbb{Z}$

La transformation admissible représente la même courbe elliptique $\mathcal{E}$ c'est l'équation E qui change, la représentation E, E', ... change mais on a toujours la même courbe elliptique $\mathcal{E}$.

10.3 VALUATION DANS $\mathbb{Q}$

Soient $a \in \mathbb{Z}^*$ et p un nombre premier, on isole p dans a:

$a = p^k A$, A ne contient pas p

on pose $k = v_p(a) \in \mathbb{N}$ la valuation de a en p

$k = v_p(a) = 0 \Rightarrow$ pas de p dans a, $(a = p^0 a)$

ex: $a = 1728 = 2^6.3^3$, $b = -117 = -3^2.13$

$v_2(1728) = 6$, $v_5(1728) = 0$

$v_3(117) = 2$, $v_{13}(117) = 1$

Soit maintenant $x \in \mathbb{Q}^*$, on isole p dans x :

$$x = \frac{a}{b} = \frac{p^k A}{p^m B} = p^{k-m} \frac{A}{B}$$

où A,B ne contiennent pas p

on pose $k\text{-}m = v_p(x) \in \mathbb{Z}$ la valuation de x en p

donc $x \in \mathbb{Q}^*$, $v_p(x) \in \mathbb{Z}$

ex: $x = -1728/117$

$v_3(-1728/117) = 3\text{-}2 = 1$, $v_{13}(-1728/117) = -1$

on a les propriétés suivantes:

$v_p(xy) = v_p(x) + v_p(y)$

$v_p(x+y) \geq \inf(v_p(x) , v_p(y))$

$v_p(-x) = v_p(x)$

par convention on pose $v_p(0) = +\infty$

10.4 LE MODÈLE MINIMAL, L'ÉQUATION MINIMALE

Soit E une équation de la courbe $\mathcal{E}$.

E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ avec $a_i \in \mathbb{Z}$

et $\Delta \in \mathbb{Z}$ son discriminant .

On va "isoler" p dans Δ, c'est-à-dire mettre Δ sous la forme:

$\Delta = p^k D$, dans D il n'y a plus de p.

$k = v_p(\Delta)$, la valuation de Δ en p,

Soit T*(u,r,s,t) rappelle que c'est une transformation admissible à coefficients dans $\mathbb{Q}$ telle que les a_i' soient entiers

$T^*(E) = E'$

E': $y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$, $a_i' \in \mathbb{Z}$

<u>Définition</u> : On dit que E est minimale en p si $\forall T^*(E)=E'$

on a

$v_p(\Delta) \leq v_p(\Delta')$

Autrement dit le $v_p(\Delta)$ est minimal.

Définition : On dit que E est minimale, si E est minimale pour tout p.

Lorsqu'on transforme E par un changement admissible T*(u,r,s,t) à coefficients dans $\mathbb{Q}$, tels que les a_i' soient entiers, le discriminant change, le discriminant minimal en p c'est celui qui a le k minimal dans p^k c'est-à-dire le $v_p(\Delta)$ minimal.

Le discriminant minimal Δ_{min} est minimal pour tout p.

Autrement dit, le discriminant minimal Δ_{min} est celui qui a un $|\Delta|$ minimal. L'équation correspond à Δ_{min} se nomme l'équation minimale de E. Bien sur il y a plusieurs équations minimales mais elles sont toutes liées entre elles par une transformation admissible avec u=1 ou -1 et r,s,t dans $\mathbb{Z}$. Et si on impose

$a_1, a_3 \in \{0,1\}$ et $a_2 \in \{-1,0,1\}$

alors l'équation minimale est unique.

Exemple:

$\Delta_1 = 2.3^4.5.7^2 = 39690$

$\Delta_2 = -2^4.3^2.5^3 = -18000$

$\Delta_3 = -2^3.3^3.7^3 = -74088$

$\Delta_4 = -2.3^2 = -18$

par exemple $\Delta_2 = -2^4.3^2.5^3$ minimal en p = 3 (l'exposant de 3 est minimal) et l'équation correspond à Δ_2 est une équation minimale en p=3.

Le discriminant minimal Δ_{min} est:

$|\Delta|$ minimal $\Rightarrow \Delta_4 = \Delta_{min} = -2.3^2.5^0.7^0 = -18$

On peut dire que parmi les équations (à coefficients dans $\mathbb{Z}$)

E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ avec $a_i \in \mathbb{Z}$

1. Il y en a une minimale en p ($v_p(\Delta)$ minimal)

2. Il y en a une minimale Δ_{min} ($|\Delta|$ minimal, ou $\forall p$, $v_p(\Delta)$ minimal)

<u>Résumons nous donc</u> :

<u>Une équation minimale en p c'est</u>:

1. Les coefficients a_i sont des entiers $\in \mathbb{Z}$

2. On a $v_p(\Delta) \leq v_p(\Delta')$, quand on transforme E en E' par T*

<u>Une équation minimale c'est</u>:

1. Les coefficients a_i sont des entiers $\in \mathbb{Z}$

2. $|\Delta|$ minimal, $v_p(\Delta) \leq v_p(\Delta')$ $\forall p$, quand on transforme E en E' par T*, $\Rightarrow \Delta_{min}$

Théorème:

On peut toujours rendre une équation minimale en p, par un changement admissible.

Démonstration : Si E n'est pas minimale en p, ça signifie que le k dans $\Delta = p^k D$ n'est pas minimal, alors on va passer par la transformation T*(p,r,s,t)

et on aura un $\Delta' = \Delta/p^{12}$ avec $v_p(\Delta') < v_p(\Delta)$ donc on diminue $v_p(\Delta)$ comme $v_p(\Delta)$ est un entier, on ne peut pas le diminuer indéfiniment on s'arrête le processus à un certain moment disons k', donc il existe un minimal k' < k avec $\Delta' = p^{k'}D'$, L'équation E' correspond à Δ' c'est l'équation minimale en p. On a:

$k=k' \pmod{12}$

Théorème :

Toute courbe elliptique E sur $\mathbb{Q}$ possède une équation minimale.
c'est-à-dire il existe une équation :

E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, avec $a_i \in \mathbb{Z}$
avec Δ_{min} ($|\Delta_{min}|$=minimal)

Note: $\Delta_{min}|\Delta$ donc si $p|\Delta_{min} \Rightarrow p|\Delta$

Démonstration :

1er méthode:

Comme on peut toujours rendre une équation en une équation minimale en p, il suffit de faire ça avec tous les p

de Δ (p|Δ) on obtiendra alors une équation minimale avec un Δ_{min} .

ex: $\Delta = 3^{27}.5^{32}.7^{18} \Rightarrow \Delta_{min} = 3^{3}.5^{8}.7^{6}$

<u>2ème méthode</u>:

E est donné par une équation de type:

E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ avec $a_i \in \mathbb{Z}$

et Δ sont discriminant

Soit S

S = {|δ|, où δ=discriminant de l'équation de Weierstrass }

l'ensemble S n'est pas vide puisque |Δ|∈S car E est un model de Weierstrass, c'est un sous ensemble de ℕ non vide, $S \subset \mathbb{N}$ et $S \neq \emptyset$ donc S possède un plus petit élément |δ| = minimal, que l'on note $\Delta_{min} = \delta$ donc l'équation minimale correspondante.

Il y a bien sûr plusieurs équations minimales, mais elles sont toutes reliées par une transformation T*(u,r,s,t) avec $u=\pm1$, $r,s,t \in \mathbb{Z}$.

Autrement dit parmi les équation à coefficients entiers

E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ avec $a_i \in \mathbb{Z}$

il y en a une minimal Δ_{min} ($|\Delta_{min}|$=minimal)

Il existe un algorithme de Tate pour trouver une équation minimale, donc pas de problème, l'ordinateur le fait pour nous !

Le fait que l'équation E admet un modèle minimal, c'est parce qu'on travaille sur $\mathbb{Q}$, et que $\mathbb{Z}$ est intégralement close sur $\mathbb{Q}$, donc c'est une propriété particulière de $\mathbb{Z}$, si on change de corps $\mathbb{Q}$ en un autre corps on n'est pas sûr d'avoir un modèle minimal.

Théorème-♡ :

Soit E une équation à coefficients entiers $a_i \in \mathbb{Z}$ alors

Si $p|\Delta$ et $p \nmid c_4 \Rightarrow$ l'équation E est minimale en p

Elle est minimale, si c'est vrai pour tout p.

Démonstration :

Si E n'est pas minimale en p, alors il existe une transformation admissible T* telle que la nouvelle équation E'=T*(E) vérifie

$v_p(\Delta) > v_p(\Delta')$

or on a : $\Delta = u^{12}\Delta'$ d'où:

$v_p(\Delta) = v_p(u^{12}\Delta') = 12v_p(u) + v_p(\Delta')$

$v_p(\Delta) - v_p(\Delta') = 12v_p(u) > 0$

$v_p(u) > 0 \Rightarrow u = p^k U$ avec $k > 0$

Or $c_4 = u^4 c'_4 \Rightarrow c_4 = p^{4k} U^4 c'_4 \Rightarrow p|c_4$ ce qui contredit $p \nmid c_4$

Note: 1. Cette condition est une condition suffisante, c'est-à-dire si on a ($p|\Delta$ et $p \nmid c_4$) alors on peut dire que E est minimale en p, si on n'a pas ($p|\Delta$ et $p \nmid c_4$) on ne peut rien dire !

$\forall p$, $(p|\Delta$ et $p\nmid c_4) \Leftrightarrow pgcd(\Delta,c_4)=(\Delta,c_4)=1 \Longrightarrow$ E est minimale

2. si $v_p(\Delta) = 0$ (il n'y a pas de p dans Δ) il est claire que E est minimale en p

Proposition 1 : si $[v_p(\Delta)<12$ ou $v_p(c_4)<4$ ou $v_p(c_6)<6]$ alors E est minimale en p.

Démonstration :

I) Cas $v_p(\Delta)<12$:

On va montrer que si $v_p(\Delta)<12$ alors E est minimal en p.

Raisonnons par l'absurde: on a $v_p(\Delta)<12$, si E n'est pas minimal en p , alors il existe une transformation admissible T*, telle que T*(E)=E' avec

$0 < v_p(\Delta') < v_p(\Delta)$

or

$u^{12}\Delta' = \Delta$

d'où

$12v_p(u) + v_p(\Delta') = v_p(\Delta)$

$12v_p(u) = v_p(\Delta) - v_p(\Delta') > 0$

$(10.4.1)\, v_p(u) > 0$

d'autre part

$12v_p(u) + v_p(\Delta') = v_p(\Delta) < 12$

$12v_p(u) < 12 - v_p(\Delta')$

$v_p(u) < 1 - v_p(\Delta')/12$

comme $0 < v_p(\Delta') < v_p(\Delta) < 12 \Rightarrow 0 < v_p(\Delta')/12 < 1$

$v_p(u) < 1 - v_p(\Delta')/12 \Rightarrow v_p(u) < 1$ comme $v_p(u)$ est un entier donc

$v_p(u) \leq 0$ contradiction avec (8.4.1) $v_p(u) > 0$

II) Pour le cas $v_p(c_4)<4$, si E n'est pas minimal en p , alors il existe une transformation admissible T*, telle que T*(E)=E' avec

$v_p(\Delta') < v_p(\Delta)$

qui implique

$v_p(c_4') < v_p(c_4)$, en effet

on a

$j' = j \Rightarrow c_4'^3/\Delta' = c_4^3/\Delta \Rightarrow \Delta c_4'^3 = \Delta' c_4^3$

$v_p(\Delta)+3v_p(c_4') = v_p(\Delta')+3v_p(c_4)$

$v_p(\Delta) - v_p(\Delta') = 3v_p(c_4) - 3v_p(c_4')$

$0 < 3v_p(c_4) - 3v_p(c_4')$

$v_p(c_4') < v_p(c_4)$

et la démonstration reprend exactement comme pour

$v_p(c_4) < 4$ comme $v_p(\Delta) < 12$

$v_p(c_4') < v_p(c_4)$ comme $v_p(\Delta') < v_p(\Delta)$

III) Pour le cas $v_p(c_6)<6$, si E n'est pas minimal en p , alors il existe une E' telle que

$v_p(\Delta') < v_p(\Delta)$

qui implique

$v_p(c_6') < v_p(c_6)$, en effet

Si $c_4=0 \Rightarrow j=0 \Rightarrow E: y^2 = x^3 + 1$ (minimale: $\forall p, v_p(\Delta)<12$)

$\Delta = -2^4 .3^3$, $c_4 = 0$, $c_6 = -2^5 .3^3$

on suppose donc $c_4 \neq 0$, on a

$j' = j \Rightarrow 1728c_4'^3/(c_4'^3 - c_6'^2) = 1728c_4^3/(c_4^3 - c_6^2)$

$(c_4'^3 - c_6'^2)/c_4'^3 = (c_4^3 - c_6^2)/c_4^3$

$c_6'^2/c_4'^3 = c_6^2/c_4^3 \Rightarrow c_6'^2.c_4^3 = c_6^2.c_4'^3$

$2v_p(c_6') + 3v_p(c_4) = 2v_p(c_6) + 3v_p(c_4')$

$3v_p(c_4) - 3v_p(c_4') = 2v_p(c_6) - 2v_p(c_6')$

d'autre part

$\Delta c_4'^3 = \Delta' c_4^3$

$v_p(\Delta) + 3v_p(c_4') = v_p(\Delta') + 3v_p(c_4)$

$v_p(\Delta) - v_p(\Delta') = 3v_p(c_4) - 3v_p(c_4')$

$0 < v_p(\Delta) - v_p(\Delta') = 3v_p(c_4) - 3v_p(c_4')$

d'où

$0 < 2v_p(c_6) - 2v_p(c_6')$

$v_p(c_6') < v_p(c_6)$

on continue la démonstration exactement comme pour

$v_p(c_6) < 6$ comme $v_p(\Delta) < 12$

$v_p(c_6') < v_p(c_6)$ comme $v_p(\Delta') < v_p(\Delta)$

Proposition 2 : Soit p premier $p \geq 5$. si ($v_p(c_4) \geq 4$ et $v_p(c_6) \geq 6$) alors E n'est pas minimale en p.

Démonstration :

Soit donc un premier $p \geq 5$, et $v_p(c_4) \geq 4$ et $v_p(c_6) \geq 6$. On va utiliser le modèle simplifié.

$E : y^2 = x^3 + a_4x + a_6 \ , a_i \in \mathbb{Z}$

où les c_i sont:

$c_4 = -2^4.3\ a_4$

$c_6 = -2^5.3^3\ a_6$

passons par la transformation T(E)=E'

$$T = \begin{cases} x \to p^2x \\ y \to p^3y \end{cases}$$

$E' : y^2 = x^3 + a'_4x + a'_6$ et on a les relations:

$a'_4 = a_4/p^4$

$a'_6 = a_6/p^6$

$p^{12}\Delta' = \Delta$

Voyons:

$v_p(c_4) = v_p(-2^4.3) + v_p(a_4)$ comme $p \geq 5$, $v_p(-2^4.3)=0$

$v_p(c_4) = v_p(a_4) \geq 4$ ce qui montre $a'_4 = a_4/p^4$ est un entier (on peut simplifier par p^4)

de même

$v_p(c_6) = v_p(-2^5.3^3) + v_p(a_6)$ comme $p \geq 5$, $v_p(-2^5.3^3)=0$

$v_p(c_6) = v_p(a_6) \geq 6$ ce qui montre $a'_6 = a_6/p^6$ est un entier (on peut simplifier par p^6)

$v_p(p^{12}\Delta') = 12v_p(p) + v_p(\Delta') = v_p(\Delta)$

$12 + v_p(\Delta') = v_p(\Delta)$

$v_p(\Delta') < v_p(\Delta)$

les a'_4 , a'_6 sont des entiers et $v_p(\Delta') < v_p(\Delta)$ cela prouve que E n'est pas minimale en p.

Note : 1. On démontre que la proposition 2 reste encore vraie pour p=2, 3 .

2. Il suffit d'avoir deux inégalités et on aura forcement la troisième, par ex si on a ($v_p(\Delta) \geq 12$ et $v_p(c_4) \geq 4$) alors on aura forcement $v_p(c_6) \geq 6$, en effet grâce à la relation

$1728\Delta = c_4^3 - c_6^2$ et $p \geq 5$ on a:

$v_p(c_6^2) = v_p(c_4^3 - 2^6.3^3\,\Delta)$

$2v_p(c_6) \geq \inf(3v_p(c_4), v_p(2^6.3^3\,\Delta))$

soit

$2v_p(c_6) \geq 3v_p(c_4) \geq 3.4 \Rightarrow 2v_p(c_6) \geq 12 \Rightarrow v_p(c_6) \geq 6$

soit

$2v_p(c_6) \geq v_p(2^6.3^3\,\Delta) = v_p(\Delta)$ car $v_p(2^6.3^3) = 0$, $(p \geq 5)$

$2v_p(c_6) \geq v_p(\Delta) \geq 12 \Rightarrow v_p(c_6) \geq 6$

autrement dit :

$(v_p(\Delta) \geq 12$ et $v_p(c_4) \geq 4) \Rightarrow v_p(c_6) \geq 6.$

Le même raisonnement s'applique pour

$(v_p(\Delta) \geq 12$ et $v_p(c_6) \geq 6) \Rightarrow v_p(c_4) \geq 4$

$(v_p(c_4) \geq 4$ et $v_p(c_6) \geq 6) \Rightarrow v_p(\Delta) \geq 12$

Exemples de courbes elliptiques:

1) $y^2+xy+y = x^3 + x^2 + 22x - 9$ (minimal: $\forall p, v_p(c_4) < 4$)

$\Delta = -2^{15}.5^2$, $c_4 = -5.211$, $c_6 = 5.13.239$

2) $y^2 + y = x^3 - x + 1$ (minimal: $\forall p, v_p(\Delta) < 12$)

$\Delta = -13.47$, $c_4 = 2^4.3$, $c_6 = -2^3.3^3.5$

3) $y^2 = x^3 + 3$ (minimal: $\forall p, v_p(\Delta) < 12$)

$\Delta = -2^4.3^5$, $c_4 = 0$, $c_6 = -2^5.3^4$

4) $y^2 = x^3 + 16$

$\Delta = -2^{12}.3^3$, $c_4 = 0$, $c_6 = -2^9.3^3$

on a ($v_2(\Delta)=12\geq 12$ et $v_2(c_4)=+\infty\geq 4$ et $v_2(c_6)=9\geq 6$) donc E n'est pas minimale en 2, Une autre façon de voir que E n'est pas minimale en 2, c'est faire un changement de variables admissibles et voir si l'équation obtenue E' est entiers et $v_2(\Delta') < v_2(\Delta)$

on change les variables ainsi (c'est du feeling !!) :

$x \rightarrow 2^2x$

$y \rightarrow 2^3y+2^2$

$(2^3y+2^2)^2 = (2^2x)^3 + 16$

$2^6y^2 + 2^6y + 16 = 2^6x^3 + 16$

E': $y^2 + y = x^3$ coefficients entiers

et $2^{12}\Delta' = \Delta = -2^{12}.3^3 \Rightarrow \Delta' = -3^3$

$v_2(\Delta')=0 < v_2(\Delta)=12$

Donc E n'est pas minimale en p=2.

5) $y^2 + xy = x^3 + x^2 - 19x + 685$ (minimal: $\forall p, v_p(c_4)<4$)

$\Delta = -2^{16}.3^5.13$, $c_4 = 937$, $c_6 = 5.23.41.127$

6) $y^2 = x^3 + 6x - 7$ (minimal: $\forall p, v_p(\Delta)<12$)

$\Delta = -2^4.3^7$, $c_4 = -2^5.3^2$, $c_6 = 2^5.3^3.7$

7) $y^2 = x^3 + x^2 + 8x + 16$ (non minimal)

$\Delta = -2^{13}.13$, $c_4 = -2^4.23$, $c_6 = -2^6.181$

10.5 POINTS SINGULIERS

Revenons à notre courbe $\mathcal{E}$, avec le modèle 2:

E : $y^2 = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbb{Z}$
on pose :
$g(x) = x^3 + a_2x^2 + a_4x + a_6$
$f(x, y) = y^2 - g(x)$

E: $y^2 = g(x)$
E: $f(x, y) = 0$

un point (a, b) singulier est solution du système:

$$\begin{cases} f(a,b) = 0 \\ \dfrac{\partial f}{\partial x}(a,b) = 0 \\ \dfrac{\partial f}{\partial y}(a,b) = 0 \end{cases}$$

c'est-à-dire:
$b^2 = g(a)$
$g'(a) = 0$
$2b = 0$
autrement dit tout se passe par les racines de $g(x) = 0$, Soit A(a,0) le point singulier, on a 3 cas possibles :
1. a=racine triple ⇒ une tangente, pente=0
2. a=racine double ⇒ 2 tangentes distinctes, pentes dans $\mathbb{Q}$

3. a=racine double ⇒ 2 tangentes distinctes, pentes dans $\overline{\mathbb{Q}}$

10.6 PROPRIÉTÉS DE F(X,Y)=0

$f(x,y) = 0$

S'il n'y a pas de terme constant et du 1er degré, alors (0,0) est un point singulier de E. Soit $f_k(x,y)$ l'ensemble des termes de plus bas degré k, alors
k = l'ordre de (0,0)
$f_k(x,y) = 0$ donne les tangentes passant par (0,0)

Exemple:
$x^3 - y^2 - xy = 0$
(0,0) est un point singulier (il n'y a pas de terme constant et du 1er degré)
$f_2(x,y) = y^2 + xy \Rightarrow$ (0,0) est d'ordre 2

$y^2 + xy = 0$ donne les équations des tangentes en (0,0)
$y(x + y) = 0$
deux tangentes distinctes , pentes dans $\mathbb{Q}$
$y = 0$
$y = - x$

Exemple:
$x^3 - y^2 - xy + x^2 = 0$
(0,0) est un point singulier (il n'y a pas de terme constant et du 1er degré)

$y^2 + xy - x^2 = x^3$
$f_2(x,y) = y^2 + xy - x^2 \Rightarrow$ (0,0) est d'ordre 2

$y^2 + xy - x^2 = 0$ donne les équations des tangentes en (0,0)

$(y + \frac{x}{2})^2 - \frac{x^2}{4} - x^2 = 0$

$(y + \frac{x}{2})^2 - \frac{5}{4}x^2 = 0$

$(y + \frac{1-\sqrt{5}}{2}x)\ (y + \frac{1+\sqrt{5}}{2}x) = 0$

deux tangentes distinctes, pentes dans $\overline{\mathbb{Q}}$

$y = \frac{\sqrt{5}-1}{2}x$

$y = -\frac{\sqrt{5}+1}{2}x$

10.7 RÉDUCTION MODULO P

Au lieu de chercher les solutions de E dans $\mathbb{Q}$, on va les chercher dans $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$, donc soit p un nombre premier donné, la réduction de E modulo p, c'est la courbe E_p dont on fait modulo p les coefficients a_i .

E : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ avec $a_i \in \mathbb{Z}$

E_p : $y^2 + m_1xy + m_3y = x^3 + m_2x^2 + m_4x + m_6$ avec $m_i \in \mathbb{F}_p$

avec $a_i = m_i \pmod p$; $m_i \in \mathbb{F}_p$

on pose

$E = E_p \pmod p$; modulo p = on travaille dans $\mathbb{F}_p$

$\Delta = \Delta_p \pmod p$

$c_4 = c_{4,p} \pmod p$

Ex:
E: $y^2 = x^3 - 13x^2 + 7$
E_5: $y^2 = x^3 - 3x^2 + 2 \pmod 5$
E_3: $y^2 = x^3 - x^2 + 1 \pmod 3$

Le problème est que lorsqu'on fait la réduction modulo p, il peut arriver que E_p sèche d'être elliptique !! c'est-à-dire la courbe modulo E_p peut avoir de points singuliers dans $\mathbb{F}_p$.

10.8 BONNE, MAUVAISE RÉDUCTION EN P

Définition : Bonne, mauvaise réduction en p

si $p \nmid \Delta \Leftrightarrow \Delta_p \neq 0 \Leftrightarrow E_p$ elliptique $\Leftrightarrow$ p=bonne réduction.

si $p|\Delta \Leftrightarrow \Delta_p = 0 \Leftrightarrow E_p$ non-elliptique $\Leftrightarrow$ p=mauvaise réduction.

Lorsqu'on a une mauvaise réduction, on a deux types de mauvaise réduction:

si c'est un point double (deux tangentes distinctes) on dit que c'est une mauvaise réduction multiplicative ($p \nmid c_4$) .

si c'est un point rebroussement (une tangente) on dit que c'est une mauvaise réduction additive ($p|c_4$) .

Voyons sur un ex:
E: $y^2 = x^3 + 5$
$E_5 : y^2 = x^3 \pmod 5$

Cette courbe E_5 a un point singulier en (0,0) dans $\mathbb{F}_5$ (avec une tangente), c'est donc une mauvaise réduction additive en p=5 en fait $\Delta = -2^4.3^3.5^2$, $c_4 = 0$, $c_6 = -2^5.3^3.5$ on a 2,3, 5 divise Δ et divise c_4 donc des mauvaises réductions additive en 2,3,5

pour p = 2,

$E_2 : y^2 = x^3 + 1 \pmod 2$

$y^2 - 1 = x^3 \pmod 2$

$y^2 + 1 = x^3 \pmod 2$

$(y + 1)^2 = x^3 \pmod 2$, car dans $\mathbb{F}_2$ on a: $(x+y)^2 = x^2 + y^2$

on pose

$y+1 = u$

$u^2 = x^3 \pmod 2$

une tangente → additive

pour p=3,

$E_3 : y^2 = x^3 + 2 \pmod 3$

$y^2 = x^3 + 2^3 \pmod 3$

$y^2 = (x + 2)^3 \pmod 3$, car dans $\mathbb{F}_3$ on a: $(x+y)^3 = x^3 + y^3$

on pose

$x+2 = v$

$y^2 = v^3 \pmod 3$

une tangente → additive

Un autre exemple:
E: $y^2 = x^3 - 625x$, $\Delta = 2^6.5^{12}$, $c_4 = 2^4.3.5^4$, $c_6 = 0$

$E_5 : y^2 = x^3 \pmod 5$

On croit que c'est une mauvaise réduction en p=5 mais en réalité 5 n'est pas une mauvaise réduction !! en effet si on fait un changement de variables admissibles par T
$x \to 5^2x$
$y \to 5^3y$
on trouve
$y^2 = x^3 - x$

$\Delta = 2^6$, $c_4 = 2^4.3$

et qui a une bonne réduction en p=5 !!!!
Pourquoi cette anomalie ?? c'est parce qu'on n' a pas pris l'équation minimale de E avant de faire la réduction !
l'équation $y^2 = x^3 - 625x$ n'est pas minimale en 5

car $(v_5(\Delta)=12 \geq 12$ et $v_5(c_4)=4 \geq 4$ et $v_5(c_6)=+\infty \geq 6)$

elle ne donne pas toutes les <u>vraies</u> mauvaises réductions .

E: $y^2 = x^3 + 16$

$\Delta = -2^{12}.3^3$, $c_4 = 0$, $c_6 = -2^9.3^3$

on a $(v_2(\Delta)=12\geq 12$ et $v_2(c_4)=+\infty\geq 4$ et $v_2(c_6)=9\geq 6)$ donc E n'est pas minimale en 2, la réduction en 2 ne donne pas de vraie mauvaise réduction

On fait un changement de variables

$$\begin{cases} x' = 4x \\ y' = 8y + 4 \end{cases}$$

L'équation devient

$y^2+y = x^3$

$\Delta = -3^3,\ c_4 = 0,\ c_6 = -2^3 3^3$

p=2 est une bonne réduction.

Pour dire que c'est une mauvaise réduction (resp. en p) il faut être sûr que l'équation est minimale (resp. en p).

Théorème :

On démontre que seules les équations minimales de E donnent les vraies mauvaises réductions.

Démonstration : On passe d'une équation minimale E à une autre minimale E' par la transformation T avec u=1,-1 et r,s,t $\in\mathbb{Z}$ donc

$|\Delta'| = |u^{-12}|\,|\Delta_{min}| \Rightarrow |\Delta'| = |\Delta_{min}|$ donc les diviseurs premiers p de Δ_{min} donnent de vraie mauvaise réduction (il n'y a pas de faux diviseur)
Donc seul le discriminant minimal, donne les vraies mauvaises réductions, c'est-à-dire seuls les diviseurs premiers p de Δ_{min} sont des vraies mauvaises réductions

Remarque: On peut montrer (en exercice) que si on prend l'équation $y^2 = g(x)$ pour représenter E , alors $y^2 = g(x)$ donne toujours une mauvaise réduction en p=2 !!!

10.9 SEMI-STABLE

Définition semi-stable : On dit qu'une courbe elliptique E est semi-stable en p (premier) si p est une bonne réduction ou bien une mauvaise réduction multiplicative (deux tangentes distingues).

Une courbe semi-stable, elle est semi-stable pour tout p. Donc semi-stable signifie elle a des bonnes réductions ou des mauvaises réductions multiplicatives .

10.10 LA FONCTION L(S) ET CONDUCTEUR N

E est donné par

$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 , a_i \in \mathbb{Z}$

modèle minimal ($\Delta = \Delta_{min}$, $|\Delta_{min}|$=minimal)

On définit le conducteur N de E, c'est le produit de tous les mauvaises réductions (ce sont des vraies mauvaises réductions car ici on a un model minimal)

$$N = \prod_{p=\text{mauvaise}} p^k$$

$$k = \begin{cases} = 1 \text{ mauvaise réduction muplicative (2 tangentes)} \\ = 2 \text{ mauvaise réduction additive (1 tangente)} \end{cases}$$

En terme de "divise" .

E semi-stable en p $\overset{\text{déf}}{\Leftrightarrow}$ $p^2 \nmid N$

ça signifie:

$$\begin{cases} \text{Soit } p \nmid N \Leftrightarrow (p, N) = 1 \Leftrightarrow p \text{ bonne réduction} \\ \text{Soit } p|N \text{ exactement } (p = \text{sans puissance}) \end{cases}$$

semi-stable ⇔ semi-stable pour tout p ⇔ N sans facteurs carrés.

Une courbe semi-stable son conducteur N n'a pas de facteurs carrés, semi-stable en p signifie :

$p|N$ et $p^2 \nmid N$ (dans la décomposition de N, il n'y a pas de puissance pour p)

Remarque : Δ dépend de l'équation utilisée tandis que Δ_{min} est propre à la courbe elliptique $\mathcal{E}$ comme le conducteur N. N est le produit des nombres premiers dans Δ.

Exemples de courbes semi-stable:

1) $y^2 + y = x^3 + x^2 - 102x - 111$
$\Delta = 60045533$, $N = 60045533$

2) $y^2 + xy = x^3 + 1078x + 134436$
$\Delta = 2^{12}.3^{10}.32569$, $N = 2.3.32569$

3) $y^2 + xy = x^3 - 844x - 9485$
$\Delta = 189670477$, $N = 189670477$

Voici un site qui vous fournit des courbes elliptiques quand on lui donne le conducteur N ou le discriminant Δ
https://www.lmfdb.org/EllipticCurve/Q/

Soient:

$E = E_p \pmod p$, E_p = la courbe E modulo p (les coefficients a_i modulo p)

$\#E_p$ = le nombre de solutions (y compris le point infini Θ) de E_p dans $\mathbb{F}_p$

On pose:

¤ si p∤N (p=bonne réduction)

$a_p = p + 1 - \#E_p$

¤ si p|N (p=mauvaise réduction)

$$a_p = \begin{cases} 0 \text{ réduction additive} \\ 1 \text{ réduction multiplicative (2 pentes dans } \mathbb{Q}) \\ -1 \text{ réduction multiplicative (2 pentes non dans } \mathbb{Q}) \end{cases}$$

On définit la fonction de Hasse-Weil L(s) par :

$$L(s) = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p|N} \frac{1}{1 - a_p p^{-s}} \quad , s \in \mathbb{C}$$

Note : On a $|a_p| \leq 2\sqrt{p}$ (th Hasse-Weil) ⇒ L(s) converge pour Re(s) > 3/2, en fait on démontre que L(s) se prolonge en une fonction holomorphe dans tout ℂ.

En développant L(s) , on a une série L nommée la série de Dirichlet (la série "en s", s=paramètre) :

$$L = \sum_{n \geq 1} \frac{a_n}{n^s}$$

Remarque : Dans la fonction L(s) les indices de a_p sont définis pour les nombres premiers p, tandis que dans la série L les indices de a_n sont définis pout tout entier $n \geq 1$.

10.11 LA COURBE $\mathcal{E}$ MODULAIRE

Définition $\mathcal{E}$ modulaire :

Soit $\mathcal{E}$ une courbe elliptique de conducteur N, et soit

$$L = \sum_{n \geq 1} \frac{a_n}{n^s}$$

la série L de $\mathcal{E}$.

$\mathcal{E}$ est donné par l'équation E, on dit que $\mathcal{E}$ ou E est modulaire (de niveau N, de poids 2), s'il existe une forme non-nulle $F \in S_2(N)$

$$F = \sum_{n \geq 1}^{\infty} b_n q^n \ ; \ b_1 = 1$$

telle que

$a_n = b_n$ pour tout n

On écrit symboliquement

L = F , les coefficients de la série L et de la série F sont égaux.

E modulaire signifie qu'on peut "retrouver" les $\#E_p$ de E à partir des coefficients de F : $b_p = p+1-\#E_p$ pour $p \nmid N$ (p=bonne réduction, qui sont en nombre infini) .

11 THÉORÈME DE WILES

Théorème de Wiles (1994): Toute courbe elliptique E sur $\mathbb{Q}$, semi-stable est modulaire.

Il n'est pas question de donner la démonstration ici, Wiles a mis 8 ans pour la trouver et la démonstration fait 127 pages !!

Exemples :

¤ Soit E la courbe elliptique

1) E: $y^2 + y = x^3 - x^2$

$\Delta = -11$, $c_4 = 2^4$, $c_6 = -2^3.19$

On peut voir que E est semi-stable et de conducteur N=11 (N=rad(Δ)=les nombres premiers dans la décomposition de Δ)

En effet:

$v_p(c_6) < 6\ \forall p \Longrightarrow$ E est minimale $\Longrightarrow \Delta=\Delta_{min}$

$\forall p, (\Delta, c_4) = 1 \Longrightarrow$ réduction multiplicative

Donc E est semi-stable, N=rad(Δ)=11

et on trouve que sa forme modulaire F associée est:

$$F = q\prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2$$

$= q - 2q^2 - q^3+2q^4 + q^5 +2q^6 - 2q^7- 2q^9 - 2q^{10} +q^{11} - 2q^{12} + ...$

$$= \sum_{n\geq 1}^{\infty} b_n\, q^n$$

$F \in S_2(11)$

pour p=3

$E_3(\mathbb{F}_3) = \{\Theta, (0,0), (0,1), (1,0), (1,1)\}$ les solutions dans $\mathbb{F}_3$

$\#E_3 = 5$

$b_3 = -1 = 3+1-5$

on a bien $b_p = p+1-\#E_p$ pour tout $p \nmid 11$

¤ Soit E la courbe elliptique

2) E: $y^2 + y = x^3 - x$

$\Delta = 37$, $c_4 = 2^4.3$, $c_6 = -2^3.3^3$

On voit que E est semi-stable et de conducteur N=37 (N=rad(Δ)=les nombres premiers dans la décomposition de Δ)

En effet:

$v_p(c_6) < 6\ \forall p \Longrightarrow$ E est minimale $\Longrightarrow \Delta=\Delta_{min}$

$\forall p, (\Delta, c_4) = 1 \Longrightarrow$ réduction multiplicative

Donc E est semi-stable, N=rad(Δ)=37

et on trouve que sa forme modulaire F associée est:

$F = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} - 5q^{11} + ...$

$$= \sum_{n \geq 1}^{\infty} b_n q^n$$

$F \in S_2(37)$

pour p=3

$E_3(\mathbb{F}_3) = \{\Theta, (0,0), (0,2), (1,0), (1,2), (2,0), (2,2)\}$ les solutions dans $\mathbb{F}_3$

$\#E_3 = 7$

$b_3 = -3 = 3+1-7$

on a bien $b_p = p+1-\#E_p$ pour tout p∤37

Exemples de courbes modulaires:

1) $y^2 + xy + y = x^3 + 4x + 20$

$\Delta = -2.3^6.11^2$, $c_4 = -5.43$, $c_6 = -13.1321$, $N = rad(\Delta) = 2.3.11$

$F = q - q^2 + q^3 + q^4 - q^6 + 2q^7 - q^8 + q^9 - q^{11} + q^{12} - 4q^{13} + ...$

2) $y^2 + xy = x^3 + x^2 - 1299x + 17325$

$\Delta = 2^8.3^{10}.13^2$, $c_4 = 7^2.19.67$, $c_6 = -5.23.269.499$, $N=rad(\Delta)=2.3.13$

$F = q - q^2 - q^3 + q^4 + 2q^5 + q^6 + 4q^7 - q^8 + q^9 - 2q^{10} - 4q^{11} - q^{12} + q^{13} + ...$

Déjà en 1955 Taniyama a remarqué que pour certaines courbes elliptiques E on trouve leur forme modulaire associée F. Puis confirmé par Shimura, mais il y avait très peu de courbes elliptiques connues , ils émettaient alors une conjecture assez vague puis reformulée et mis en forme par Weil, on nomme maintenant la conjecture de Taniyama-Shimura-Weil (TSW)

Conjecture TSW : Toute courbe elliptique sur $\mathbb{Q}$ est modulaire.

ça signifie:

Soit E une courbe elliptique sur $\mathbb{Q}$ de conducteur N,

de série L

$$L = \sum_{n\geq 1} \frac{a_n}{n^s}$$

alors il existe une forme modulaire $F \in S_2(N)$

$$F = \sum_{n\geq 1}^{\infty} b_n q^n \ ; b_1 = 1$$

telle que

$a_n = b_n \ \forall n$

en particulier

$b_p = p+1-\#E_p$ pour tout $p \nmid N$

ce qui est important c'est qu'on récupère $\#E_p$, les bonnes réductions ($p \nmid N$) qui sont en nombre infini. Ce n'est pas

importante pour les mauvaises réductions car il n'y a qu'un nombre fini.

En 1994 Wiles a démontré la conjecture TSW pour une famille de courbes elliptiques: les courbes semi-stable.

En 1996 F. Diamond a montré que les courbes elliptiques sur $\mathbb{Q}$ semi-stable en 3 et en 5 sont modulaires.

Puis en 1999 un groupe de 4 mathématiciens : Brian Conrad, Fred Diamond, Richard Taylor et Christophe Breuil a complètement démontré la conjecture TSW c'est-à-dire pour tous les courbes elliptiques sur $\mathbb{Q}$, ils démontrent d'abord pour N ne comporte pas 3^2 et 5^2, puis N ne comporte pas 3^3 et finalement pour N quelconque.

La conjecture TSW devient maintenant un théorème nommé le théorème de modularité (1999).

12 REPRÉSENTATION GALOISIENNE

12.1 LOI DE GROUPE SUR $E(\overline{\mathbb{Q}})$

On pose:

$\xi(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$, $a_i \in \mathbb{Z}$

E: $\xi(x, y) = 0$

Rappel :

* $E(\mathbb{Q}) = \{P=(x,y)\in\mathbb{Q}^2 / \xi(x,y) = 0\} \cup \{\Theta\}$

les points rationnels de E (à coordonnées rationnels), par convention le point Θ est un point rationnel

* $E(\mathbb{C}) = \{P=(x,y)\in\mathbb{C}^2 / \xi(x,y) = 0\} \cup \{\Theta\}$

les points complexe de E (à coordonnées complexes)

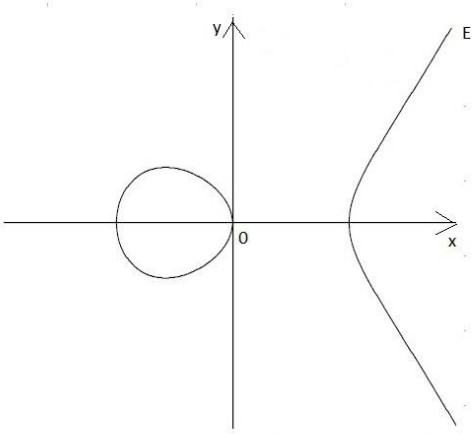
* $E(\overline{\mathbb{Q}}) = \{P=(x,y)\in\overline{\mathbb{Q}}^2 / \xi(x,y) = 0\} \cup \{\Theta\}$

les points de E (à coordonnées algébriques).

On peut définir une loi de groupe sur E : $(E(\overline{\mathbb{Q}}),+)$

Définition la loi + géométriquement:

On se donne un point de E, pour nous on va prendre Θ, qui va jouer le rôle d'élément neutre de $(E(\overline{\mathbb{Q}}),+)$.



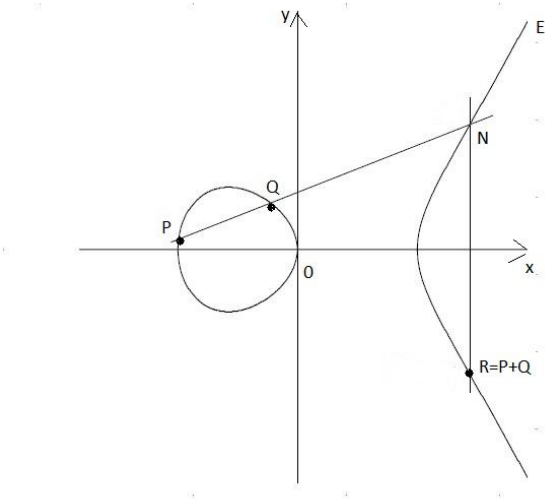
Une courbe elliptique

Règle:

La somme de deux points P+Q

cas P≠Q

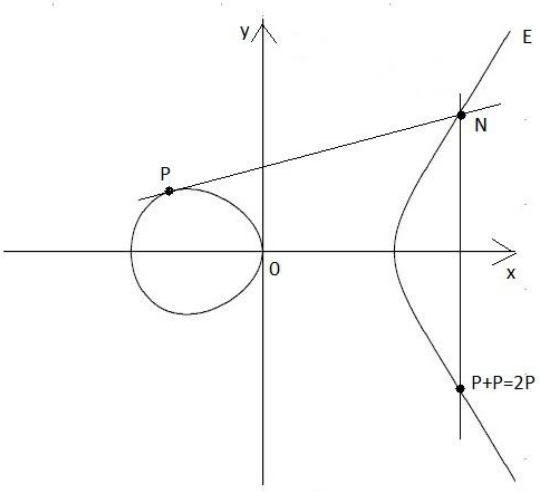
1. Former la droite (PQ), qui coupe E en N: (PQ)∩E=N
2. Former la droite (NΘ) c'est la perpendiculaire à Ox passant par N, (NΘ) coupe E en R, (NΘ)∩E=R , par définition R = P+Q



P+Q=R

cas P=Q

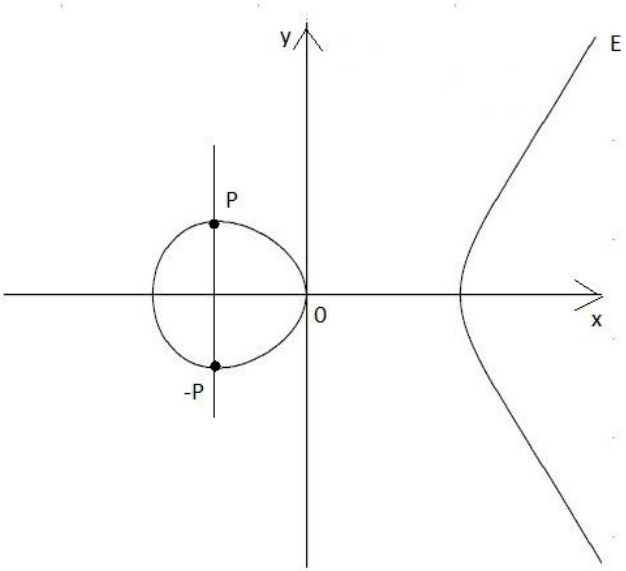
1. Former la tangente en P, qui coupe E en N: tg(P)∩E=N
2. Former la droite (NΘ) c'est la perpendiculaire à Ox passant par N, (NΘ) coupe E en R, (NΘ)∩E=R , par définition R = P+P = 2P



P+P=2P

Calculer -P

-P ⇒ c'est le symétrique de P , par rapport à l'axe Ox



-P

Note : Les droites verticales représentent Θ, ce sont les seules qui rencontrent Θ.

Définition la loi + algébriquement

E est donné par l'équation:

E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, avec $a_i \in \mathbb{Z}$

et la somme de deux points P_1+P_2 est définie par :

$P_1 + P_2 = P_3$

avec $P_i=(x_i ,y_i)$ où i=1,2,3

¤ cas $x_1 \neq x_2$

$a = (y_2 - y_1)/(x_2 - x_1)$

$b = (y_1x_2 - y_2x_1)/(x_2 - x_1)$

¤ cas $x_1 = x_2$

(12.1.1) $a = (3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)/(2y_1 +a_1 x_1 +a_3)$

$b = (-x_1^3 + a_4x_1 + 2a_6 - a_3y_1)/(2y_1 +a_1 x_1 +a_3)$

$x_3 = a^2 + a_1a - a_2 - x_1 - x_2$

$y_3 = -(a + a_1)x_3 - b - a_3$

¤ $-P = (x, - y - a_1x - a_3)$ où $P=(x,y)$

On peut vérifier que $(E(\overline{\mathbb{Q}}),+)$ forme un groupe abélien dont l'élément neutre est Θ et le $(E(\mathbb{Q}),+)$ est un sous groupe de $(E(\overline{\mathbb{Q}}),+)$

12.2 POINTS DE TORSION

Vers l'année 1922 Mordell démontrait le théorème suivant:

Théorème Mordell-Weil (1922-1937) :

Le groupe $(E(\mathbb{Q}),+)$ des points rationnels est abélien et de type fini, plus précisément il est de la forme:

$E(\mathbb{Q}) = T(\mathbb{Q}) \times \mathbb{Z}^r$ où r=entier naturel, le rang de E.

Autrement dit, soient $\omega_1, \omega_2, \ldots, \omega_r$ les points rationnels bases, on a

$\forall P \in E(\mathbb{Q})$

$$P = U + \sum_{k=1}^{r} a_k \omega_k$$

où $U \in T(\mathbb{Q})$

$T(\mathbb{Q})$ est un groupe abélien fini, nommé le groupe de torsion de E

Les éléments de $T(\mathbb{Q})$ sont d'ordres finis, les éléments de $\mathbb{Z}^r$ sont d'ordres infinis.

On note

$$E[n] = E[n](\mathbb{Q}) = \{P \in E(\mathbb{Q}) \,/\, \underbrace{P + P + \cdots + P}_{\text{n fois}} = nP = \Theta\}$$

les points n-torsion , c'est aussi l'ensemble des points d'ordre d|n.

Un point de torsion est donc

$$T(\mathbb{Q}) = \{P \in E(\mathbb{Q}), \exists n \in \mathbb{N}^* \,/\, \underbrace{P + P + \cdots + P}_{\text{n fois}} = nP = \Theta\}$$

$$T(\mathbb{Q}) = \bigcup_{n \geq 1} E[n]$$

En 1937 Weil généralisait ce théorème pour les corps de nombres $\mathbb{K}=\mathbb{Q}(\theta)$ où θ=un nombre algébrique.

(12.2.1) Théorème de Mazur (1977) :

Le groupe de torsion $T(\mathbb{Q})$ est l'un des groupes suivants :

$$T(\mathbb{Q}) = \begin{cases} \mathbb{Z}/n\mathbb{Z} \ \ ,1 \leq n \leq 10 \text{ ou } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \ x \ \mathbb{Z}/2n\mathbb{Z} \ \ ,1 \leq n \leq 4 \end{cases}$$

On voit donc l'ordre de $T(\mathbb{Q})$ est

$\# T(\mathbb{Q}) \leq 16$

<u>Les point de 2-torsion</u>

Supposons que $P \neq \Theta$

$P+P = 2P = \Theta = (\infty,\infty)$

ceci implique que

$2y + a_1 x + a_3 = 0$ d'après (12.1.1)

Si l'équation de E est donnée par

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

et f(x) n'a pas de racines multiples (E elliptique).

$f(x) = (x - e_1)(x - e_2)(x - e_3)$

Les points d'ordre 2 sont les trois racines de f(x) dans $\overline{\mathbb{Q}}$, avec Θ ils forment un groupe abélien.

$\{\Theta, (e_1,0), (e_2,0), (e_3,0)\}$

Les points 2-torsion (les points rationnels d'ordre 2) sont des racines dans $\mathbb{Q}$ de f(x), si f(x) a 3 racines dans $\mathbb{Q}$ on aura donc 4 points d'ordre 2 avec Θ:

$\{\Theta, (e_1,0), (e_2,0), (e_3,0)\}$

Θ est un point rationnel (par définition) et d'ordre 2.

Note : on dit parfois les points de n-division pour les points de n-torsion.

12.3 REPRÉSENTATION ATTACHÉE À $E[\mu]$

On se donne un nombre premier $\mu \geq 5$ fixé .

$\sigma: \overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}}$, σ=automorphismes de $\overline{\mathbb{Q}}$ laissant fixe $\mathbb{Q}$.

$Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ = c'est l'ensemble des automorphismes de $\overline{\mathbb{Q}}$ qui laissent fixe $\mathbb{Q}$.

$\overline{\mathbb{Q}}$ = les nombres algébriques = la clôture algébrique de $\mathbb{Q}$ (dans $\mathbb{C}$) = où se trouvent toutes les racines de $P \in \mathbb{Q}[X]$.

$$E[\mu] = E[\mu](\overline{\mathbb{Q}}) = \{P \in E(\overline{\mathbb{Q}}) \,/\, \underbrace{P + P + \cdots + P}_{\mu \text{ fois}} = \mu P = \Theta\}$$

$E[\mu] \subset E(\overline{\mathbb{Q}})$

$E[\mu] = \mathbb{F}_\mu$-esv

Alors on peut associer une représentation ρ_μ de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ dans $Aut(E[\mu])$ ainsi :

$\rho_\mu : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow Aut(E[\mu])$

On va donc étudier les propriétés de ρ_μ , mais avant on va se rappeler brièvement comment on a obtenu ρ_μ

Soient donc

$\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, et $P=(x,y) \in E \Rightarrow \sigma \bullet P=P'=(\sigma(x),\sigma(y)) \in E$ en effet comme $\sigma(a_i)=a_i$

l'équation:

$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, avec $a_i \in \mathbb{Q}$

devient:

$E': \ y'^2 + a_1x'y' + a_3y' = x'^3 + a_2x'^2 + a_4x' + a_6$, avec $a_i \in \mathbb{Q}$

ce qui montre bien que $P'=(x',y') \in E$ donc on a:

$\sigma \bullet P=P'$ ça signifie que $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ agit sur E. Le passage de P à P' assure par des fonctions f de E, plus précisément par des automorphismes f de E

$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \times E \rightarrow E$

$(\sigma,P) \rightarrow \sigma \bullet P=P'$

d'où

$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow Aut(E)$

$\sigma \to f_\sigma$

En passant par la restriction

$\rho_\mu : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(E[\mu])$

$$Aut(E[\mu]) = GL_2(\mathbb{F}_\mu) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{matrix} a, b, c, d \in \mathbb{F}_\mu \\ ad - cb \neq 0 \end{matrix} \right\}$$

$\sigma \to f_\sigma$ (=c'est simplement une matrice)

$\rho_\mu : \sigma \to \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{F}_\mu$ et $ad - cb \neq 0$

$\rho_\mu(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où $a, b, c, d \in \mathbb{F}_\mu$ et $ad - cb \neq 0$

$$\begin{array}{l} \rho_\mu : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(E[\mu]) \\ \qquad\qquad \sigma \longrightarrow \rho_\mu(\sigma) = f_\sigma \end{array}$$

$$\begin{array}{ll} & \sigma : \overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}} \\ \rho_\mu & \Big\downarrow \\ & f_\sigma : E[\mu] \longrightarrow E[\mu] \\ & \qquad P \longrightarrow f_\sigma(P) = P' = \sigma \bullet P \end{array}$$

On a donc une représentation de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ dans $Aut(E[\mu])$ càd on prolonge $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ dans $Aut(E[\mu])$, $Im(\rho_\mu) \subset Aut(E[\mu])$, mais pour simplifier le vocabulaire, on dira simplement que ρ_μ est la représentation attachée à $E[\mu]$ ou provenant de $E[\mu]$, ou fournie par $E[\mu]$.

Rappel:

$Frob_p : \overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}}$

$x \longrightarrow Frob_p(x) = x^p$, le Frobenius de $\overline{\mathbb{Q}}$ en p.

$f_p : E(\overline{\mathbb{Q}}) \longrightarrow E(\overline{\mathbb{Q}})$, $P=(x,y)$, $P'=(x',y')$

$P \longrightarrow f_p(P) = P'$

$(x,y) \longrightarrow f_p(x,y) = (x^p,y^p)$, le Frobenius de E en p.

$f_p : E[\mu] \longrightarrow E[\mu]$, $P=(x,y)$, $P'=(x',y')$

$(x,y) \longrightarrow f_p(x,y) = (x^p,y^p)$, la restriction de f_p sur $E[\mu]$.

Soit un $p \nmid \mu N$, alors on a:

$$\rho_\mu(Frob_p) = \begin{pmatrix} \alpha_p & \beta_p \\ \gamma_p & \delta_p \end{pmatrix} ; \begin{cases} \alpha_p, \beta_p, \gamma_p, \delta_p \in \mathbb{F}_\mu \\ \alpha_p\delta_p - \gamma_p\beta_p \neq 0 \end{cases}$$

$Trace = \alpha_p+\delta_p$

$Déterminant = \alpha_p\delta_p - \gamma_p\beta_p$

On pose $t_p = Trace(\rho_\mu(Frob_p))$ pour tout $p \nmid \mu N$

Remarque : Le couple (ρ_μ,t_p) ressemble beaucoup au couple (L,a_p)

$t_p = \text{Trace}(\rho_\mu(\text{Frob}_p))$ pour tout $p \nmid \mu N$

$a_p = p+1-\#E_p$ pour tout $p \nmid N$

(12.3.1) Théorème :

Pour tout $p \nmid \mu N$ on a:

$t_p = p + 1 - \#E_p \pmod{\mu}$

12.4 LA REPRÉSENTATION P_μ EST FINIE EN P

Définition : Si $v_p(\Delta_{min}) = 0 \pmod{\mu}$

On dit que ρ_μ est finie en p.

12.5 LA REPRÉSENTATION P_μ MODULAIRE

Définition: ρ_μ modulaire.

On dit que ρ_μ est modulaire de niveau N, s'il existe une forme non-nulle $F \in S_2(N)$

$$F = \sum_{n \geq 1}^{\infty} b_n q^n \ ; (\text{rappel: } b_1 = 1)$$

telle que :

pour tout p∤μN on ait : $t_p = b_p \pmod{\mu}$.
On écrira symboliquement

$\rho_\mu = F \pmod{\mu}$

exemples :

1) ρ_μ modulaire de niveau N:

μ=5, N=2.3.11

p	2	3	5	7	11	13	17
t_p	0	-1	2	14	-1	7	-4
b_p	0	1	-3	9	-1	-13	6

$t_7 = b_7 \pmod 5$, 7∤μN
$t_{13} = b_{13} \pmod 5$, 13∤μN
.....

2) ρ_μ modulaire de niveau N:

μ=5, N=2.3.13

p	2	3	5	7	11	13	17
t_p	-1	1	-3	-1	6	1	-3
b_p	-1	-1	2	4	-4	1	2

$t_7 = b_7 \pmod 5$, 7∤μN
$t_{11} = b_{11} \pmod 5$, 11∤μN
.....

Remarque importante: il y a une différence entre la définition de "E modulaire" et de "ρ_μ modulaire" . En effet

dans "E modulaire" les coefficients a_n de L et les coefficients b_n de F sont identiques pour tout n, alors que dans "ρ_μ modulaire" les coefficients t_p de ρ_μ et les coefficients b_p de F ne sont définis que pour p=premier et p∤μN, de plus ce sont des "restes" de t_p et b_p qui sont identiques ! , mais ce qui est important c'est que les p∤μN sont en nombre infini.

Il y a une analogie entre le couple (L, a_p) et le coupe (ρ_μ, t_p)

1) $E \to \#E_p \to L$, $a_p=p+1-\#E_p$ quand p∤N

2) $E \to E[\mu] \to \rho_\mu$, $t_p=\text{Trace}(\rho_\mu(\text{Frob}_p))$ quand p∤μN

ce qui lie entre L et ρ_μ quand p≠μ et p∤N est :

$a_p=p+1-\#E_p$ quand p∤μN

$a_p=p+1-\#E_p \pmod{\mu}$ quand p∤μN

$t_p=p+1-\#E_p \pmod{\mu}$ quand p∤μN

d'où

$a_p=t_p \pmod{\mu}$ quand p∤μN

(12.5.1)Théorème **:**

Si E est modulaire alors ρ_μ est modulaire.

Démonstration :

E modulaire ⇒ il existe une forme non-nulle $F \in S_2(N)$

$$F = \sum_{n\geq 1}^{\infty} b_n q^n$$

telle que:

$a_n = b_n$ pour tout n

donc en particulier n=p avec p∤μN

$\forall$ p∤μN , $a_p = b_p$

ou encore , en passant par le modulo

$\forall$ p∤μN , $a_p = b_p \pmod{\mu}$

Mais,

$\forall$ p∤μN, $t_p = p + 1 - \#E_p \pmod{\mu}$; théorème (12.3.1)

et

$\forall$ p∤μN, $a_p = p+1-\#E_p$

$\forall$ p∤μN, $a_p = p+1-\#E_p \pmod{\mu}$

d'où

$\forall$ p∤μN, $t_p = a_p \pmod{\mu}$

et

$\forall$ p∤μN, $t_p = b_p \pmod{\mu}$

C'est bien la définition de ρ_μ modulaire.

Note : Le théorème (12.3.1) est un résultat vraiment merveilleux car il lie t_p et a_p quand $p \nmid \mu N$.

$t_p = p + 1 - \#E_p \pmod{\mu}$, quand $p \nmid \mu N$

12.6 REPRÉSENTATION Pμ IRRÉDUCTIBLE

Soient E une courbe elliptique sur $\mathbb{Q}$ et μ premier ≥5 .

Soit ρ_μ la représentation définie par :

$\rho_\mu : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow Aut(E[\mu])$

Définition : On dit que ρ_μ est irréductible si on a:

$Im(\rho_\mu) = Aut(E[\mu])$

On démontre alors le théorème suivant :

(12.6.1)Théorème :

Soient E une courbe elliptique sur $\mathbb{Q}$, semi-stable et μ premier ≥5.

Alors on a l'une des 3 situations suivantes :

1) $Im(\rho_\mu) = Aut(E[\mu])$
2) E contient un point rationnel d'ordre μ.
3) E' contient un point rationnel d'ordre μ où E' une courbe isomorphe à E (une μ-isogénie de E).

12.7 THÉORÈME DE MAZUR

(12.7.1) Théorème de Mazur :

$\rho_\mu : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(E[\mu]) = GL_2(\mathbb{F}_\mu)$

Si $\mu \geq 11$ et E semi-stable $\Rightarrow \rho_\mu$ est irréductible.

(12.7.2) Théorème de Mazur :

Si $\mu \geq 5$, E semi-stable et E contient 3 points rationnels d'ordre 2 $\Rightarrow \rho_\mu$ est irréductible.

Remarque : Il y a plusieurs façons de dire la condition : "E contient 3 points rationnels d'ordre 2":

(i) $\longrightarrow$ Tous les points d'ordre 2 sont rationnels.

(ii) $\longrightarrow$ Si E est donnée par : $y^2 = f(x)$

alors f(x) a 3 racines rationnels.

(iii) $\longrightarrow$ ρ_2 est triviale = $Im(\rho_2) = \{id\}$.

Démonstration :

Supposons que ρ_μ est réductible, càd $Im(\rho_\mu) \neq Aut(E[\mu])$. Alors d'après le théorème (12.6.1) on a :

(i) Soit E contient un point rationnel d'ordre μ.

(ii) Soit E' contient un point rationnel d'ordre μ.

Cas (i) : E contient déjà 3 points rationnels d'ordre 2 : R_1, R_2, R_3 et avec le point Θ on a 4 points rationnels d'ordre 2,

Soit P le point rationnel d'ordre μ, le groupe engendré par P : <P> possède μ points rationnels d'ordre fini.

Avec les 4 points R_1, R_2, R_3 , Θ on forme avec les μ points de <P> ça donne 4μ points rationnels d'ordre fini et :

$4\mu \leq \#T(\mathbb{Q})$ (les points de torsion de E)

comme $5 \leq \mu$

$20 \leq 4\mu \leq \#T(\mathbb{Q}) \leq 16$

Ce qui contredit le théorème de Mazur (12.2.1)

Pour le cas (ii) c'est E' qui contredit le théorème de Mazur (12.2.1)

Donc ρ_μ est irréductible.

13 UN THÉORÈME

13.1 THÉORÈME DE RIBET

Soient E une courbe elliptique semi-stable et ρ_μ la représentation définie par :

$\rho_\mu : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow Aut(E[\mu])$, μ premier ≥ 5

On suppose que ρ_μ est : irréductible, modulaire de niveau N (rappel: N sans facteurs carrés $\Leftrightarrow$ E semi-stable).

Soit un $q|N$ et ρ_μ finie en q.

Serre s'est posé la question suivante : Peut-on baisser le niveau N au niveau N/q ? si oui dans quelles conditions ?

Peu de temps après, Mazur montre qu' on peut baisser le niveau N au niveau N/q si q n'est pas de la forme $(h\mu+1)$, h=entier

<u>condition-a</u> : $q \neq 1 \pmod{\mu}$

Plus tard Ribet montre ceci (un gros morceau) :

Si N ne contient pas μ càd $\mu \nmid N \Leftrightarrow (\mu,N)=1$, alors on peut passer de niveau N à niveau N/q.

<u>condition-b</u> : $\mu \nmid N$

Si on combine ces deux conditions on arrive à ce qu'on appelle le théorème de Ribet. En effet :

On commence par débarrasser de μ :

$\rightarrow$ Si N contient μ ($\Leftrightarrow \mu | N$), on utilise la condition-a :

en effet comme $\mu \neq 1 \pmod{\mu}$ on passe donc de N à N/μ , on supprime μ dans N en fait.

$\rightarrow$ Si N ne contient pas μ ($\Leftrightarrow \mu \nmid N \Leftrightarrow (\mu, N)=1$), on utilise la condition-b :

on passe directement de N à N/q , on supprime q dans N.

Théorème de Ribet (1986):

Soient E une courbe elliptique semi-stable et ρ_μ la représentation définie par :

$\rho_\mu : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow Aut(E[\mu])$, μ premier ≥ 5

On suppose que ρ_μ est : irréductible, modulaire de niveau N (rappel: N sans facteurs carrés $\Leftrightarrow$ E semi-stable).

Soit un $q|N$.

Si ρ_μ est finie en q, alors ρ_μ est modulaire de niveau N/q .

En gros ça veut dire qu'on peut supprimer tous les q dans N quand dans Δ_{min} on a $q^{k\mu}$

$$\begin{cases} N = \cdots q \ldots \\ \Delta_{min} = \cdots q^{k\mu} \ldots \end{cases} \Rightarrow \text{on suprime q dans N}$$

Autre fois le théorème de Ribet s'appelait la conjecture-epsilon.

Exemple:

1) E : $y^2 + xy = x^3 + x^2 - 19x + 685$

$\Delta = -2^{16}.3^5.13$

$c_4 = 937$

$c_6 = -5.23.41.127$

E est minimale car $\forall p, v_p(c_4)<4$

donc $\Delta = \Delta_{min}$

d'autre par $\forall p, (\Delta,c_4)=1$ donc E admet soit de bonnes réductions soit de mauvaises réductions multiplicatibles. La courbe E est donc semi-stable, et son conducteur vaut:
$N = rad(\Delta_{min}) = 2.3.13$
on prend $\mu=5$.

E est modulaire de niveau N donc ρ_μ aussi modulaire de niveau N (théorème (12.5.1)) et on montre que ρ_μ est irréductible . On voit que ρ_μ finie en 3|N (dans Δ la puissance de 3 est 5=1x5) donc ρ_μ modulaire de niveau $N/3 = 2.13$

2) E : $y^2 + xy = x^3 - 10055x - 390309$

$\Delta = -2.3^2.11^{10}$

$c_4 = 482641$

$c_6 = 5.17.19.139.1499$

E est minimale car $\forall p, v_p(c_4)<4$

donc $\Delta = \Delta_{min}$

d'autre par $\forall p$, $(\Delta, c_4)=1$ donc E admet soit de bonnes réductions soit de mauvaises réductions multiplicatibles.

La courbe E est donc semi-stable, et son conducteur vaut:

$N = rad(\Delta_{min}) = 2.3.11$

on prend $\mu=5$.

E est modulaire de niveau N donc ρ_μ aussi modulaire de niveau N (théorème(12.5.1)) et on montre que ρ_μ est irréductible . On voit que ρ_μ finie en 11|N (dans Δ la puissance de 11 est 10=2x5) donc ρ_μ modulaire de niveau $N/11 = 2.3$

13.2 LES COURBES DE HELLEGOUARCH-FREY $E_{A,B}$

Un exemple de courbe elliptique semi-stable.

On se donne trois nombres entiers A, B, C non-nuls ($ABC\neq0$) et premiers entre eux ($(A,B,C)=1$)[1] tels que :

$$\begin{cases} A + B = C \\ A = -1 \pmod 4 \\ B = 0 \pmod{32} \end{cases}$$

[1] Premier entre eux ⇔ premier entre eux 2à2 voir (3.1.1)

et on pose

$E_{A,B}$: $y^2 = x(x - A)(x + B)$; (non minimale)

$E_{A,B}$: $y^2 = x^3 + (B - A)x^2 - ABx$

on appelle courbe de Hellegouarch-Frey.

on a :

$\Delta = 2^4(ABC)^2$

$c_4 = 2^4(-AB+AC+BC)$

$E_{A,B}$ est elliptique car $\Delta \neq 0$.

On voit que $E_{A,B}$ n'est pas minimale en 2, car $2|\Delta$ et $2|c_4$

Voyons si ce model est minimal en tout $p \neq 2$.

Soit $p \neq 2$ et $p|\Delta \Rightarrow p|ABC$ comme p est premier le lemme d'Euler dit que p divise l'un des termes du produit, par ex $p|A$

on a

$c_4 = 2^4(-AB+AC+BC)$

$c_4 = BC \pmod p$

$c_4 = B(A+B) \pmod p$

$c_4 = B^2 \pmod p$

mais

$B^2 \neq 0 \pmod p$ car $B \neq 0 \pmod p$ car $(A,B)=1$ donc

$c_4 \neq 0 \pmod p$ càd $p \nmid c_4$

donc le model $E_{A,B}$ est minimal pour tout $p \neq 2$

Cherchons maintenant les mauvaises réductions pour $p \neq 2$

$p \neq 2$ et mauvaise réduction $\Rightarrow p|\Delta \Rightarrow p|ABC \Rightarrow p|A$ par ex.

$E_{A,B}$: $y^2 = x^3 + (B - A)x^2 - ABx$

$E_{A,B,p}$: $y^2 = x^3 + Bx^2 \pmod p$

$y^2 - Bx^2 = x^3 \pmod p$

Les équations des tangentes en (0,0) sont:

$y^2 - Bx^2 = 0 \pmod p$

Soit ω une racine de B dans $\overline{\mathbb{F}}_p$ (une clôture algébrique de $\mathbb{F}_p$ où se trouvent toutes les racines de $P \in \mathbb{F}_p[X]$), $\omega \in \overline{\mathbb{F}}_p$ et $\omega^2 = B$

$y^2 - \omega^2 x^2 = 0 \pmod p$

$(y - \omega x)(y + \omega x) = 0 \pmod p$

$y = \omega x \pmod p$

$y = -\omega x \pmod p$

deux tangentes distinctes (dans $\overline{\mathbb{F}}_p$) donc c'est une mauvaise réduction multiplicative pour $p \neq 2$.

Cherchons un model minimal pour p=2, pour ça on fait un changement de variables:

$$\begin{cases} x \to 4x \\ y \to 8y + 4x \end{cases}$$

$E_{A,B}$: $y^2 = x^3 + (B - A)x^2 - ABx$

devient

$E'_{A,B}$: $(8y+4x)^2 = (4x)^3 + (B - A)(4x)^2 - 4ABx$

$(8y+4x)^2 = 4^3x^3 + 4^2(B - A)x^2 - 4ABx$

$8^2y^2+4^2x^2+8^2xy = 4^3x^3 + 4^2(B - A)x^2 - 4ABx$

$2^6y^2+2^6xy = 2^6x^3 + 2^4(B - A)x^2 - 2^2ABx - 2^4x^2$

$y^2+xy = x^3 + 2^{-2}(B - A)x^2 - 2^{-4}ABx - 2^{-2}x^2$

$E'_{A,B}$: $y^2+xy = x^3 + 2^{-2}(B - A - 1)x^2 - 2^{-4}ABx$

comme A+1=4A' et B=32B', les coefficients de $E'_{A,B}$ sont des entiers.

$\Delta' = 2^{-8}(ABC)^2$

$c_4' = A^2+B^2+AB$

Soit $2|\Delta'$

$\Rightarrow 2|A$ impossible car (A,B)=1

$\Rightarrow 2|B \Rightarrow$

$c_4' = A^2 \pmod 2$, comme A = impair

$c_4' = 1 \pmod 2 \Leftrightarrow 2 \nmid c_4'$

donc $E'_{A,B}$ est un model minimal pour p=2.

Voyons la réduction en p=2.

$E'_{A,B} : y^2+xy = x^3 +2^{-2}(B - A - 1)x^2 - 2^{-4}ABx$.

$E'_{A,B,2} : y^2+xy = x^3 +kx^2 \pmod 2$

¤ Cas : k=0

$y^2+xy = x^3 \pmod 2$

Les équations des tangentes sont:

$y^2+xy = 0 \pmod 2$

$y(y+x) = 0 \pmod 2$

ça donne 2 tangentes distinctes.

$y = 0 \pmod 2$

$y = -x \pmod 2$

¤ Cas : k=1

$E'_{A,B,2} : y^2+xy = x^3 +x^2 \pmod 2$

$y^2+xy = x^3 +x^2 \pmod 2$

Les équations des tangentes sont:

$y^2+xy - x^2 = 0 \pmod 2$

on pose

$y = \alpha x$

d'où

$\alpha^2x^2 + \alpha x^2 - x^2 = 0 \pmod 2$

$x^2(\alpha^2 + \alpha - 1) = \pmod 2$

on a

$x^2 = 0 \rightarrow x = 0 \pmod 2 \rightarrow y^2 = 0 \pmod 2 \rightarrow y = 0 \pmod 2$

ou

$\alpha^2 + \alpha - 1 = 0 \pmod 2 \rightarrow$ impossible

donc 2 tangentes distinctes.

$x = 0 \pmod 2$

$y = 0 \pmod 2$

on a 2 tangentes distinctes. En p=2 on a aussi une réduction multiplicative.

Donc la courbe $E_{A,B}$ est semi-stable, car on a: soit une bonne réduction, soit une mauvaise réduction multiplicative.

Remarque : dans le calcul pour voir si le model $E'_{A,B}$ est minimal pour 2, on peut faire la même chose avec un p premier ≠2.

$\Delta' = 2^{-8}(ABC)^2$

$c_4^{'} = A^2+B^2+AB$

Soit $p \neq 2$ et $p|\Delta'$
$\Rightarrow p|ABC \Rightarrow p|A$ par exemple $\Rightarrow$
$\Rightarrow c_4^{'} = B^2 \pmod p$ or

$B^2 \neq 0 \pmod p$ car $B \neq 0 \pmod p$ car $(A,B)=1$
$c_4' \neq 0 \pmod 2 \Leftrightarrow p \nmid c_4'$
Ce qui prouve que le model $E'_{A,B}$ est un model minimal.
donc le $\Delta' = \Delta_{min}$

$\Delta_{min} = 2^{-8}(ABC)^2$

$$N = rad(ABC) = \prod_{p|(ABC)} p$$

rad(n) = radical de n = les nombres premiers dans la décomposition de n, par exemple

$n = 2^4.5^2.11.7^3$

$rad(n) = 2.5.11.7$

$E_{A,B}$ est semi-stable ⇒ N=sfc (sans facteurs carrés)

<u>Résumons</u> :

⟶ La courbe $E_{A,B}$ est une courbe elliptique, semi-stable ayant un modèle minimal

$E'_{A,B} : y^2+xy = x^3 + \frac{B-A-1}{4}x^2 - \frac{AB}{16}x$

$\Delta_{min} = 2^{-8}(ABC)^2 = 2^{2h-8}(A'B'C')^2$, dans (A'B'C') pas de 2

$$N = 2.rad(A'B'C') = 2 \prod_{p|A'B'C'} p$$

⟶ La représentation ρ_μ est irréductible, en effet $E_{A,B}$ contient 3 points rationnels (A,0), (-B,0), (0,0) d'ordre 2 et $\mu \geq 5$ (théorème Mazur (12.7.2))

$\longrightarrow \rho_\mu$ est modulaire de niveau N (th Wiles: E modulaire $\Longrightarrow$ ρ_μ modulaire).

$\longrightarrow$ Mais on ne sait pas si ρ_μ est finie en q|N .

14 FIN D'UN ÉNIGME

14.1 L'ÉQUATION DE FERMAT

L'équation de Fermat s'écrit ainsi:

L_n: $x^n + y^n = z^n$

D'après Fermat (1636) elle n'a pas de solution primitive pour n≥3 . Une solution primitive, c'est une solution (a,b,c) $\in \mathbb{Z}^3$ telle que

$a^n + b^n = c^n$

$abc \neq 0$ et

pgcd(a,b,c) = (a,b,c) = 1 premier entre eux

On pourrait restreindre n aux nombres premiers $\mu \geq 5$, en effet si n n'est pas premier il sera de la forme:

$n=2^k p_1 p_2 \ldots$; k=entier naturels, p_i=premier impair

ou (pour simplifier la discution)

$n=2^k\mu$; k=entier naturels, μ=1 ou premier≥3

→ μ=1 (que des nombre premiers 2)

n=2.2.2.... (k≥2 car n≥3)

n=4a

$x^n + y^n = z^n \Rightarrow (x^a)^4 + (y^a)^4 = (z^a)^4$

donc il suffit d'étudier l'équation

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

Si l'équation n=4 n'a pas de solutions alors l'équation $n=2^k$ n'a pas de solutions non plus .

→μ=premier ≥3

$x^n + y^n = z^n \Rightarrow \left(x^{2^k}\right)^\mu + \left(y^{2^k}\right)^\mu = \left(z^{2^k}\right)^\mu$

donc il suffit d'étudier l'équation

$x^\mu + y^\mu = z^\mu$

Si l'équation μ=premier≥3 n'a pas de solutions alors l'équation $n=d\mu$ n'a pas de solutions non plus .

Or on sait que l'équation n'a pas de solutions pour μ=3 et μ=4 donc il suffit de résoudre

L_μ : $x^\mu + y^\mu = z^\mu$ où $\mu \geq 5$ premier

Pendant 358 ans personne n'arrive, la résolution se fait seulement en Septembre 1994 par Andrew Wiles. Cette

équation n'a pas du tout de solutions primitives comme prédisait Fermat.

Supposons que l'équation L_μ admet une solution primitive $(a,b,c) \in \mathbb{Z}^3$ càd :

$$\begin{cases} a^\mu + b^\mu = c^\mu \\ abc \neq 0 \\ (a,b,c) = 1 \end{cases}$$

On va maintenant examiner les propriétés de ce triplet (a,b,c)

Les permutations :

Dans l'écriture $a^\mu + b^\mu = c^\mu$ on peut dire que c est célibataire et que a,b sont en couple, les permutations de a,b,c revient à dire que tout le monde peut devenir célibataire, on veut donc trouver une règle de devenir célibataire.

$a^\mu + b^\mu = c^\mu \Rightarrow$ (a,b,c) ; c=célibataire

$(-a)^\mu + c^\mu = b^\mu \Rightarrow$ (-a,c,b) ; b=célibataire ($-a^\mu=(-a)^\mu$ car μ=impair)

$(-b)^\mu + c^\mu = a^\mu \Rightarrow$ (-b,c,a) ; a=célibataire

$b^\mu + a^\mu = c^\mu \Rightarrow$ (b,a,c) ; échanger a,b

et on peut faire aussi

$-a^\mu - b^\mu = -c^\mu$

$(-a)^\mu + (-b)^\mu = (-c)^\mu$ c'est-à-dire prendre le triplet (-a,-b,-c)

Donc à partir du triplet (a,b,c) on fabrique les 4 autres :

Q = { (a,b,c), (-a,c,b), (-b,c,a), (b,a,c), (-a,-b,-c) }

Autrement dit à partir d'une solution primitive de L_μ on peut en fabriquer 4 autres.

La parité de b :

Les trois nombres a,b,c ne peuvent pas être tous pairs , car ils sont premiers entre eux, donc il y en a un qui est impair disons c = 2k+1 (si c'est a on prend le triplet (-b,c,a) , si c'est b on prend (-a,c,b)) .

a et b ne peuvent pas non plus être tous pairs , ou tous impairs car c est impair donc l'un d'eux est impair disons a=2m+1. et l'autre b=2t pair (si b est impair on prend le triplet (b,a,c)

Finalement on a:

a = 2m+1

b = 2t

c = 2k+1

Modulo 4 :

a = 2m+1 , comme m=2d ou m=2d+1 ça donne

a=2(2d)+1 = 4d +1 $\Rightarrow$ a=1 (mod 4)

a=2(2d+1)+1 = 4d+3 $\Rightarrow$ a=-1 (mod 4)

si a=-1 (mod 4) on prend le triplet (a,b,c)

$a = 2m+1$

$b = 2t$

$c = 2k+1$

sinon on prend $(-a) = -1 \pmod 4$ c'est-à-dire

le triplet (a',b',c') avec a'=-a, b'=-b et c'=-c et on a:

$a'^{\mu} + b'^{\mu} = c'^{\mu}$

$a' = -1 \pmod 4$, a' =2m'-1 impair

b' = 2t' pair

c' = 2k'-1 impair

<u>En résumé</u> : à partir d'une solution primitive (u,v,w) on peut toujours construire une autre solution primitive (a,b,c) qui vérifie en plus les conditions suivantes:

$a = -1 \pmod 4$

b = pair

14.2 LA COURBE $E_{A^{\mu},B^{\mu}}$ EST SEMI-STABLE

Supposons que l'équation de Fermat L_{μ} admet une solution primitive $(u,v,w) \in \mathbb{Z}^3$, elle vérifie donc

$u^{\mu} + v^{\mu} = w^{\mu}$

$uvw \neq 0$

pgcd(u,v,w) = 1 premier entre eux dans leur ensemble

à partir de cette solution (u,v,w) on peut toujours fabriquer une autre solution primitive (a,b,c)

$a^\mu + b^\mu = c^\mu$

$abc \neq 0$

pgcd(a,b,c) = 1 premier entre eux dans leur ensemble

et qui vérifie en plus :

$a = -1 \pmod 4$

$b = 0 \pmod 2$

On va maintenant construire une courbe elliptique E_{a^μ,b^μ} donnée par l'équation ci-dessous:

$E_{a^\mu,b^\mu} : y^2 = x(x - a^\mu)(x + b^\mu)$ (non minimale)

$E_{a^\mu,b^\mu} : y^2 = x^3 + (b^\mu - a^\mu)x^2 - a^\mu b^\mu x$

C'est une courbe de Hellegouarch-Frey $E_{A,B}$ avec $A=a^\mu$ et $B=b^\mu$ le calcule est déjà fait, mais ça ne fait pas mal si on refait le calcul.

Calculons son discriminant Δ et le c_4

$\Delta = - b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9 b_2b_4b_6$

$c_4 = b_2^2 - 24b_4$

On a:

$a_1 = 0, a_3 = 0, a_2 = b^{\mu} - a^{\mu}, \quad a_4 = -a^{\mu} b^{\mu}, \quad a_6 = 0$

$b_2 = 4a_2$

$b_4 = 2a_4$

$b_6 = 0$

$b_8 = -a_4^2$

$\Delta = -b_2^2 b_8 - 8b_4^3 = 4^2 (b^{\mu} - a^{\mu})^2 (a^{\mu} b^{\mu})^2 + 2^6 (a^{\mu} b^{\mu})^3$

$\Delta = 2^4 (a^{\mu} b^{\mu} c^{\mu})^2 = 2^4 (abc)^{2\mu}$

Remarque : On peut aussi utiliser la formule:

$\Delta = \Delta(E) = 16\Delta(P) = 16(0 - a^{\mu})^2 (0 + b^{\mu})^2 (a^{\mu} + b^{\mu})^2$

$\Delta = 2^4 (abc)^{2\mu}$

Comme $abc \neq 0 \Rightarrow \Delta \neq 0 \Rightarrow E_{a^{\mu},b^{\mu}}$ est bien une courbe elliptique

$c_4 = b_2^2 - 24b_4 = 4^2 (b^{\mu} - a^{\mu})^2 + 24.2\, a^{\mu} b^{\mu}$

$= 4^2 (a^{2\mu} + a^{\mu} b^{\mu} + b^{2\mu})$

$c_4 = 2^4 (a^{2\mu} + a^{\mu} b^{\mu} + b^{2\mu})$

On va montrer que l'équation $E_{a^{\mu},b^{\mu}}$ est minimale pour tout p, sauf p=2.

soit p un nombre premier impair tel que $p|\Delta$.

$p|\Delta \Rightarrow p|abc \Rightarrow p|a$ par exemple.

$a = 0 \pmod p$

$c_4 = 2^4(a^{2\mu} + a^\mu b^\mu + b^{2\mu}) \pmod p$

$2^4(a^{2\mu} + a^\mu b^\mu + b^{2\mu}) = 2^4 b^{2\mu} \pmod p$ puisque $a=0 \pmod p$

$b^{2\mu} \neq 0 \pmod p$ car

$b \neq 0 \pmod p$ puisque $p|a$ et $pgcd(a,b)=1$ premier entre eux,

$c_4 \neq 0 \pmod p$

$p \nmid c_4$

Comme $p|\Delta$ et $p \nmid c_4$ le théorème3 nous dit que le modèle E_{a^μ,b^μ} est minimal en p . Donc tous les p impair $p|\Delta$ est une vraie mauvaise réduction.

On va voir quel type de mauvaise réduction pour $p|\Delta$

comme $a=0 \pmod p$ ça donne

$y^2 = x(x - a^\mu)(x + b^\mu)$

$y^2 = x^2(x + b^\mu) \pmod p$, il reste b^μ car $pgcd(a,b)=1$ premiers entre eux

$y^2 - b^\mu x^2 = x^3 \pmod p$

Les équations des tangentes en (0,0):

$y^2 - b^\mu x^2 = 0 \pmod p$

Soit ω une racine de b^μ dans $\overline{\mathbb{F}}_p$, d'où

$y^2 - \omega^2 x^2 = 0 \pmod p$

$y = \omega x \pmod p$

$y = -\omega x \pmod p$

La courbe E_p modulo p donne 2 tangentes distinctes donc c'est une mauvaise réduction multiplicative pour p impair $p|\Delta$.

Voyons le cas p=2, il faut trouver un modèle minimal en p=2 (pour avoir de <u>vraie</u> mauvaise réduction)

On va faire un changement de variables admissibles u=2,

$$\begin{cases} x \to 2^2 x \\ y \to 2^3 y + 2^2 x \end{cases}$$

L'équation E_{a^μ,b^μ} devient:

$$E'_{a^\mu,b^\mu} : y^2 + xy = x^3 + \left(\frac{b^\mu}{4} - \frac{a^\mu + 1}{4}\right)x^2 - \frac{a^\mu b^\mu}{16}x$$

C'est une équation à coefficients entiers , en effet on a:

$\mu \geq 5$

$a = -1 \pmod 4$

$b = 2t$ (pair)

donc

$$\frac{b^\mu}{4} = \frac{2^\mu t^\mu}{4} \Rightarrow \text{entier pair}$$

$a = -1 \pmod 4 \Rightarrow a^\mu = -1 \pmod 4$ car μ=impair

$\Rightarrow \dfrac{a^{\mu}+1}{4} \Rightarrow$ entier

$\dfrac{b^{\mu}}{16} = \dfrac{2^{\mu}t^{\mu}}{16} \Rightarrow$ entier pair

grâce aux formules $\Delta'=u^{-12}\Delta$ et $c'_4 = u^{-4}c_4$ on trouve:

$$\Delta' = \frac{\Delta}{2^{12}}$$

$\Delta' = 2^{-8}(abc)^{2\mu}$, c'est un entier pair car b est pair et $\mu \geq 5$

$c'_4 = (a^{2\mu} + a^{\mu}b^{\mu} + b^{2\mu})$

$2| \Delta'$

$c'_4 = (a^{2\mu} + a^{\mu}b^{\mu} + b^{2\mu})$

$c'_4 = a^{2\mu} \pmod 2$

$c'_4 \neq 0 \pmod 2$ car a est impair

on a $2|\Delta'$ et $2\nmid c'_4$ cela montre que le modèle $E'_{a^{\mu},b^{\mu}}$ est minimal en 2.

Voyons la réduction en 2.

$y^2 + xy = x^3 + \left(\frac{b^{\mu}}{4} - \frac{a^{\mu}+1}{4}\right)x^2 - \frac{a^{\mu}b^{\mu}}{16}x$

comme $a^{\mu} + 1 = 0 \pmod 4 \Rightarrow \frac{a^{\mu}+1}{4} = k$ entier

$y^2 + xy = x^3 + k'x^2 \pmod 2$

¤ Soit cas I , k'=0

$y^2+xy = x^3 \pmod 2$

Les équations des tangentes:

$y^2+xy = 0 \pmod 2$

$y(y+x) = 0 \pmod 2$

$y = 0 \pmod 2$

$y = -x \pmod 2$

deux tangentes distinctes.

¤ Soit cas II, k'=1

$y^2+xy = x^3 +x^2 \pmod 2$

Les équations des tangentes :

$y^2+xy - x^2 = 0 \pmod 2$

on pose

$y = \alpha x$

d'où

$\alpha^2x^2 + \alpha x^2 - x^2 = 0 \pmod 2$

$x^2(\alpha^2 + \alpha - 1) = \pmod 2$

on a

$x^2 = 0 \rightarrow x = 0 \pmod 2 \rightarrow y = 0 \pmod 2$

où

$\alpha^2 + \alpha - 1 = 0 \pmod 2 \rightarrow$ impossible

donc 2 tangentes distinctes.

$x = 0 \pmod 2$

$y = 0 \pmod 2$

finalement la réduction en 2 donne une mauvaise réduction multiplicative.

On peut donc énoncer le théorème suivant:

Théorème 7 : La courbe E_{a^μ,b^μ} est semi-stable (youpi !!!)

Remarque : L'équation

$$E'_{a^\mu,b^\mu} : y^2 + xy = x^3 + \left(\frac{b^\mu}{4} - \frac{a^\mu + 1}{4}\right)x^2 - \frac{a^\mu b^\mu}{16}x$$

est minimale (car on a: $p|\Delta'$ et $p \nmid c'_4$ pour tout p) donc $\Delta' = \Delta_{min} = 2^{-8}(abc)^{2\mu}$

Le conducteur N de E_{a^μ,b^μ} (produit des mauvaises réductions) vaut

$$N = \prod_{p=\text{mauvaise}} p^k$$

comme E_{a^μ,b^μ} est semi-stable $\Rightarrow$ k=1 , N sans facteurs carrés

$$N = \prod_{p=\text{mauvaise}} p$$

$$N = \prod_{p|\Delta_{min}} p$$

$$N = \prod_{p|abc} p$$

14.3 LA CONJECTURE DE FERMAT (1636-1994)

D'après le théorème de Wiles E_{a^μ,b^μ} est modulaire de niveau N, avec N sans facteur carrés (car E_{a^μ,b^μ} est semi-stable) .

Voyons maintenant ce qui ce passe du côté de ρ_μ la représentation attachée de $E_{a^\mu,b^\mu}[\mu]$.

Comme E_{a^μ,b^μ} est modulaire, d'après le théorème (12.5.1), ρ_μ est modulaire de niveau N (=le conducteur de E_{a^μ,b^μ})

Et d'après le théorème de Mazur (12.7.2) la représentation ρ_μ :

$\rho_\mu : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow Aut(E_{a^\mu,b^\mu}[\mu])$

est irréductible, en effet E_{a^μ,b^μ} contient 3 points rationnels d'ordre 2 : $(a^\mu,0)$, $(-b^\mu,0)$ et (0,0) et $\mu \geq 5^{(*)}$.

D'autre part on a :

$\Delta_{min} = 2^{-8}(abc)^{2\mu} = 2^{2h\mu-8}(a'b'c')^{2\mu}$; pas de 2 dans (a'b'c')

$$N = \prod_{p|a'b'c'} p = 2\,\mathrm{rad}(a'b'c')$$

Voyons maintenant si ρ_μ est finie en q=2 ?? ,

$2h\mu - 8 = 0 \pmod{\mu}$

$8 = 0 \pmod{\mu}$

$8 = m\mu \Rightarrow$ impossible car μ=premier ≥ 5

donc ρ_μ n'est pas finie en 2. Voyons les autres q|N et $q \neq 2$

$\Delta_{min} = 2^{2h\mu-8}(a'b'c')^{2\mu}$; pas de 2 dans (a'b'c')

$\Delta_{min} = q^{2m\mu}\ 2^{2h\mu-8}(a''b''c'')^{2\mu}$; isolons q

$\Delta_{min} = q^{2m\mu} D \Rightarrow \mu | v_q(\Delta_{min}) \Rightarrow$ ρ_μ est bien finie en $q \neq 2$

donc d'après le théorème de Ribet, ρ_μ est modulaire de niveau N/q,

Comme à chaque fois qu' on a $q \neq 2$ et q|N, ρ_μ est finie en q (on a vraiment de la chance !!)

on peut donc continuer comme ça , ρ_μ est modulaire de niveau $N \rightarrow N/q \rightarrow N/qq' \rightarrow N/qq'q'' \rightarrow$ ... ainsi on supprime tous les premiers impairs de N et il ne reste plus que 2. Finalement ρ_μ est modulaire de niveau 2.

C'est-à-dire il existe une forme modulaire non-nulle $F \in S_2(2)$

$$F = \sum_{n\geq 1}^{\infty} b_n q^n$$

telle que

$t_p = b_p \pmod{\mu}$ pour tout $p \nmid \mu N$

Mais alors on a:

dim $S_2(2) = 0 \Rightarrow S_2(2) = \{0\}$, une telle forme F non-nul n'existe pas d'où la contradiction .

Conclusion le triplet (a,b,c) n'existe pas !! donc l'équation de Fermat L_μ n'a pas de solutions entiers non-nuls.

Ouuuffe !!! 358 ans de galère !!!!

Remarque : Pour la courbe Hellegouarch-Frey $E_{A,B}$, on ne sait pas si ρ_μ est finie en q|N , par contre pour la courbe E_{a^μ,b^μ} c'est l'équation de Fermat ($a^\mu+b^\mu = c^\mu$) qui permet à ρ_μ d'être finie en q|N donc d'appliquer le théorème de Ribet qui conduit au contradiction .

(°) Puisque la conjecture est déjà démontrée pour μ=3,4,5,7 .

On pourrait prendre μ premier ≥11 et utilise le théorème de Mazur (12.7.1) (ρ_μ est irréductible) .

15 UNE BRÈVE HISTOIRE DE LA CONJECTURE DE FERMAT

15.1 UN DÉFIT

En 1636 Fermat lançait un défit suivant aux mathématiciens:

L'équation $x^n + y^n = z^n$ n'a pas de solutions entiers naturels non-nuls pour $n \geq 3$, et d'autant plus il prétendait d'avoir une démonstration.

Depuis ce jour-là beaucoup de grands mathématiciens essayaient de démontrer ce théorème mais personne arrive, et on ne montre que des cas particuliers de n.

¤ Fermat lui même (1636) n=4

¤ Euler (1753) n=3

¤ Dirichlet et Legendre (1825) n=5

¤ Lamé (1839) n=7

¤ Kummer (1847) n=p premier régulier

Puis .... rien ... plus rien ... jusqu'en ....

¤ En 1969 (112 ans plus tard) Hellegouarch a une idée révolutionnaire ... Il suppose que l'équation de Fermat a une solution primitive (a,b,c) c'est-à-dire on a la relation

$a^\mu + b^\mu = c^\mu$; avec $\mu \geq 5$ premier

et à partir de cette solution il construit la courbe elliptique

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

et il étude l'ensemble E[μ] des points de μ-torsion en espérant que cela conduira à une contradiction, mais malheureusement il n'a pas abouti ...

¤ Fallting (1983) : l'équation de Fermat possède un nombre fini de solutions en entiers, mais le théorème ne dit pas qu'on a zéro 0 solution !

¤ En 1984 Frey reprend l'idée de Hellegouarch mais au lieu d'étudier E[μ] il étudie la représentation ρ_μ provenant E[μ] et il arrive à trouver une contradiction ! par contre ses explications sont vagues, pas très claires mais tout le monde s'y croit ! et tout le monde travaille dessus. Et c'est Serre qui reformule mathématiquement les idées de Frey, puis les met sous la forme d'une conjecture nommée la conjecture epsilon .

conjecture- epsilon: Si ρ_μ irréductible, modulaire de niveau N (sans facteur carré), et finie en q|N alors ρ_μ est modulaire de niveau N/q.

¤ Après deux ans d'effort (1986) Ribet arrive à démontrer la conjecture-epsilon (théorème de Ribet)

¤ Un peu plus tard Mazur démontre que ρ_μ est irréductible (théorème de Mazur), et l'équation de Fermat L_μ montre que ρ_μ est finie en q|N.

Voilà maintenant pour démontrer la conjecture de Fermat il suffit de montrer que ρ_μ est modulaire de niveau N (sans facteur carré), ou que E_{a^μ,b^μ} est modulaire de niveau N sans facteur carré (car on voit facilement que E_{a^μ,b^μ} modulaire $\Rightarrow$ ρ_μ modulaire). Avant on ne sait pas comment attaquer la conjecture de Fermat dans le cas général μ=premier ≥ 5, maintenant on a un angle d'attaque la conjecture TSW (toute courbe elliptique est modulaire) .

¤ C'est ainsi que Wiles procède, il attaque la conjecture TSW, pendant 7 ans de travail dans un secret absolu il annonce la démonstration en 6/1993 mais assez tôt on découvre une erreur dans sa démonstration !! et finalement il a réussi à corriger cette erreur en 9/1994 (à l'aide de Taylor) il fallait plus un an pour corriger cette erreur ... Wiles a démontré la conjecture TSW pour la famille de courbes elliptiques semi-stable (N sans facteur carré) dont E_{a^μ,b^μ} fait partie.
Ainsi E_{a^μ,b^μ} $\Rightarrow$ semi-stable $\Rightarrow$ E_{a^μ,b^μ} modulaire de niveau N $\Rightarrow$ ρ_μ modulaire de niveau N $\Rightarrow$ ρ_μ modulaire de niveau 2 $\Rightarrow$ contradiction car $S_2(2) = \{0\}$.
Résumons les noms des acteurs:

<u>Saison 1</u> :

¤ Fermat (1636)

¤ Euler (1753)

¤ Dirichlet, Legendre (1825)

¤ Lamé (1839)

¤ Kummer (1847)

Saison 2 :

Taniyama (1955)

Shimura (1958)

Weil (1960)

Hellegouarch (1969)

Frey (1984)

Serre (1985)

Ribet (1986)

Mazur (1987)

Wiles (1994)

TABLE DES MATIÈRES

Du même auteur

¤*1 La conjecture de Fermat*

C'est un livre qui démontre la conjecture de Fermat, (appelé souvent "le dernier théorème de Fermat") en s'appuyant sur deux théorèmes: le théorème de Ribet et le théorème de Wiles. Un document rare et exceptionnel.

¤*2 La Relativité Générale*

Tout sur la Relativité Générale et on trouve une démonstration de l'équation tensorielle d'Einstein à partir du principe moindre action, ce qui est très rare.

¤*3 Le Groupe du Rubik's Cube (Tome I, II)*

Le Rubik's Cube possède un groupe très riche en propriétés et si la partie mathématique du puzzle vous intéresse alors ce livre est pour vous.

¤*4 La Relativité Restreinte*

La Relativité Restreinte est une théorie physique proposée par Einstein pour remplacer la mécanique newtonienne quand la vitesse des objets est proche à celle de la lumière c.

¤*5 La chasse aux nombres transcendants (Tome I, II)*

Les nombres transcendants sont très mystérieux, ils sont partout, beaucoup plus nombreux que les nombres algébriques et pour tant on connaît très peu de ces nombres, le premier est e, puis π, cos(1) , ...

¤*6 La Cubologie (Tome I, II)*

Pour comprendre les propriétés des twists il faut passer par les mathématiques, à chaque twist on associe un groupe et ce sont des propriétés de ce groupe qui expliquent les propriétés du twist.

¤*7 La physique quantique (Tome I, II)*

Si vous voulez savoir ce que c'est la physique quantique , ce livre est pour vous.