# Intersection arithmétique et problème de Lehmer elliptique

Bruno Winckler

20 novembre 2015

# Plan

# Plan

# Plan

# Plan

# Plan

# Problèmes diophantiens

Une équation diophantienne est une équation polynomiale à coefficients entiers, dont on cherche les solutions entières ou rationnelles.

# Problèmes diophantiens

Une équation diophantienne est une équation polynomiale à coefficients entiers, dont on cherche les solutions entières ou rationnelles.
Exemples :

# Problèmes diophantiens

Une équation diophantienne est une équation polynomiale à coefficients entiers, dont on cherche les solutions entières ou rationnelles.
Exemples :

- l'équation $x + y = 1$ a une infinité de solutions entières (et rationnelles), $(x, y) = (2, -1)$, $(3, -2)$, *etc.* ;

# Problèmes diophantiens

Une équation diophantienne est une équation polynomiale à coefficients entiers, dont on cherche les solutions entières ou rationnelles.
Exemples :

- l'équation $x + y = 1$ a une infinité de solutions entières (et rationnelles), $(x, y) = (2, -1)$, $(3, -2)$, *etc.* ;
- l'équation $x^2 + y^2 = 1$ a un nombre fini de solutions entières ($(x, y) = (0, \pm 1)$ ou $(\pm 1, 0)$), mais un nombre infini de solutions rationnelles ($(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ pour $t$ rationnel) ;

# Problèmes diophantiens

Une équation diophantienne est une équation polynomiale à coefficients entiers, dont on cherche les solutions entières ou rationnelles.
Exemples :

- l'équation $x + y = 1$ a une infinité de solutions entières (et rationnelles), $(x, y) = (2, -1)$, $(3, -2)$, *etc.* ;
- l'équation $x^2 + y^2 = 1$ a un nombre fini de solutions entières ($(x, y) = (0, \pm 1)$ ou $(\pm 1, 0)$), mais un nombre infini de solutions rationnelles ($(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ pour $t$ rationnel) ;
- l'équation $y^2 = x^3 + x$ a un nombre fini de solutions rationnelles ($(x, y) = (0, \pm 1)$).

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Z}$

$|x| \leqslant 1$, $|y| \leqslant 1$, on teste toutes les possibilités, et $(x, y) = (\pm 1, 0)$ ou $(0, \pm 1)$.

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Q}$ : méthode 1

On cherche les solutions *entières* et premières entre elles de

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

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Q}$ : méthode 1

On cherche les solutions *entières* et premières entre elles de

$$(X + iY)(X - iY) = Z^2.$$

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Q}$ : méthode 1

On cherche les solutions *entières* et premières entre elles de

$$\underbrace{(X + iY)}_{=(u+iv)^2}(X - iY) = Z^2.$$

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Q}$ : méthode 1

On cherche les solutions *entières* et premières entre elles de

$$\underbrace{(X + iY)}_{=(u+iv)^2}(X - iY) = Z^2.$$

Alors $X + iY = (u + iv)^2 \Rightarrow (X, Y, Z) = (u^2 - v^2, 2uv, u^2 + v^2)$,

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Q}$ : méthode 1

On cherche les solutions *entières* et premières entre elles de

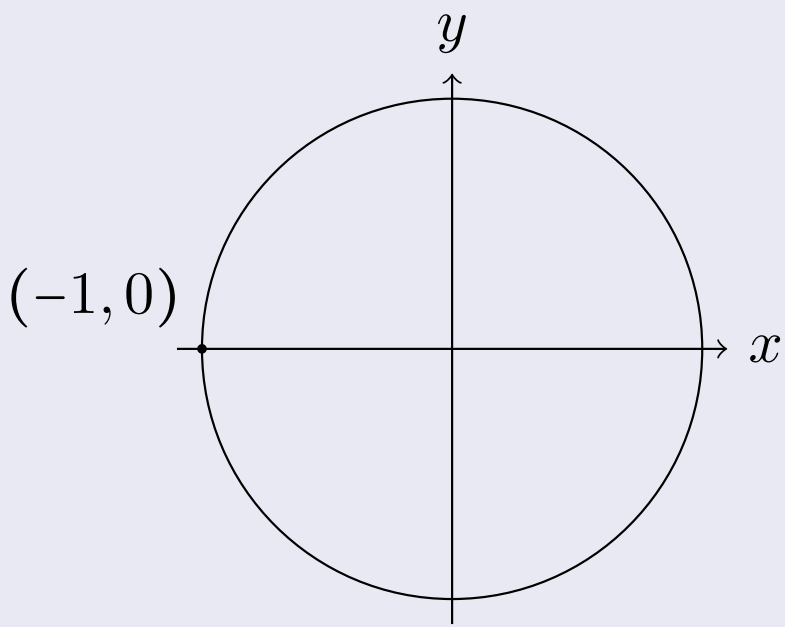
$$\underbrace{(X + iY)}_{=(u+iv)^2}(X - iY) = Z^2.$$

Alors $X + iY = (u + iv)^2 \Rightarrow (X, Y, Z) = (u^2 - v^2, 2uv, u^2 + v^2)$, et $(x, y) = \left(\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, $t = \frac{v}{u} \in \mathbb{Q}$.

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Q}$ : méthode 2

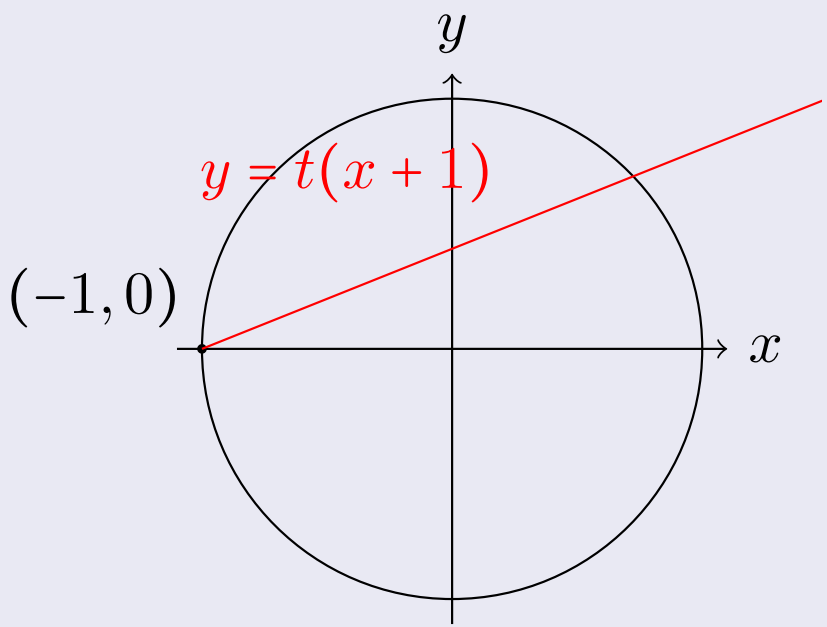



et $(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, $t \in \mathbb{Q}$.

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Q}$ : méthode 2

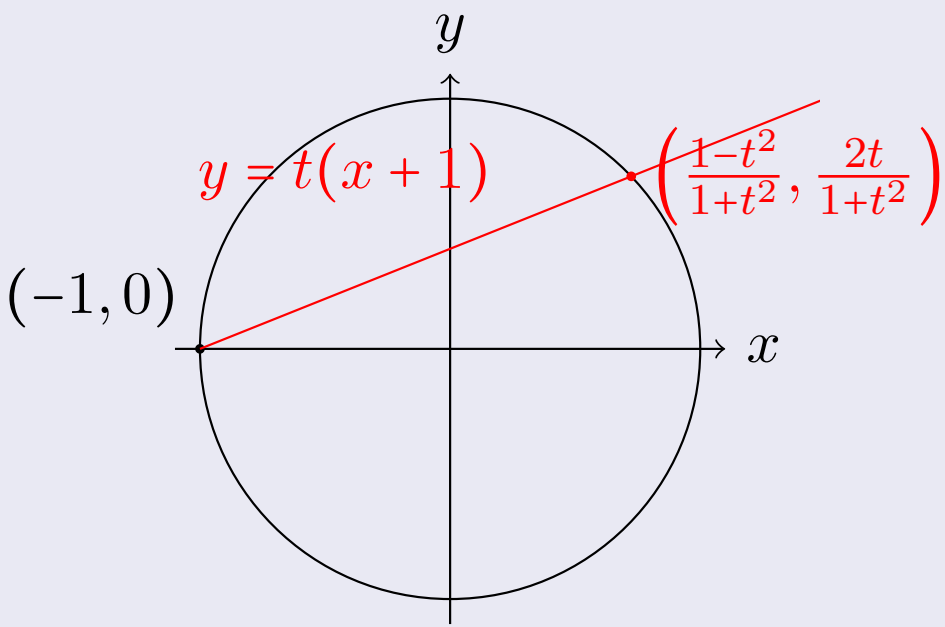



et $(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, $t \in \mathbb{Q}$.

# Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$.

## Résolution dans $\mathbb{Q}$ : méthode 2




et $(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, $t \in \mathbb{Q}$.

# Exemple introductif : quelques enseignements

- On gagne à étudier les équations dans $\bar{\mathbb{Q}}$ (nombres algébriques) plutôt que dans $\mathbb{Q}$ ;

# Exemple introductif : quelques enseignements

- On gagne à étudier les équations dans $\bar{\mathbb{Q}}$ (nombres algébriques) plutôt que dans $\mathbb{Q}$ ;
- On gagne à voir géométriquement les équations ;

# Exemple introductif : quelques enseignements

- On gagne à étudier les équations dans $\bar{\mathbb{Q}}$ (nombres algébriques) plutôt que dans $\mathbb{Q}$ ;
- On gagne à voir géométriquement les équations ;
- Pour $x = \frac{a}{b} \in \mathbb{Q}$, $\mathrm{pgcd}(a, b) = 1$, on peut étudier la *hauteur de* $x$, définie par :

$$h(x) = \ln(\max(|a|, |b|)),$$

pour tout $c > 0$, l'ensemble $\{x \in \mathbb{Q} \mid h(x) \leqslant c\}$ est fini.

# Exemple introductif : quelques enseignements

- On gagne à étudier les équations dans $\bar{\mathbb{Q}}$ (nombres algébriques) plutôt que dans $\mathbb{Q}$ ;
- On gagne à voir géométriquement les équations ;
- Pour $x = \frac{a}{b} \in \mathbb{Q}$, $\mathrm{pgcd}(a, b) = 1$, on peut étudier la *hauteur de* $x$, définie par :

$$h(x) = \ln(\max(|a|, |b|)) = \ln\left(|b| \max\left(\left|\frac{a}{b}\right|, |1|\right)\right),$$

pour tout $c > 0$, l'ensemble $\{x \in \mathbb{Q} \mid h(x) \leqslant c\}$ est fini.

# Exemple introductif : quelques enseignements

- On gagne à étudier les équations dans $\bar{\mathbb{Q}}$ (nombres algébriques) plutôt que dans $\mathbb{Q}$ ;
- On gagne à voir géométriquement les équations ;
- Pour $x = \frac{a}{b} \in \mathbb{Q}$, $\mathrm{pgcd}(a, b) = 1$, on peut étudier la *hauteur de* $x$, définie par :

$$h(x) = \ln(\max(|a|, |b|)) = \ln\left(|b| \max\left(|x|, |1|\right)\right),$$

pour tout $c > 0$, l'ensemble $\{x \in \mathbb{Q} \mid h(x) \leqslant c\}$ est fini.

# Exemple introductif : quelques enseignements

- On gagne à étudier les équations dans $\bar{\mathbb{Q}}$ (nombres algébriques) plutôt que dans $\mathbb{Q}$ ;
- On gagne à voir géométriquement les équations ;
- Pour $x = \frac{a}{b} \in \mathbb{Q}$, $\mathrm{pgcd}(a, b) = 1$, on peut étudier la *hauteur de* $x$, définie par :

$$h(x) = \ln(\max(|a|, |b|)) = \ln(\max(|x|, 1)) - \sum_p \ln(|b|_p),$$

où $|b|_p = \frac{1}{p^k}$, avec $p^k$ la plus grande puissance de $p$ divisant $b$ ; pour tout $c > 0$, l'ensemble $\{x \in \mathbb{Q} \mid h(x) \leqslant c\}$ est fini.

# Exemple introductif : quelques enseignements

- On gagne à étudier les équations dans $\bar{\mathbb{Q}}$ (nombres algébriques) plutôt que dans $\mathbb{Q}$ ;
- On gagne à voir géométriquement les équations ;
- Pour $x = \frac{a}{b} \in \mathbb{Q}$, $\mathrm{pgcd}(a, b) = 1$, on peut étudier la *hauteur de* $x$, définie par :

$$h(x) = \ln(\max(|a|, |b|)) = \ln(\max(|x|, 1)) + \sum_p \ln(\max(|x|_p, 1)),$$

où $|b|_p = \frac{1}{p^k}$, avec $p^k$ la plus grande puissance de $p$ divisant $b$ ; pour tout $c > 0$, l'ensemble $\{x \in \mathbb{Q} \mid h(x) \leqslant c\}$ est fini.

# Exemple introductif : quelques enseignements

- On gagne à étudier les équations dans $\bar{\mathbb{Q}}$ (nombres algébriques) plutôt que dans $\mathbb{Q}$ ;
- On gagne à voir géométriquement les équations ;
- Pour $x \in \bar{\mathbb{Q}}$, on peut étudier la *hauteur de* $x$, définie par :

$$h(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \ln(\max(|x|_v, 1)),$$

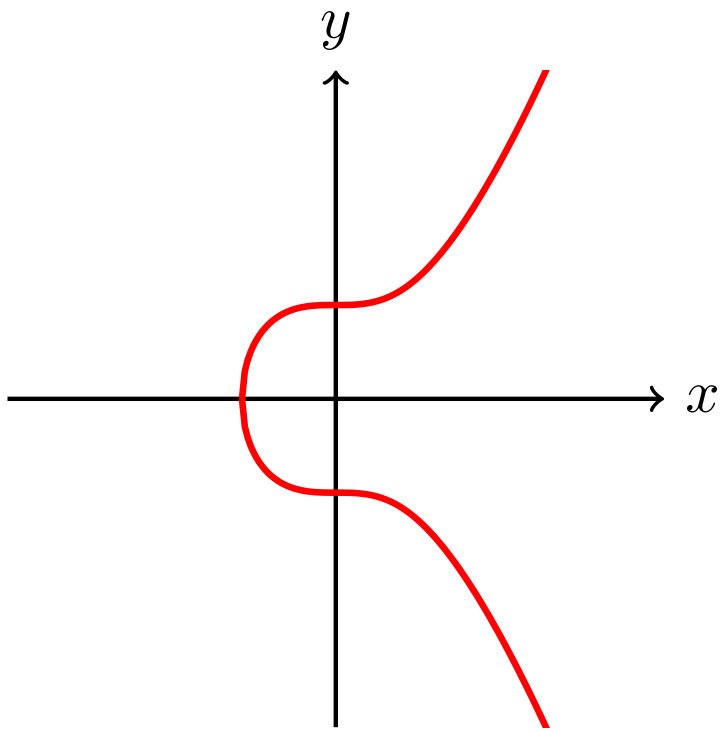
où $x \in K$, $K$ corps de nombres.
Pour tous $c, d > 0$, l'ensemble

$$\{x \in \bar{\mathbb{Q}} \mid h(x) \leqslant c, [\mathbb{Q}(x) : \mathbb{Q}] \leqslant d\}$$

est fini.

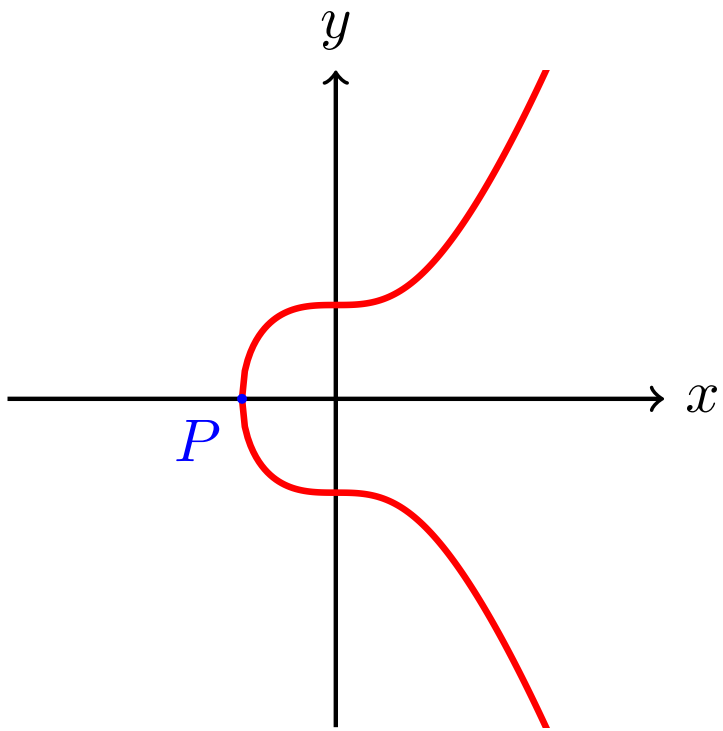
# Courbes elliptiques
## loi de groupe et points rationnels

Soit $K$ un corps de nombres. Une courbe elliptique $E/K$ est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ sont tels que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



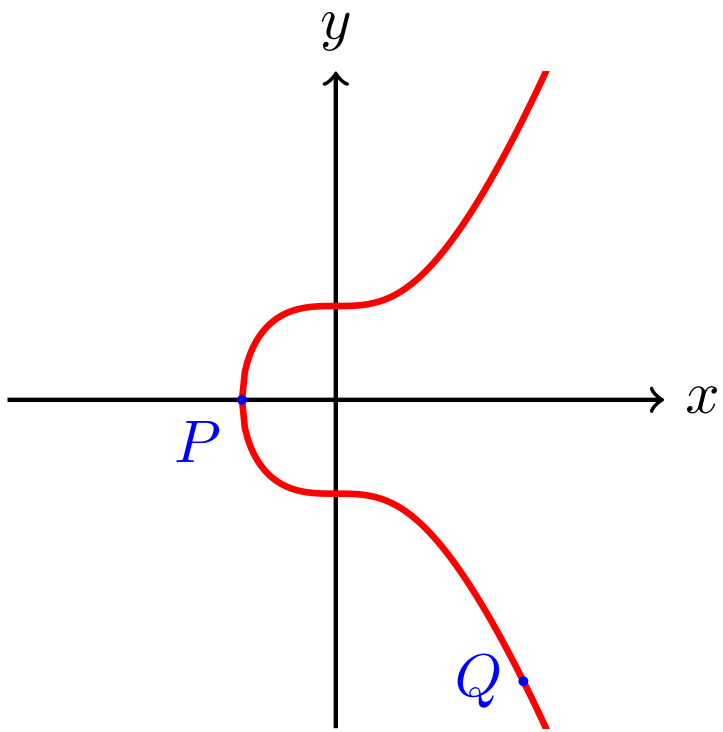
# Courbes elliptiques
## loi de groupe et points rationnels

Soit $K$ un corps de nombres. Une courbe elliptique $E/K$ est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ sont tels que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



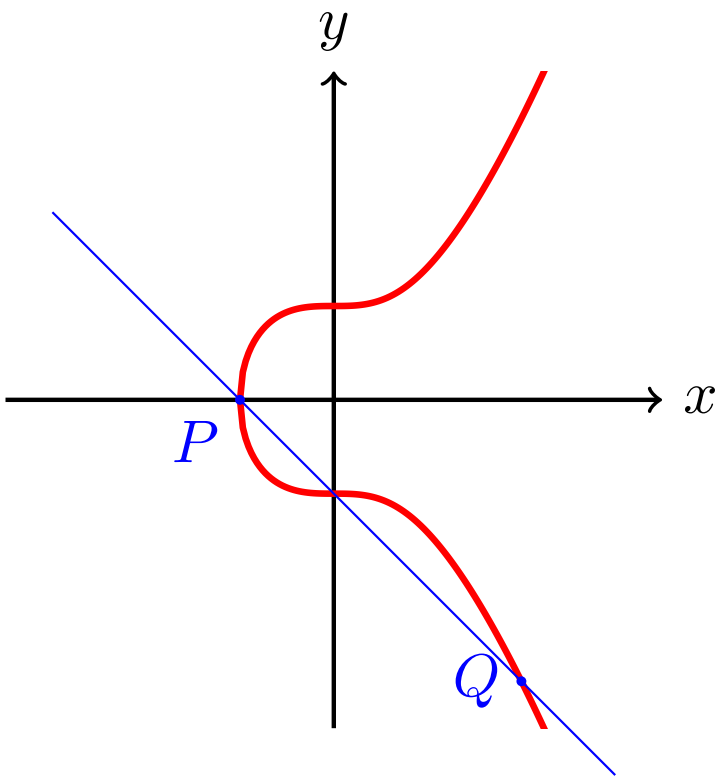
# Courbes elliptiques
## loi de groupe et points rationnels

Soit $K$ un corps de nombres. Une courbe elliptique $E/K$ est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ sont tels que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



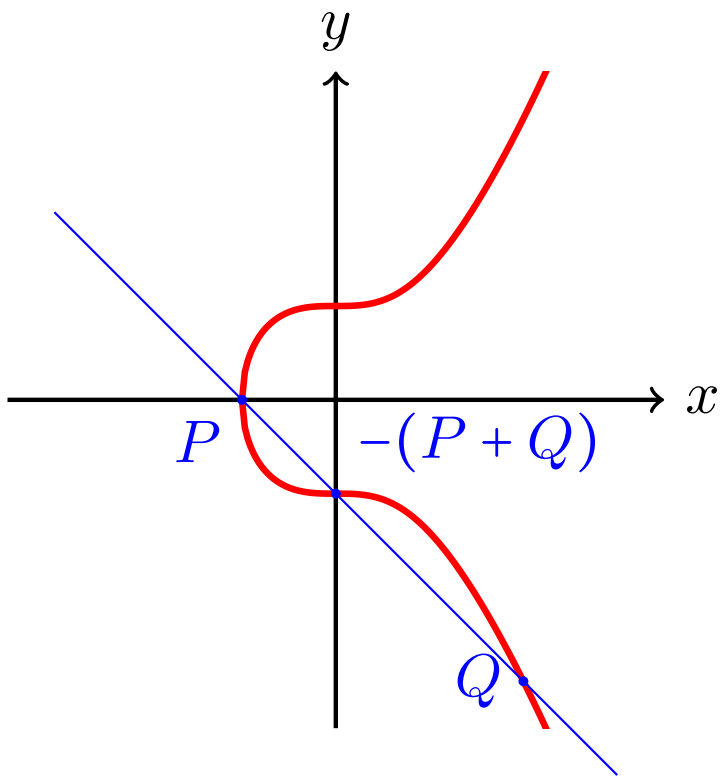
# Courbes elliptiques
## loi de groupe et points rationnels

Soit $K$ un corps de nombres. Une courbe elliptique $E/K$ est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ sont tels que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



# Courbes elliptiques
## loi de groupe et points rationnels

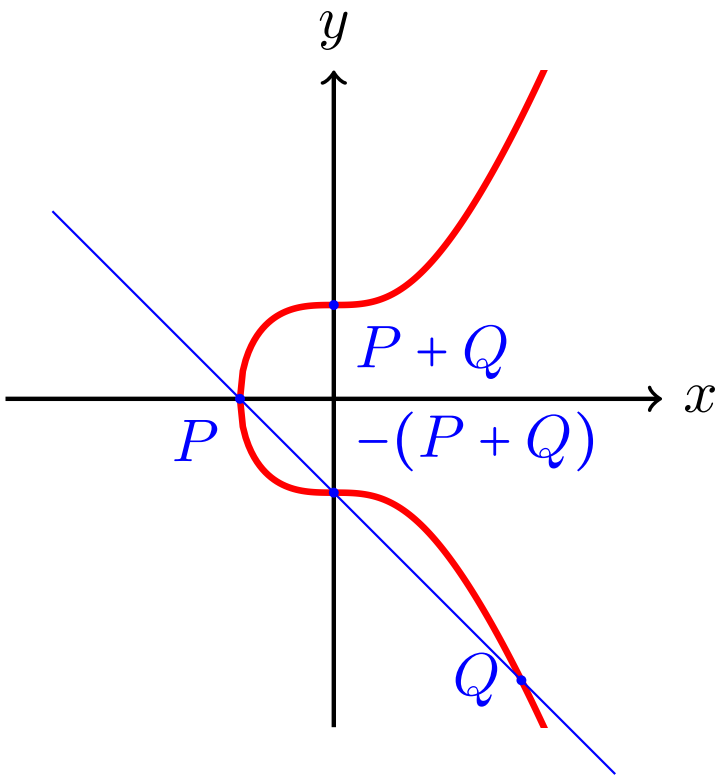
Soit $K$ un corps de nombres. Une courbe elliptique $E/K$ est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ sont tels que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



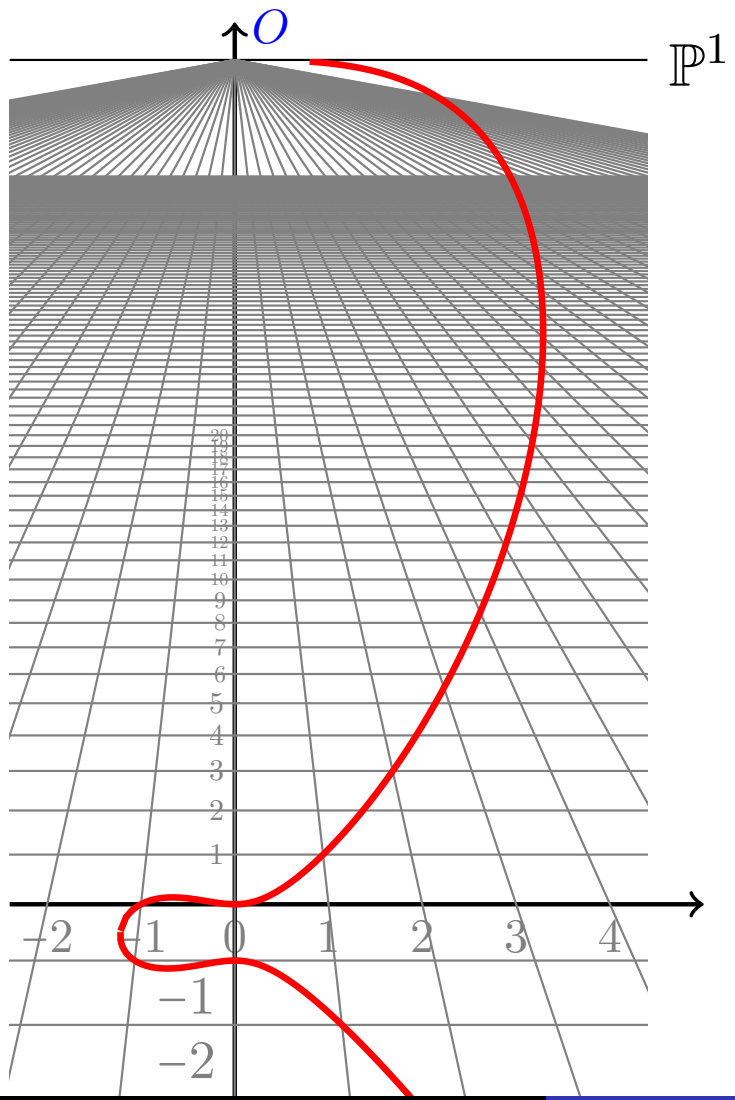
# Courbes elliptiques

## loi de groupe et points rationnels

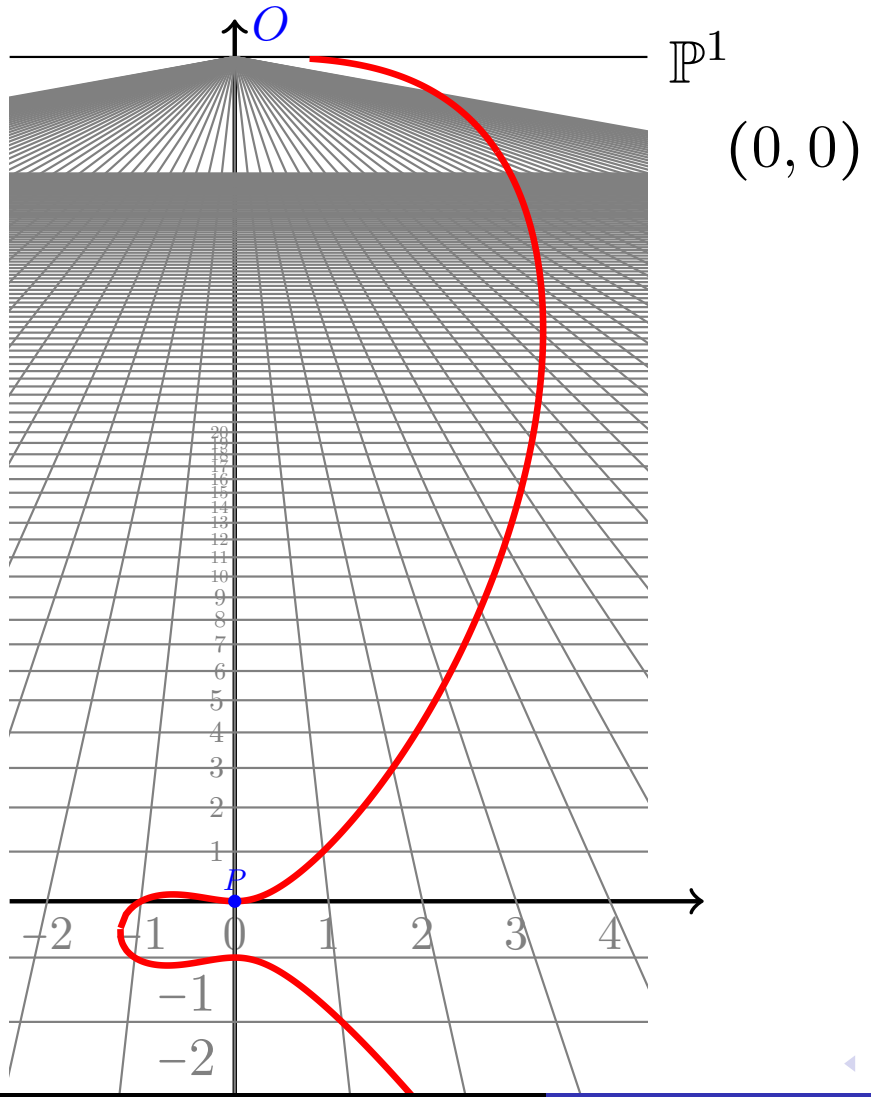
Soit $K$ un corps de nombres. Une courbe elliptique $E/K$ est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ sont tels que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



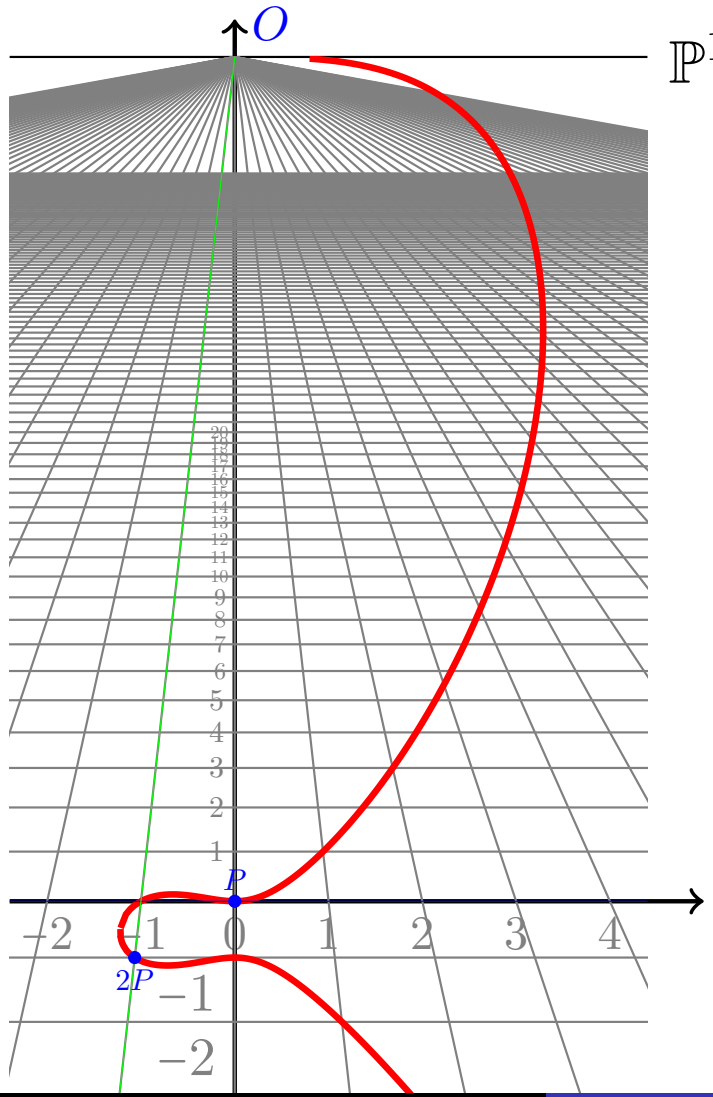
# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.



# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.



# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.

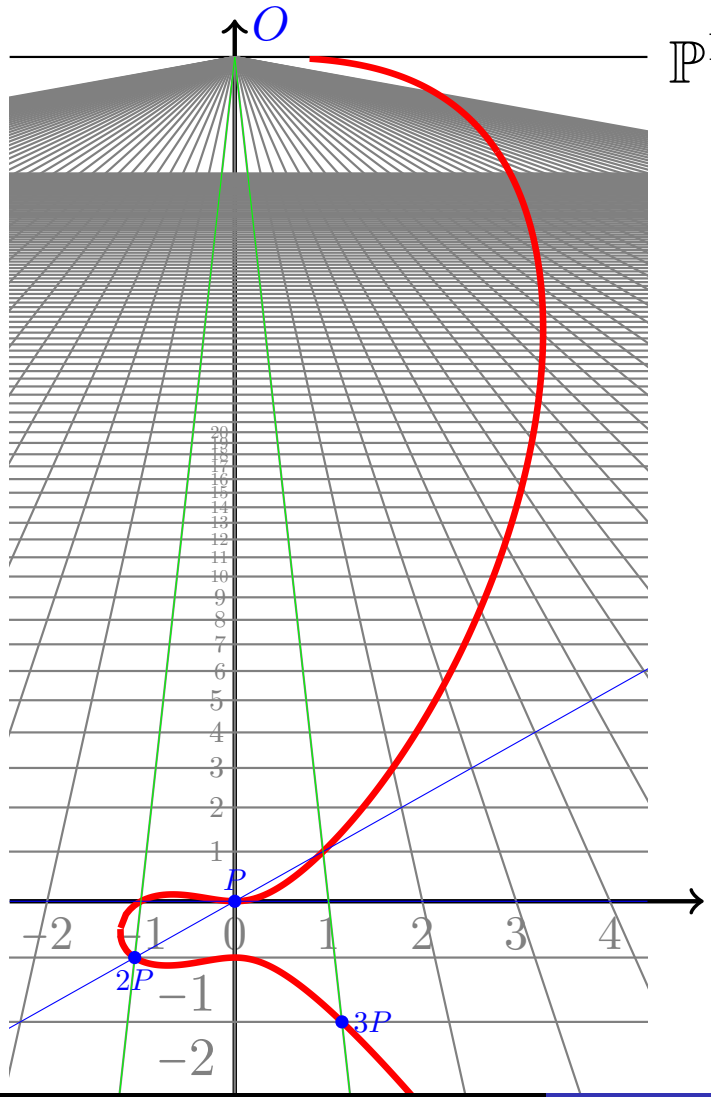



$\mathbb{P}^1$

$(0, 0)$

$(-1, -1)$

# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.



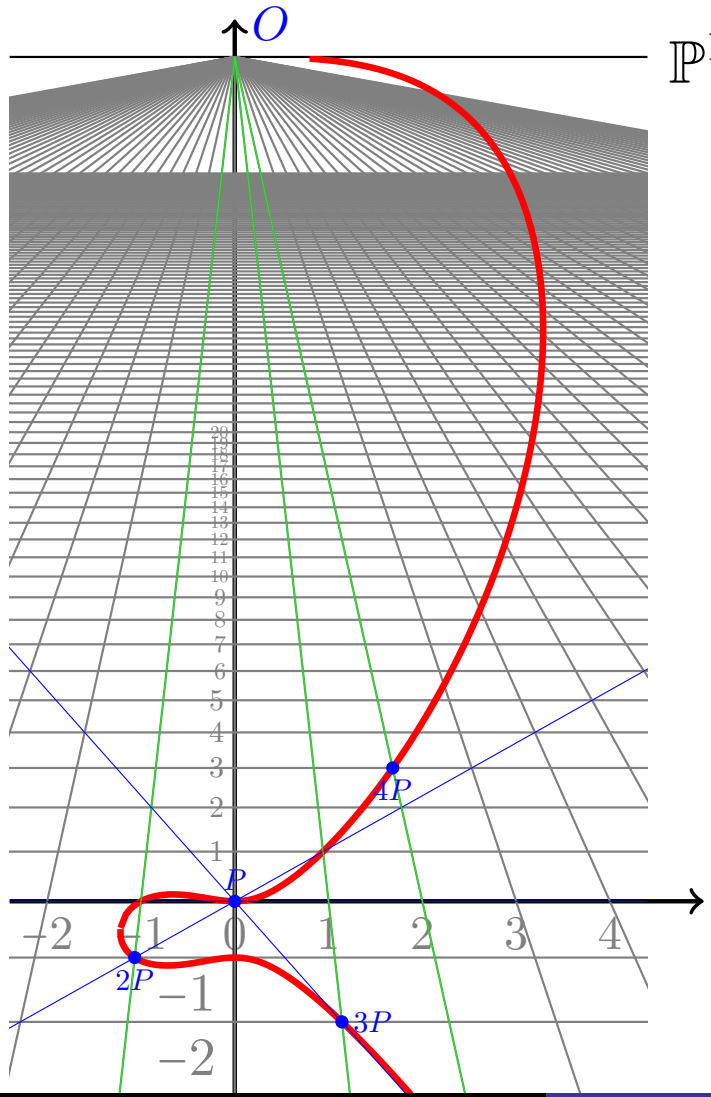

$\mathbb{P}^1$

$(0, 0)$

$(-1, -1)$

$(1, -2)$

# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.




$\mathbb{P}^1$

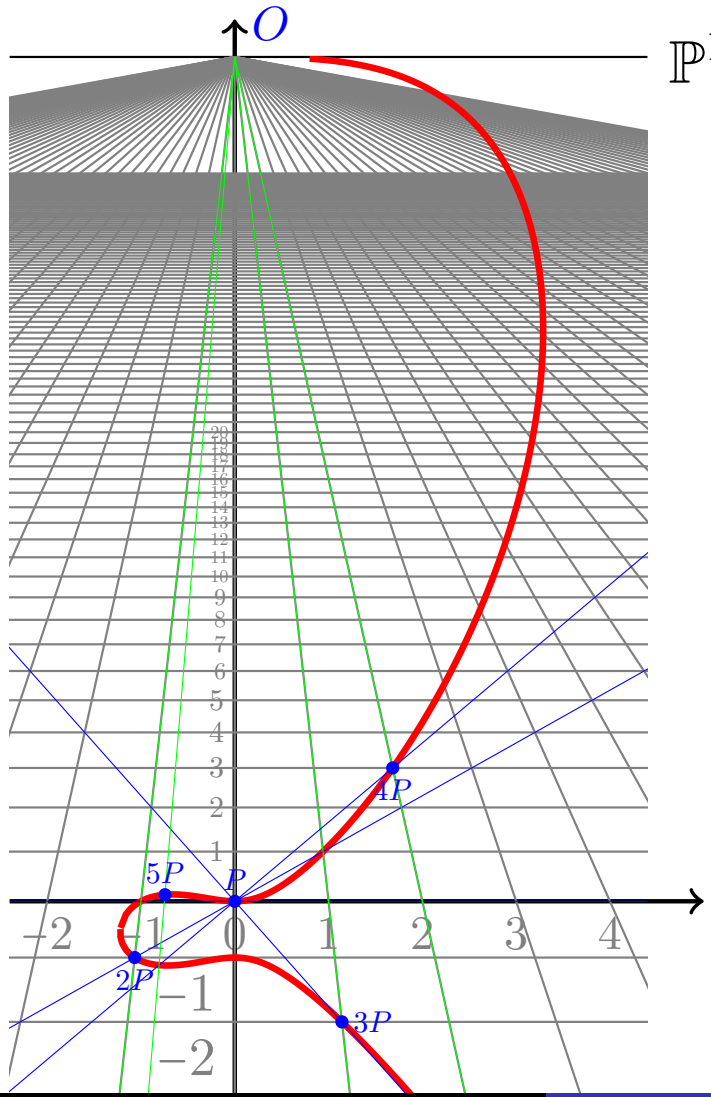
$(0,0)$

$(-1,-1)$

$(1,-2)$

$(2,3)$

# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.




$\mathbb{P}^1$

$(0,0)$

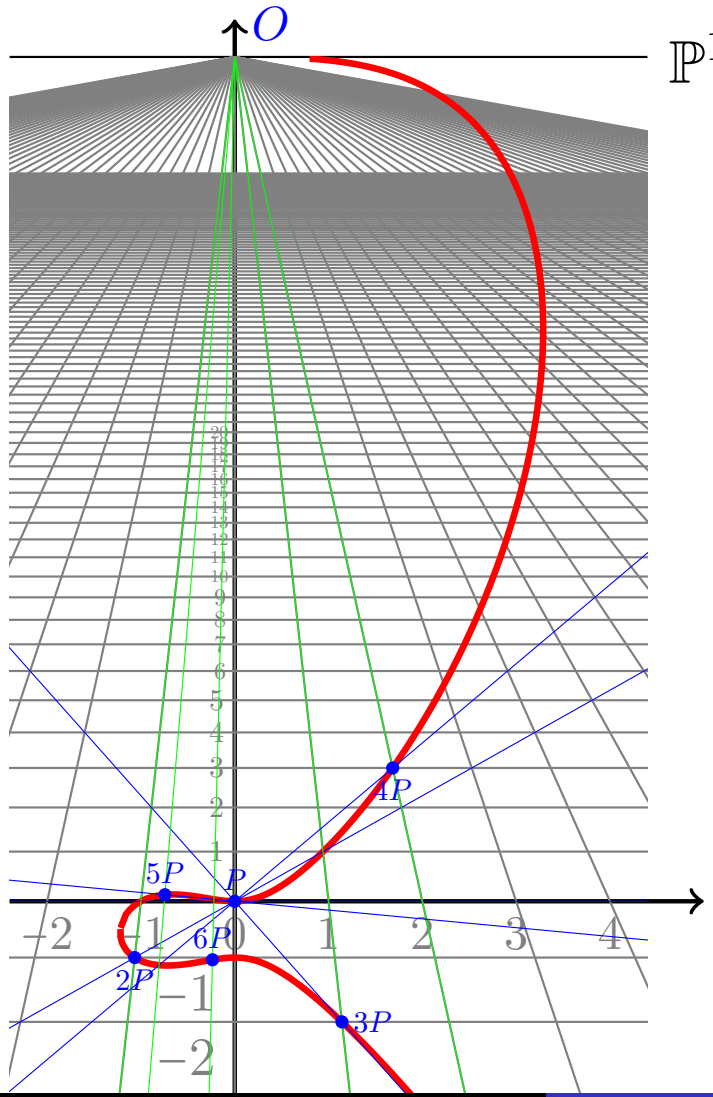
$(-1,-1)$

$(1,-2)$

$(2,3)$

$\left(-\frac{3}{4},\frac{1}{8}\right)$

# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.




$\mathbb{P}^1$

$(0, 0)$

$(-1, -1)$

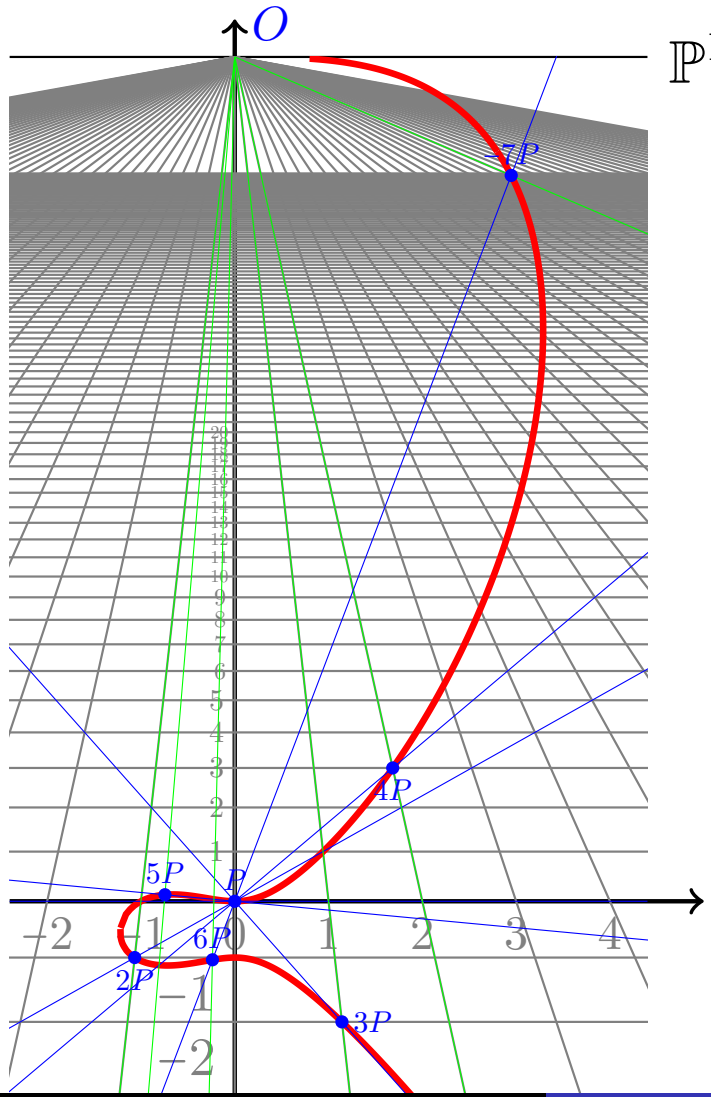
$(1, -2)$

$(2, 3)$

$\left(-\frac{3}{4}, \frac{1}{8}\right)$

$\left(-\frac{2}{9}, -\frac{28}{27}\right)$

# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.




$\mathbb{P}^1$

$(0,0)$

$(-1,-1)$

$(1,-2)$

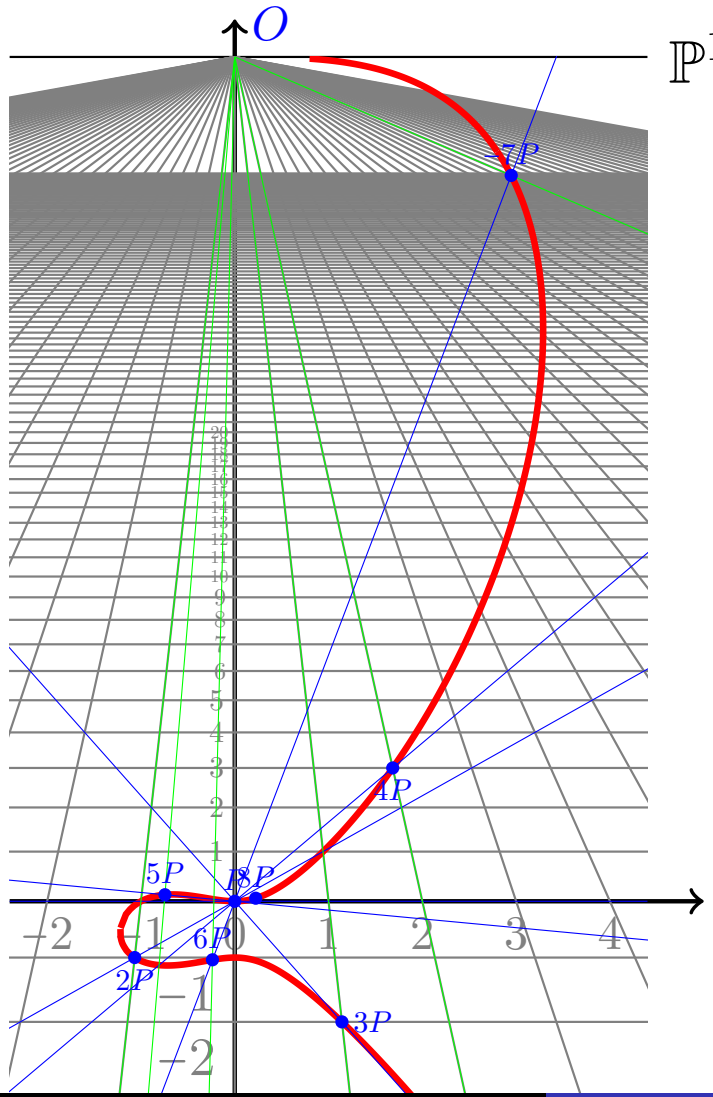
$(2,3)$

$\left(-\frac{3}{4},\frac{1}{8}\right)$

$\left(-\frac{2}{9},-\frac{28}{27}\right)$

$(21,98)$

# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.




$\mathbb{P}^1$

$(0,0)$

$(-1,-1)$

$(1,-2)$

$(2,3)$

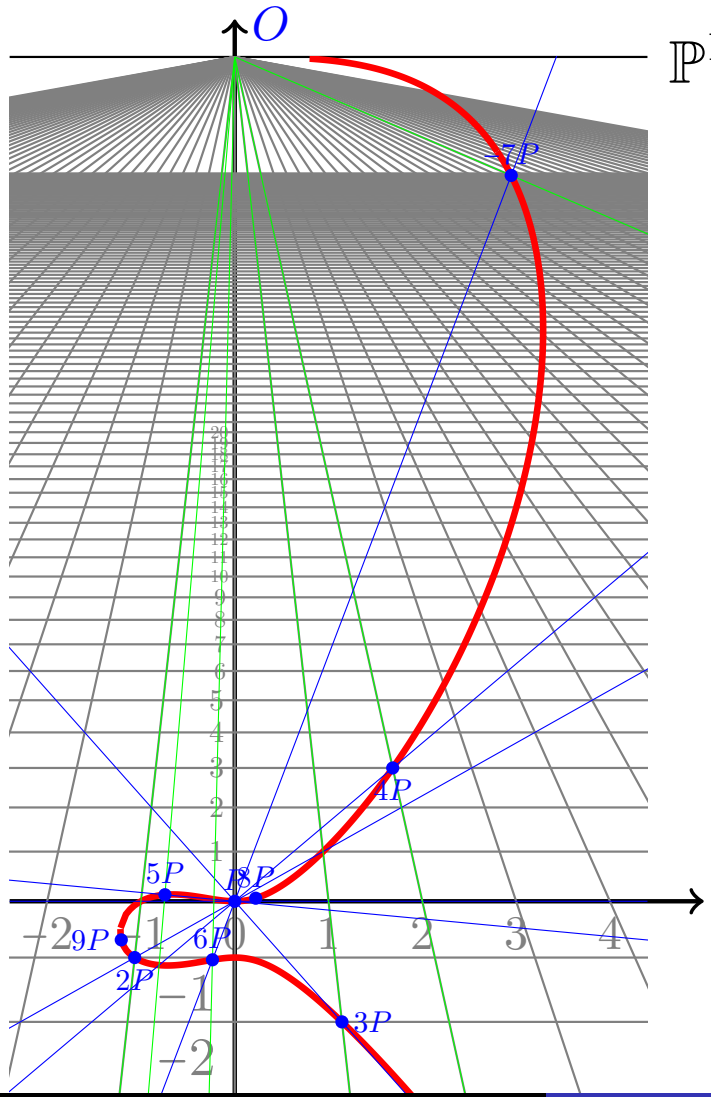
$\left(-\frac{3}{4},\frac{1}{8}\right)$

$\left(-\frac{2}{9},-\frac{28}{27}\right)$

$(21,98)$

$\left(\frac{11}{49},\frac{20}{343}\right)$

# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.




$\mathbb{P}^1$

$(0,0)$

$(-1,-1)$

$(1,-2)$

$(2,3)$

$\left(-\frac{3}{4},\frac{1}{8}\right)$

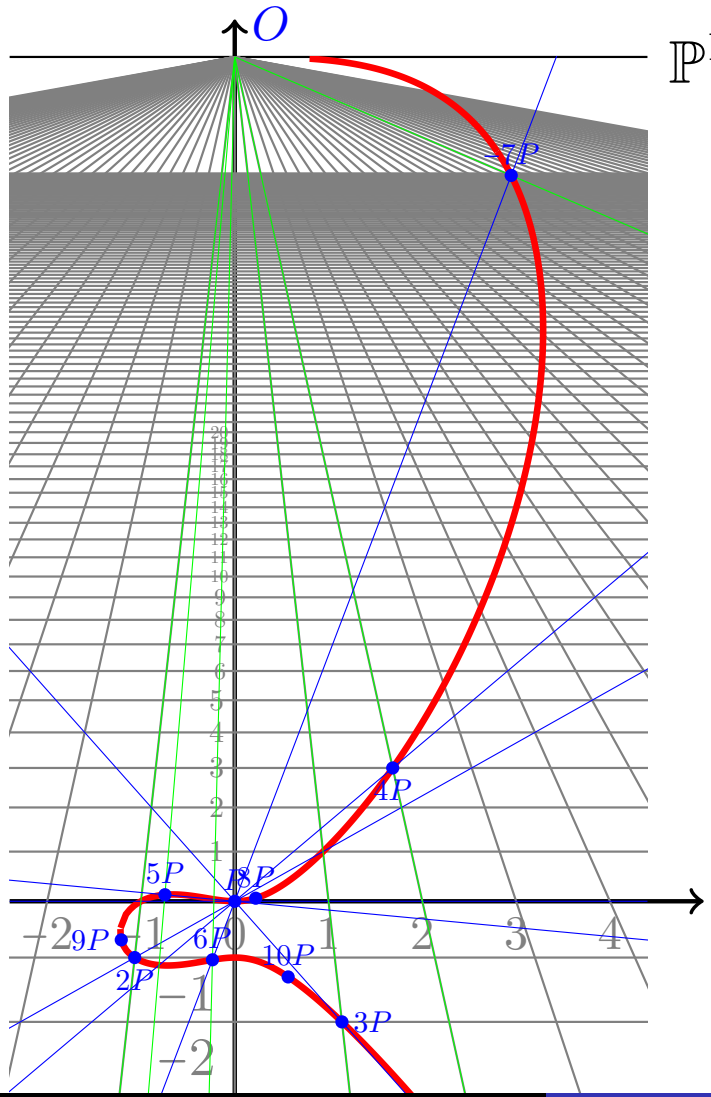
$\left(-\frac{2}{9},-\frac{28}{27}\right)$

$(21,98)$

$\left(\frac{11}{49},\frac{20}{343}\right)$

$\left(-\frac{140}{121},-\frac{931}{1331}\right)$

# Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.




$\mathbb{P}^1$

$(0,0)$

$(-1,-1)$

$(1,-2)$

$(2,3)$

$\left(-\frac{3}{4},\frac{1}{8}\right)$

$\left(-\frac{2}{9},-\frac{28}{27}\right)$

$(21,98)$

$\left(\frac{11}{49},\frac{20}{343}\right)$

$\left(-\frac{140}{121},-\frac{931}{1331}\right)$

$\left(\frac{209}{400},-\frac{10527}{8000}\right)$

Soit $E/K$ une courbe elliptique. Pour $P(x, y) \in E(\bar{K})$, on pose $h(P) = h(x)$, et $h(O) = 0$.

Soit $E/K$ une courbe elliptique. Pour $P(x,y) \in E(\bar{K})$, on pose $h(P) = h(x)$, et $h(O) = 0$.

On a :

- $h(P+Q) + h(P-Q) = 2(h(P) + h(Q)) + O(1)$ ;

Soit $E/K$ une courbe elliptique. Pour $P(x,y) \in E(\bar{K})$, on pose $h(P) = h(x)$, et $h(O) = 0$.

On a :

- $h(P+Q) + h(P-Q) = 2(h(P) + h(Q)) + O(1)$ ;
- $h(\phi(P)) = \deg(\phi)h(P) + O(1)$ pour $\phi \in \mathrm{End}(E)$ ;
- $h(nP) = n^2 \cdot h(P) + O(1)$ pour $n \in \mathbb{Z}$ ;

Soit $E/K$ une courbe elliptique. Pour $P(x,y) \in E(\bar{K})$, on pose $h(P) = h(x)$, et $h(O) = 0$.

On a :

- $h(P+Q) + h(P-Q) = 2(h(P) + h(Q)) + O(1)$ ;
- $h(\phi(P)) = \deg(\phi)h(P) + O(1)$ pour $\phi \in \mathrm{End}(E)$ ;
- $h(nP) = n^2 \cdot h(P) + O(1)$ pour $n \in \mathbb{Z}$ ;
- pour tous $c, d > 0$, l'ensemble $\{P \in E(\bar{K}) \mid h(P) \leqslant d, [K(P) : K] \leqslant c\}$ est fini ;

Soit $E/K$ une courbe elliptique. Pour $P(x,y) \in E(\bar{K})$, on pose $h(P) = h(x)$, et $h(O) = 0$. On définit alors la hauteur canonique comme suit :

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}.$$

On a :

- $h(P+Q) + h(P-Q) = 2(h(P) + h(Q)) + O(1)$ ;
- $h(\phi(P)) = \deg(\phi)h(P) + O(1)$ pour $\phi \in \mathrm{End}(E)$ ;
- $h(nP) = n^2 \cdot h(P) + O(1)$ pour $n \in \mathbb{Z}$ ;
- pour tous $c, d > 0$, l'ensemble $\{P \in E(\bar{K}) \mid h(P) \leqslant d, [K(P) : K] \leqslant c\}$ est fini ;

Soit $E/K$ une courbe elliptique. Pour $P(x,y) \in E(\bar{K})$, on pose $h(P) = h(x)$, et $h(O) = 0$. On définit alors la hauteur canonique comme suit :

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}.$$

On a :

- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2(\hat{h}(P) + \hat{h}(Q))$ ;
- $\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P)$ pour $\phi \in \mathrm{End}(E)$ ;
- $\hat{h}(nP) = n^2 \cdot \hat{h}(P)$ pour $n \in \mathbb{Z}$ ;
- pour tous $c, d > 0$, l'ensemble $\{P \in E(\bar{K}) \mid \hat{h}(P) \leqslant d, [K(P) : K] \leqslant c\}$ est fini ;

Soit $E/K$ une courbe elliptique. Pour $P(x,y) \in E(\bar{K})$, on pose $h(P) = h(x)$, et $h(O) = 0$. On définit alors la hauteur canonique comme suit :

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}.$$

On a :

- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2(\hat{h}(P) + \hat{h}(Q))$ ;
- $\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P)$ pour $\phi \in \mathrm{End}(E)$ ;
- $\hat{h}(nP) = n^2 \cdot \hat{h}(P)$ pour $n \in \mathbb{Z}$ ;
- pour tous $c, d > 0$, l'ensemble $\{P \in E(\bar{K}) \mid \hat{h}(P) \leqslant d, [K(P) : K] \leqslant c\}$ est fini ;
- $\hat{h}(P) = 0$ si, et seulement si $P$ est de torsion.

# Minoration de la hauteur

Soit $E/K$ une courbe elliptique sur un corps de nombres.

## Conjecture de Lang

On a, pour tout point $P \in E(K)$ d'ordre infini :

$$\hat{h}(P) \geqslant c_K \max(\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))), h(j_E)).$$

# Minoration de la hauteur

Soit $E/K$ une courbe elliptique sur un corps de nombres.

## Conjecture de Lang

On a, pour tout point $P \in E(K)$ d'ordre infini :

$$\hat{h}(P) \geqslant c_K \max(\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))), h(j_E)).$$

## Conjecture de Lehmer

On a, pour tout point $P \in E(\bar{K})$ d'ordre infini :

$$\hat{h}(P) \geqslant \frac{c_{E,K}}{[K(P) : K]}.$$

# Minoration de la hauteur

## Théorème (Laurent (1983))

Soit $E/K$ une courbe elliptique à multiplications complexes. Pour tout point $P \in E(\bar{K})$ d'ordre infini, où $D = [K(P) : K]$, on a :

$$\hat{h}(P) \geqslant \frac{c_{E,K}}{D} \left( \frac{\ln(\ln(4D))}{\ln(4D)} \right)^3 .$$

# Minoration de la hauteur

## Théorème (Laurent (1983), W. (2015))

Soit $E/K$ une courbe elliptique à multiplications complexes. Pour tout point $P \in E(\bar{K})$ d'ordre infini, où $D = [K(P) : K]$, on a :

$$\hat{h}(P) \geqslant \frac{c_{E,K}}{D} \left( \frac{\ln(\ln(4D))}{\ln(4D)} \right)^3, \text{ où}$$

$$\begin{cases} c_{K,E} & \gg & (\ln(|d_{\hat{K}}|))^{-6,5} (h(j_E))^{-9} \text{ si HRG} \\ \ln(c_{K,E}) & \gg & (d_{\hat{K}} h(j_E))^{-1}, \end{cases}$$

où $\hat{K}$ est la clôture galoisienne de $K/\mathbb{Q}$.

# Minoration de la hauteur

## Théorème (Laurent (1983), W. (2015))

Soit $E/K$ une courbe elliptique à multiplications complexes. Pour tout point $P \in E(\bar{K})$ d'ordre infini, où $D = [K(P) : K]$, on a :

$$\hat{h}(P) \geqslant \frac{c_{E,K}}{D} \left( \frac{\ln(\ln(4D))}{\ln(4D)} \right)^3, \text{ où}$$

$$c_{K,E}^{-1} \leqslant 10^{10} \cdot f\sqrt{n_{\hat{K}}}(59,07 + 276,48 \ln(|d_{\hat{K}}|)$$
$$+192 n_{\hat{K}} (87,4 + 2,9 \ln(6N_E) + 0,5 \ln(-4d)))^6 \cdot (3,89 + 0,13 h(j_E))^3$$

si HRG ($\mathrm{End}(E) = \mathbb{Z} + f\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$).

# Ingrédients de la démonstration

Soit $P$ un point d'ordre infini sur une courbe elliptique à multiplications complexes.

# Ingrédients de la démonstration

Soit $P$ un point d'ordre infini sur une courbe elliptique à multiplications complexes. Les deux principaux ingrédients sont :

**Théorème de Faltings-Hriljac**

L'accouplement bilinéaire $(\cdot|\cdot)$ sur $E/K$ s'exprime comme somme de « termes locaux », associés à chaque place de $K$.

# Ingrédients de la démonstration

Soit $P$ un point d'ordre infini sur une courbe elliptique à multiplications complexes. Les deux principaux ingrédients sont :

## Théorème de Faltings-Hriljac

## Théorème de Deuring

Soit $E/K$ une courbe elliptique à multiplications complexes par $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Supposons que $K$ contient $\mathbb{Q}(\sqrt{d})$. Pour presque tout idéal premier $\mathfrak{p}$ de $K$, $(x, y) \bmod \mathfrak{p} \mapsto (x^q, y^q) \bmod \mathfrak{p}$ (où $q = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$) se relève en un endomorphisme $\mathrm{F}_\mathfrak{p} : E \to E$.

# Ingrédients de la démonstration

Soit $P$ un point d'ordre infini sur une courbe elliptique à multiplications complexes. Les deux principaux ingrédients sont :

## Théorème de Faltings-Hriljac

## Théorème de Deuring

On compare alors $\hat{h}(P)$ à des intersections entre $\mathrm{F}_{\mathfrak{p}}(P)$ et $P$ (entre autres). Ces calculs font intervenir des sommes indexées par des nombres premiers bien choisis.

Soit $L/K$ une extension galoisienne de corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ qui ne se ramifie pas dans $L$, et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de $G$ qui relève $\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \to & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \end{array}$, et $\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right); \mathfrak{P}|\mathfrak{p}\right\}$.

Soit $L/K$ une extension galoisienne de corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ qui ne se ramifie pas dans $L$, et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de $G$ qui relève $\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \to & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \end{array}$, et $\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right); \mathfrak{P}|\mathfrak{p}\right\}$. Si $C$ est une classe de conjugaison, soit $\pi_C(x)$ la fonction de décompte des idéaux premiers de norme inférieure à $x$ tels que $\left(\frac{L/K}{\mathfrak{p}}\right) = C$.

Soit $L/K$ une extension galoisienne de corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ qui ne se ramifie pas dans $L$, et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de $G$ qui relève $\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \to & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \end{array}$, et $\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right); \mathfrak{P}|\mathfrak{p}\right\}$. Si $C$ est une classe de conjugaison, soit $\pi_C(x)$ la fonction de décompte des idéaux premiers de norme inférieure à $x$ tels que $\left(\frac{L/K}{\mathfrak{p}}\right) = C$. Alors

$$\pi_C(x) \sim \frac{|C|}{|G|}\mathrm{Li}(x) := \frac{|C|}{|G|}\int_2^x \frac{\mathrm{d}t}{\ln(t)} \sim \frac{|C|}{|G|}\frac{x}{\ln(x)}.$$

Soit $L/K$ une extension galoisienne de corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ qui ne se ramifie pas dans $L$, et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de $G$ qui relève $\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \to & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \end{array}$, et $\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right); \mathfrak{P}|\mathfrak{p}\right\}$. Si $C$ est une classe de conjugaison, soit $\pi_C(x)$ la fonction de décompte des idéaux premiers de norme inférieure à $x$ tels que $\left(\frac{L/K}{\mathfrak{p}}\right) = C$.

**Théorème de Chebotarev explicite avec HRG (W. (2014))**

Supposons que HRG est vraie pour $\zeta_L$. Alors, pour tout $x \geqslant 2$,

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\left[1,2\ln(d_L) + 0,6\ln(x)n_L + \mathrm{reste}\right].$$

Soit $L/K$ une extension galoisienne de corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ qui ne se ramifie pas dans $L$, et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de $G$ qui relève $\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \to & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \end{array}$, et $\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right); \mathfrak{P}|\mathfrak{p}\right\}$. Si $C$ est une classe de conjugaison, soit $\pi_C(x)$ la fonction de décompte des idéaux premiers de norme inférieure à $x$ tels que $\left(\frac{L/K}{\mathfrak{p}}\right) = C$.

## Théorème de Chebotarev explicite avec HRG (W. (2014))

Supposons que HRG est vraie pour $\zeta_L$. Alors, pour tout $x \geqslant 2$,

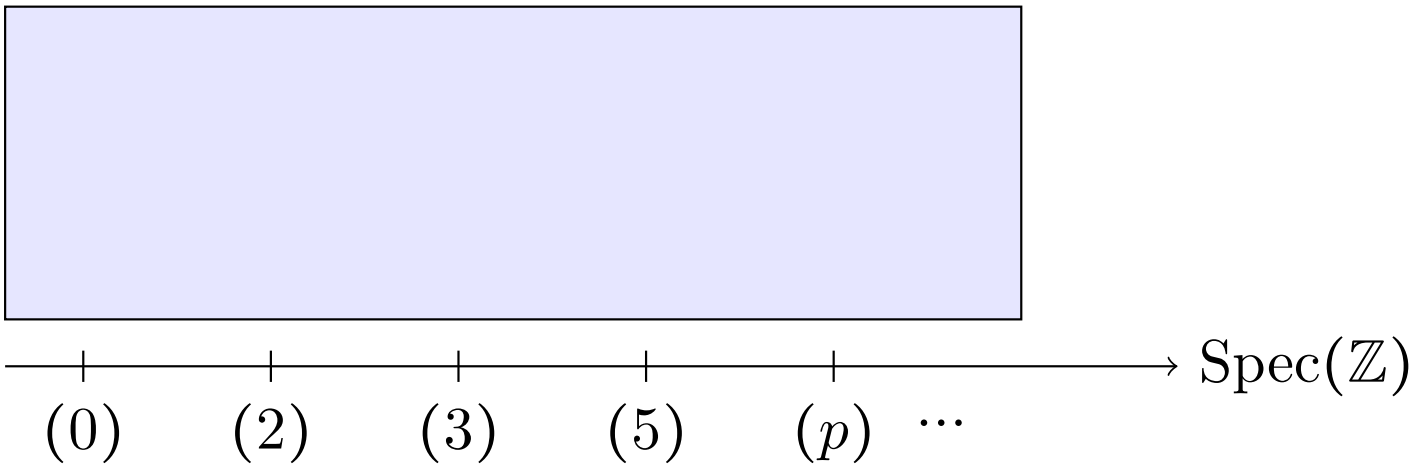
$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\Big[\left(\frac{55}{48} + \frac{177}{\ln(x)}\right)\ln(d_L) + \left(\frac{605}{1152}\ln(x) + 13 + \frac{866}{\ln(x)}\right)n_L + 680\Big].$$

# Plan

Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

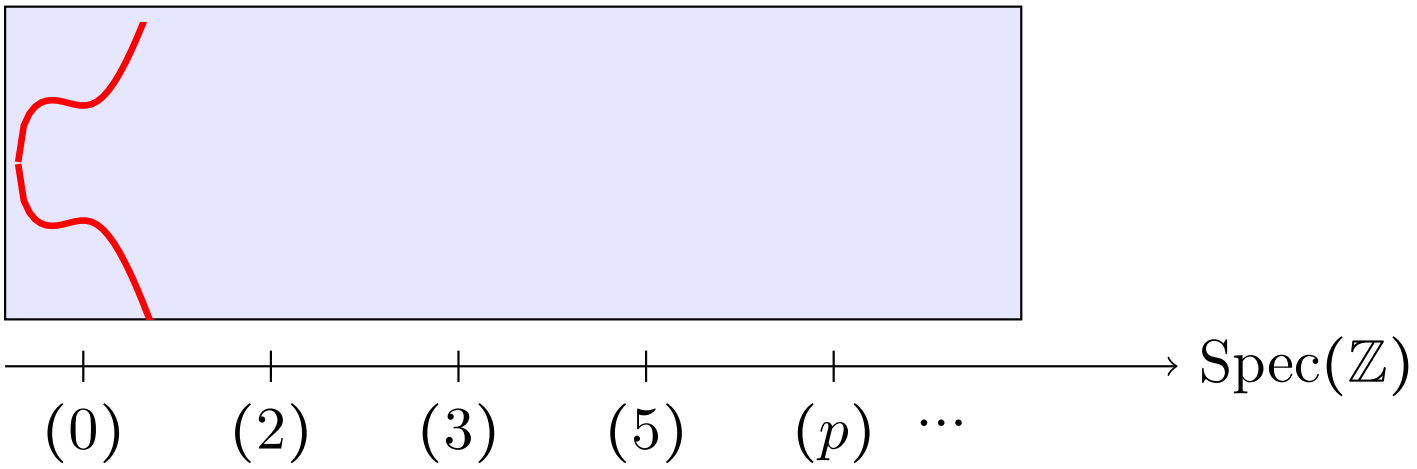
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



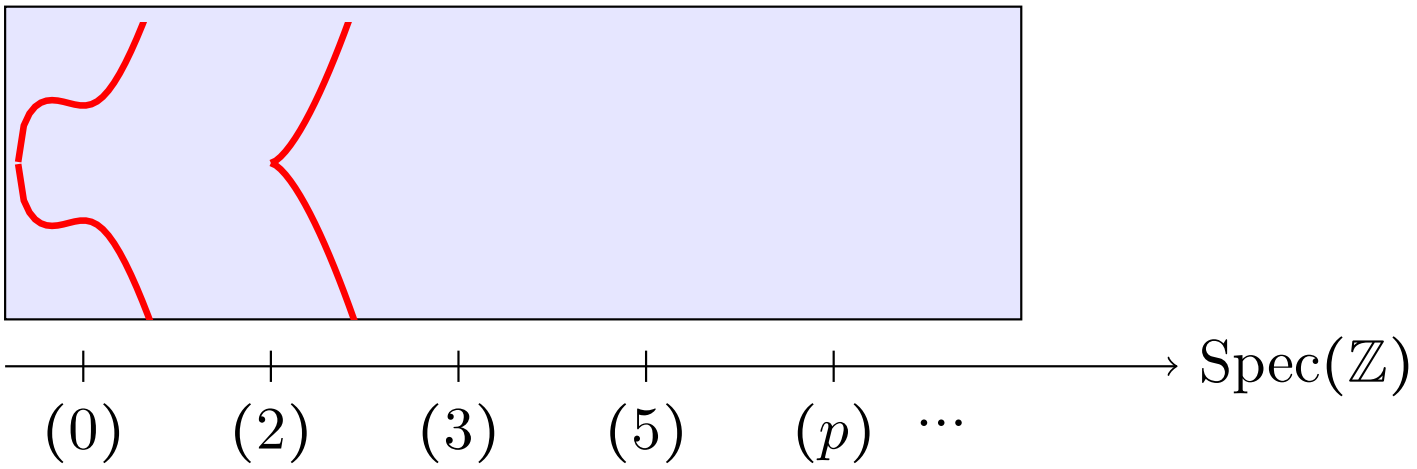
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



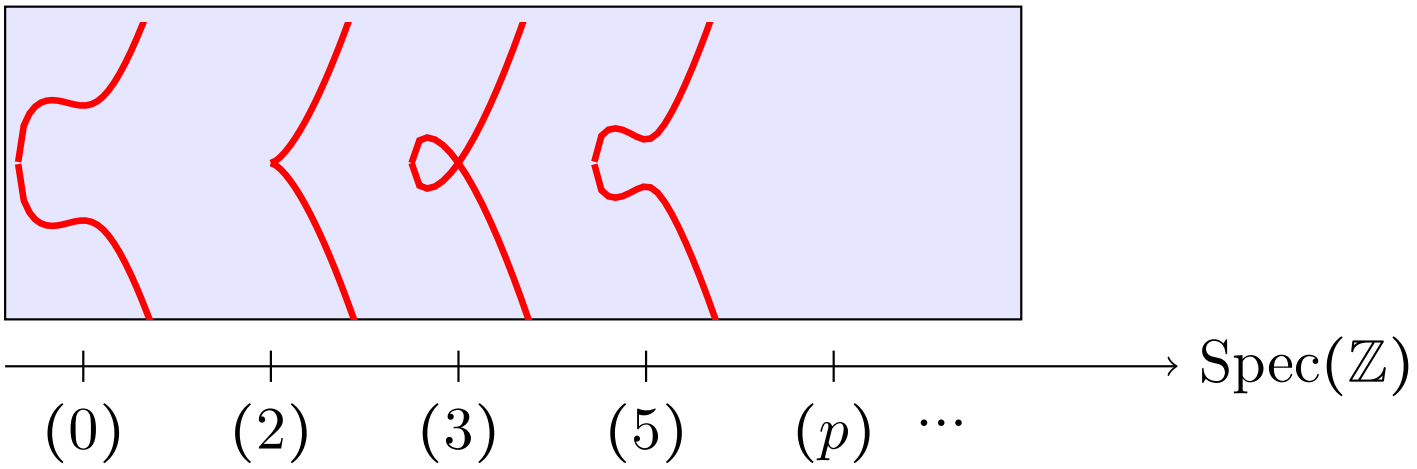
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



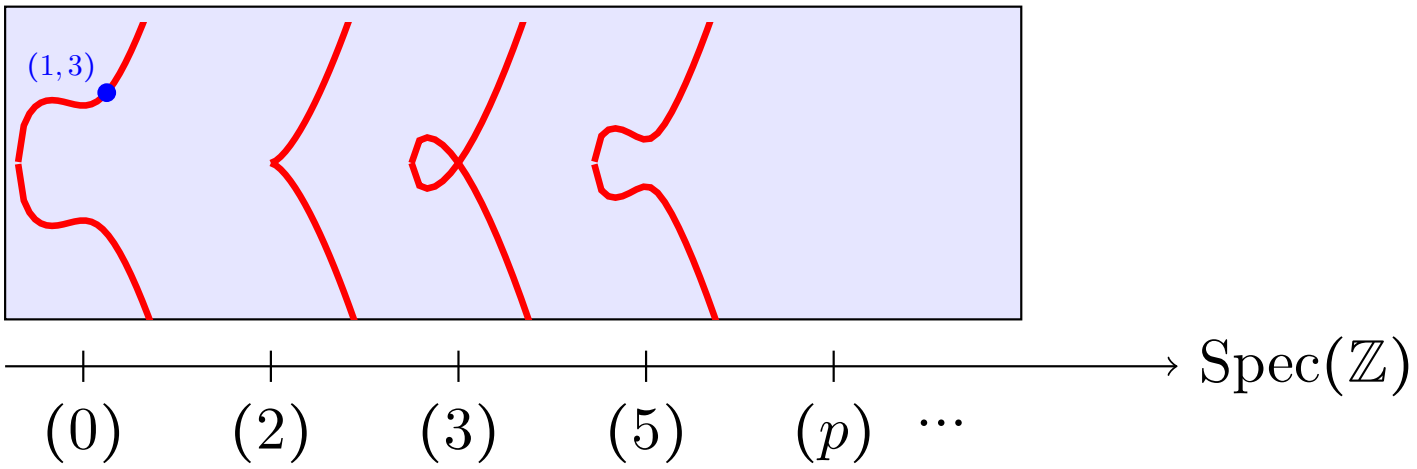
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



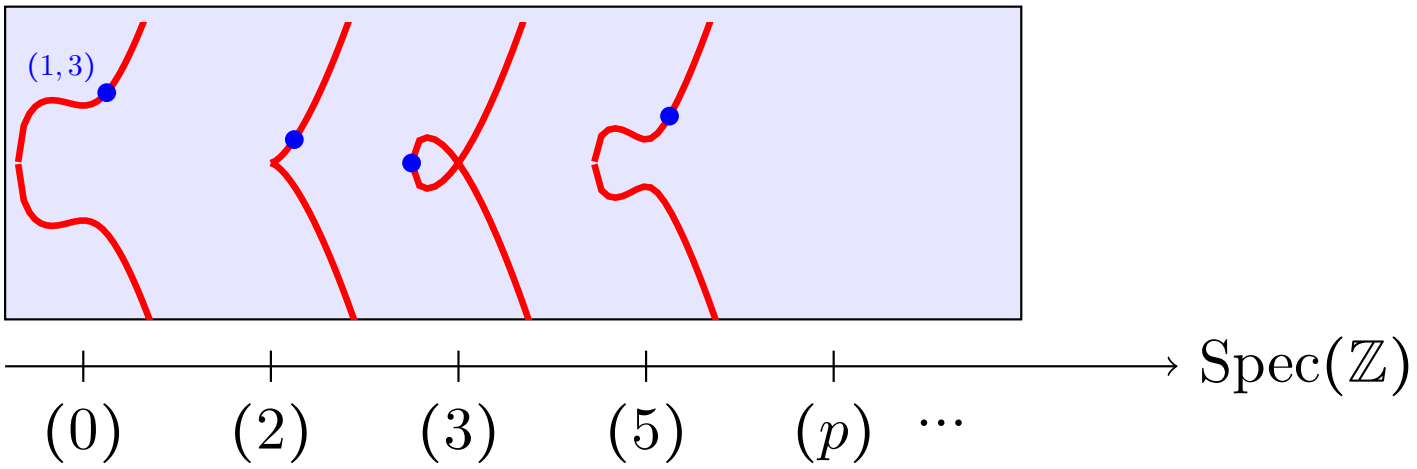
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



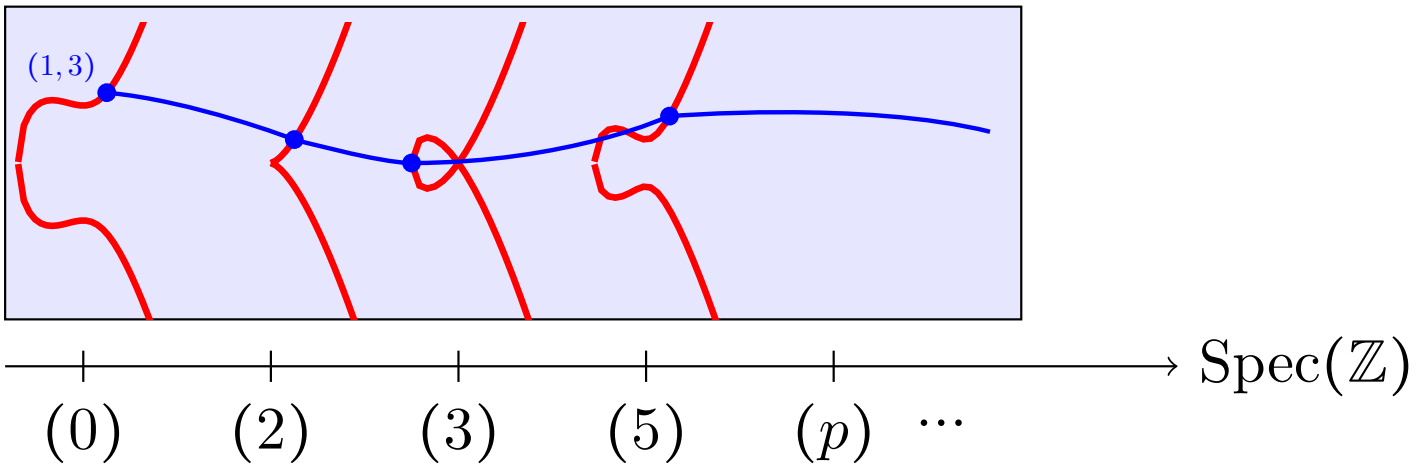
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



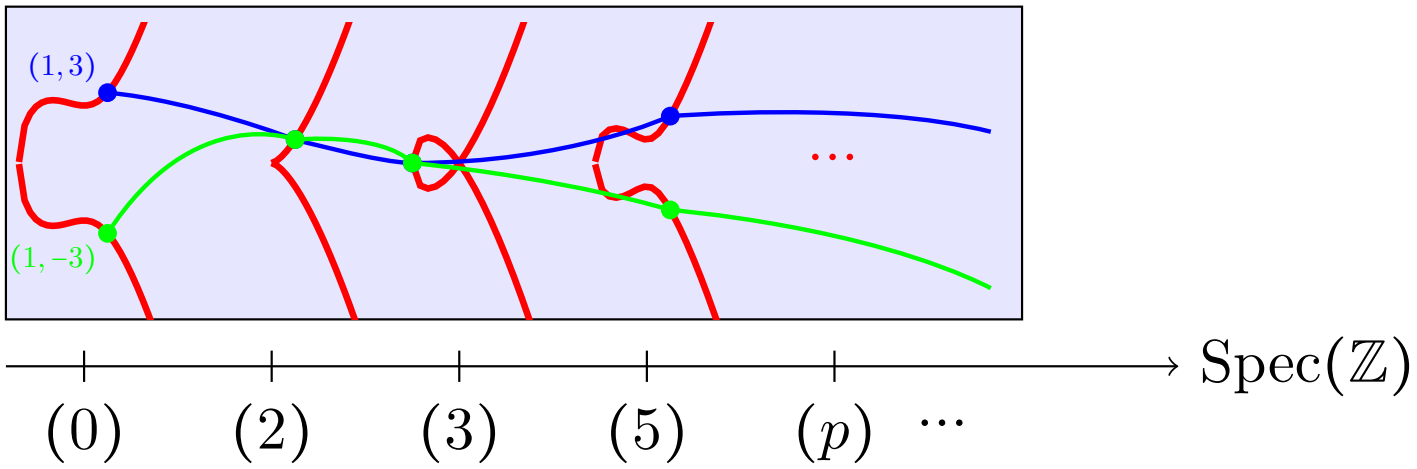
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

## Intersection locale

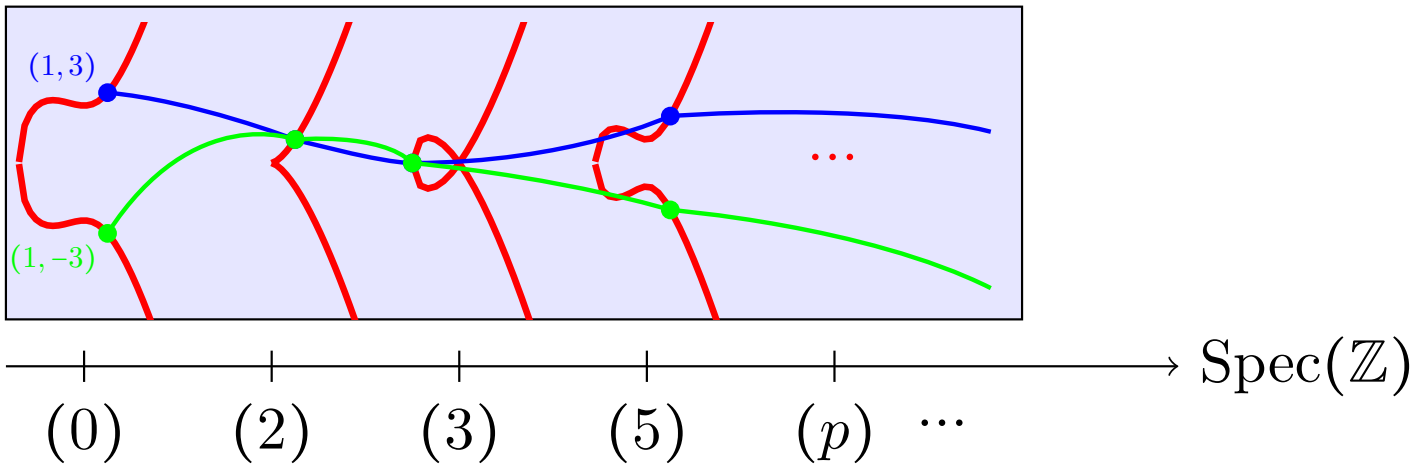
Soient $\mathcal{D}_1$ et $\mathcal{D}_2$ deux diviseurs distincts et irréductibles sur $\mathcal{X}/\mathcal{O}_K$, soient $\mathfrak{p}$ un idéal premier et $x \in \mathcal{X}_\mathfrak{p}$. On pose :

- $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_x = (\text{mult. d'intersection en } x) \ln(|k(x)|)$ ;
- $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_\mathfrak{p} = \sum_{x \in \mathcal{X}_\mathfrak{p}} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_x$.

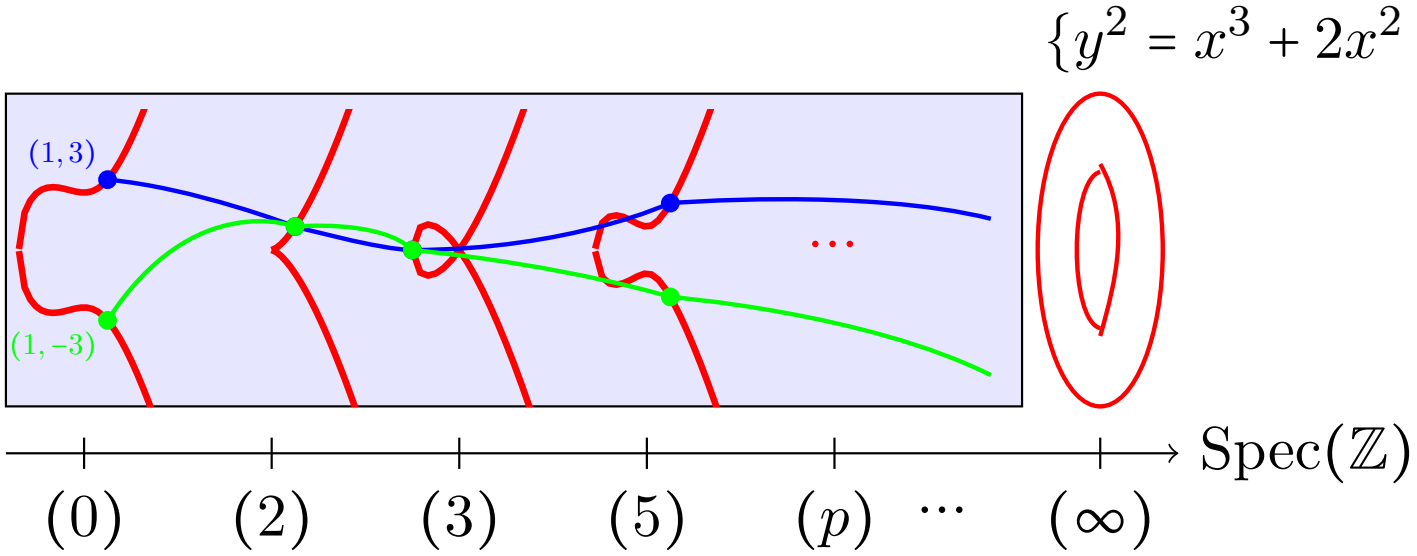
On pose alors $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle = \sum_{\mathfrak{p} \subseteq K} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_\mathfrak{p}$.

Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

$$\{y^2 = x^3 + 2x^2 + 6\}/\mathbb{Z}$$



Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.



# Intersection aux places infinies

Pour toute place $v$, la restriction de l'intersection locale à $\mathrm{Div}^0(\mathcal{X}/\mathcal{O}_K) \times \mathrm{Div}^0(\mathcal{X}/\mathcal{O}_K)$ est bilinéaire symétrique, continue (pour la topologie $v$-adique), localement bornée et vérifie, pour $\mathcal{D}_1$ l'adhérence d'un diviseur principal $\mathrm{div}(f) \in \mathrm{Div}(X)$, et $\mathcal{D}_2$ un diviseur de Weil de degré nul dont le support est génériquement disjoint de celui de $\mathcal{D}_1$ : $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v = -n_v \ln(|f(\mathcal{D}_{2|K})|_v)$.

# Intersection aux places infinies

Pour toute place $v$, la restriction de l'intersection locale à $\mathrm{Div}^0(\mathcal{X}/\mathcal{O}_K) \times \mathrm{Div}^0(\mathcal{X}/\mathcal{O}_K)$ est bilinéaire symétrique, continue (pour la topologie $v$-adique), localement bornée et vérifie, pour $\mathcal{D}_1$ l'adhérence d'un diviseur principal $\mathrm{div}(f) \in \mathrm{Div}(X)$, et $\mathcal{D}_2$ un diviseur de Weil de degré nul dont le support est génériquement disjoint de celui de $\mathcal{D}_1$ : $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v = -n_v \ln(|f(\mathcal{D}_{2|K})|_v)$.

- si $\mathcal{D}_1$ un diviseur horizontal et $\mathcal{D}_2$ une section, $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_\sigma = g_\sigma(D_1^\sigma, D_2^\sigma) = \lambda_\sigma(D_1^\sigma - D_2^\sigma)$ où $g_\sigma$ est la fonction de Green-Arakelov sur la surface de Riemann $(\mathcal{X} \otimes_\sigma \mathbb{C})(\mathbb{C})$ ;
- si $\mathcal{D}_1$ ou $\mathcal{D}_2$ est un diviseur de Weil vertical, $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v = 0$ ;
- si $\mathcal{D}_1$ un diviseur horizontal et $F_\sigma$ une fibre à l'infini, $\langle \mathcal{D}_1, F_\sigma \rangle_\sigma = \deg(\mathcal{D}_{1|K})$, et $\langle \mathcal{D}_1, F_\sigma \rangle_v = 0$ sinon.

On pose alors $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle = \sum_{\mathfrak{p} \subseteq K} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_{\mathfrak{p}} + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_{\sigma}$.

On pose alors $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle = \sum_{\mathfrak{p} \subseteq K} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_{\mathfrak{p}} + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_{\sigma}$. Cet accouplement bilinéaire se prolonge, et définit un accouplement d'intersection $\langle \cdot, \cdot \rangle : \widehat{\mathrm{Cl}(\mathcal{X})} \times \widehat{\mathrm{Cl}(\mathcal{X})} \to \mathbb{R}$.

On pose alors $\langle \mathcal{D}_1, \mathcal{D}_2 \rangle = \sum_{\mathfrak{p} \subseteq K} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_{\mathfrak{p}} + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_{\sigma}$. Cet accouplement bilinéaire se prolonge, et définit un accouplement d'intersection $\langle \cdot, \cdot \rangle : \widehat{\mathrm{Cl}(\mathcal{X})} \times \widehat{\mathrm{Cl}(\mathcal{X})} \to \mathbb{R}$.

## Cas des auto-intersections : formule d'adjonction

Soit $\mathcal{X} \to B$ une surface arithmétique et $\mathcal{Q} : \mathrm{Spec}(\mathcal{O}_L) \to \mathcal{X}$ un diviseur horizontal. Notant $\mathrm{K}_{\mathcal{X}/B}$ le diviseur canonique (d'Arakelov) de $\mathcal{X}/B$, on a :

$$\langle \mathcal{Q}, \mathrm{K}_{\mathcal{X}/B} \rangle_K + \langle \mathcal{Q}, \mathcal{Q} \rangle_K = \mathrm{d}_{\mathcal{Q}/L} - \sum_{v \in M_K^{\infty}} n_v \sum_{\substack{\sigma, \tau : L \hookrightarrow \mathbb{C} \\ \sigma, \tau | v \\ \sigma \neq \tau}} g_v(Q^{\sigma}, Q^{\tau}),$$

où $\mathrm{d}_{\mathcal{Q}/L} \geqslant 0$.

## Théorème de Faltings-Hriljac

Soit $E$ une courbe elliptique définie sur un corps de nombres $K$, avec bonne réduction partout, et $\mathcal{E} \to B$ son modèle minimal régulier. Alors, pour tous diviseurs $D_1$ et $D_2 \in \mathrm{Div}(E)$ de degré nul, à support dans des points de $E(L)$ et dont on note $\mathcal{D}_1$ et $\mathcal{D}_2$ l'adhérence dans $\mathcal{E}$, on a

$$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_K = -2[L:\mathbb{Q}](D_1|D_2).$$

## Théorème de Faltings-Hriljac

Soit $E$ une courbe elliptique définie sur un corps de nombres $K$, avec bonne réduction partout, et $\mathcal{E} \to B$ son modèle minimal régulier. Alors, pour tous diviseurs $D_1$ et $D_2 \in \mathrm{Div}(E)$ de degré nul, à support dans des points de $E(L)$ et dont on note $\mathcal{D}_1$ et $\mathcal{D}_2$ l'adhérence dans $\mathcal{E}$, on a

$$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_K = -2[L:\mathbb{Q}](D_1|D_2).$$

## Corollaire

Sous les mêmes hypothèses, pour tout point $Q \in E(\bar{K})$ d'adhérence $\mathcal{Q}$ dans $\mathcal{E}$, on a :

$$\hat{h}(Q) = \frac{\langle \mathcal{Q}, \mathcal{O} \rangle_K}{[K(Q):\mathbb{Q}]}.$$

# Démonstration du résultat principal

Supposons $K \supseteq \mathrm{End}(E) \otimes \mathbb{Q}$, $K/\mathbb{Q}$ galoisienne et $E/K$ de bonne réduction partout.

# Démonstration du résultat principal

Supposons $K \supseteq \mathrm{End}(E) \otimes \mathbb{Q}$, $K/\mathbb{Q}$ galoisienne et $E/K$ de bonne réduction partout. Soit $P$ un point d'ordre infini, $L = K(P)$, $D = [L : K]$.

# Démonstration du résultat principal

Supposons $K \supseteq \mathrm{End}(E) \otimes \mathbb{Q}$, $K/\mathbb{Q}$ galoisienne et $E/K$ de bonne réduction partout. Soit $P$ un point d'ordre infini, $L = K(P)$, $D = [L : K]$. Soit $s \geqslant 3$, et soit $\Pi_s = \{p_1, \ldots, p_r\}$ l'ensemble des nombres premiers qui se décomposent complètement dans $K$.

# Démonstration du résultat principal

Supposons $K \supseteq \mathrm{End}(E) \otimes \mathbb{Q}$, $K/\mathbb{Q}$ galoisienne et $E/K$ de bonne réduction partout. Soit $P$ un point d'ordre infini, $L = K(P)$, $D = [L : K]$. Soit $s \geqslant 3$, et soit $\Pi_s = \{p_1, \ldots, p_r\}$ l'ensemble des nombres premiers qui se décomposent complètement dans $K$. Pour tout $p_i \in \Pi_s$, on fixe $\mathfrak{p}_i | p_i$, et soit $\mathrm{F}_{p_i}$ le relèvement de Frobenius associé à $\mathfrak{p}_i$. On pose $p_0 = 1$ et $\mathrm{F}_1 = \mathrm{Id}$.

# Démonstration du résultat principal

Supposons $K \supseteq \mathrm{End}(E) \otimes \mathbb{Q}$, $K/\mathbb{Q}$ galoisienne et $E/K$ de bonne réduction partout. Soit $P$ un point d'ordre infini, $L = K(P)$, $D = [L : K]$. Soit $s \geqslant 3$, et soit $\Pi_s = \{p_1, \ldots, p_r\}$ l'ensemble des nombres premiers qui se décomposent complètement dans $K$. Pour tout $p_i \in \Pi_s$, on fixe $\mathfrak{p}_i | p_i$, et soit $\mathrm{F}_{p_i}$ le relèvement de Frobenius associé à $\mathfrak{p}_i$. On pose $p_0 = 1$ et $\mathrm{F}_1 = \mathrm{Id}$.

Nous pouvons supposer que pour tous $p, p' \in \Pi_s$ et $\sigma, \tau \in \mathrm{Hom}_K(L, \mathbb{C})$ tels que $(\sigma, p) \neq (\tau, p')$ et donc $\mathrm{F}_p(P)^\sigma \neq \mathrm{F}_{p'}(P)^\tau$ (en particulier, on a $K(\mathrm{F}_p(P)) = L$).

# Contributions aux places finies

On a, en conservant les notations précédentes,

$$\sum_{\substack{0\leqslant i,j\leqslant r\\ i\neq j}} \sum_{v\in M_K^0} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v \geqslant [L:\mathbb{Q}] m_0 \sum_{i=1}^{r} m_i \ln(p_i).$$

# Contributions aux places finies

On a, en conservant les notations précédentes,

$$\sum_{\substack{0\leqslant i,j\leqslant r\\ i\neq j}} \sum_{v\in M_K^0} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v \geqslant [L:\mathbb{Q}] m_0 \sum_{i=1}^{r} m_i \ln(p_i).$$

Esquisse : si $\mathfrak{p}$ divise $p_i$, on montre que $\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathcal{P}\rangle_{\mathfrak{p}} > 0$.

# Contributions aux places finies

On a, en conservant les notations précédentes,

$$\sum_{\substack{0\leqslant i,j\leqslant r\\ i\neq j}} \sum_{v\in M_K^0} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v \geqslant [L:\mathbb{Q}] m_0 \sum_{i=1}^{r} m_i \ln(p_i).$$

Esquisse : si $\mathfrak{p}$ divise $p_i$, on montre que $\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathcal{P}\rangle_{\mathfrak{p}} > 0$.

- Si $P \equiv O \mod \mathfrak{p}$ : rien à dire ;

# Contributions aux places finies

On a, en conservant les notations précédentes,

$$\sum_{\substack{0\leqslant i,j\leqslant r\\ i\neq j}} \sum_{v\in M_K^0} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v \geqslant [L:\mathbb{Q}] m_0 \sum_{i=1}^{r} m_i \ln(p_i).$$

Esquisse : si $\mathfrak{p}$ divise $p_i$, on montre que $\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathcal{P}\rangle_{\mathfrak{p}} > 0$.

- Si $P \equiv O \mod \mathfrak{p}$ : rien à dire ;
- Sinon, on montre que pour tout $\sigma : L \hookrightarrow \bar{L}$ et pour tout $x \in \mathcal{O}_{L,\mathfrak{P}}$ (où $\mathfrak{P}|\mathfrak{p}$), l'idéal premier $\mathfrak{p}$ divise $\prod_{\tau:L\hookrightarrow\bar{L}} ((x^p)^\sigma - x^\tau)$.

# Contributions aux places finies

On a, en conservant les notations précédentes,

$$\sum_{\substack{0\leqslant i,j\leqslant r\\ i\neq j}} \sum_{v\in M_K^0} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v \geqslant [L:\mathbb{Q}] m_0 \sum_{i=1}^{r} m_i \ln(p_i).$$

Esquisse : si $\mathfrak{p}$ divise $p_i$, on montre que $\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathcal{P}\rangle_{\mathfrak{p}} > 0$.

- Si $P \equiv O \mod \mathfrak{p}$ : rien à dire ;
- Sinon, on montre que pour tout $\sigma : L \hookrightarrow \bar{L}$ et pour tout $x \in \mathcal{O}_{L,\mathfrak{P}}$ (où $\mathfrak{P}|\mathfrak{p}$), l'idéal premier $\mathfrak{p}$ divise $\prod_{\tau:L\hookrightarrow\bar{L}} ((x^p)^\sigma - x^\tau)$.

Sinon, on utilise $\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_{\mathfrak{p}} \geqslant 0$.

## Lemme d'Elkies

Soit $v$ une place archimédienne, et soient $P_1, \ldots, P_N$ des points distincts de $E(K)$. Alors,

$$\sum_{1 \leqslant i \neq j \leqslant N} \langle P_i, P_j \rangle_v \geqslant -N \cdot \left( \frac{1}{2} \ln(N) + \frac{1}{12} J_v + \frac{16}{5} \right),$$

où l'on note $J_v = \max(\ln(|j_E|_v), 0)$.

## Lemme d'Elkies

Soit $v$ une place archimédienne, et soient $P_1, \ldots, P_N$ des points distincts de $E(K)$. Alors,

$$\sum_{1 \leqslant i \neq j \leqslant N} \langle P_i, P_j \rangle_v \geqslant -N \cdot \left( \frac{1}{2} \ln(N) + \frac{1}{12} J_v + \frac{16}{5} \right),$$

où l'on note $J_v = \max(\ln(|j_E|_v), 0)$.

Esquisse : Imaginons que $\langle P_i, P_i \rangle_v$ soit bien défini. Alors :

$$\sum_{1 \leqslant i \neq j \leqslant N} \langle P_i, P_j \rangle_v = N^2 \iint_{E(\mathbb{C})^2} \lambda_v(P - Q) \mathrm{d}\mu(P) \mathrm{d}\mu(Q) - \frac{1}{N^2} \sum_{i=1}^{N} \langle P_i, P_i \rangle_v$$

## Lemme d'Elkies

Soit $v$ une place archimédienne, et soient $P_1, \ldots, P_N$ des points distincts de $E(K)$. Alors,

$$\sum_{1 \leqslant i \neq j \leqslant N} \langle P_i, P_j \rangle_v \geqslant -N \cdot \left( \frac{1}{2} \ln(N) + \frac{1}{12} J_v + \frac{16}{5} \right),$$

où l'on note $J_v = \max(\ln(|j_E|_v), 0)$.

Esquisse : Imaginons que $\langle P_i, P_i \rangle_v$ soit bien défini. Alors :

$$\sum_{1 \leqslant i \neq j \leqslant N} \langle P_i, P_j \rangle_v = N^2 \iint_{E(\mathbb{C})^2} \lambda_v(P - Q) \mathrm{d}\mu(P) \mathrm{d}\mu(Q) - \frac{1}{N^2} \sum_{i=1}^{N} \langle P_i, P_i \rangle_v$$

$$= N^2 \sum_{\chi} \widehat{\lambda_v}(\chi) |\hat{\mu}(\chi)^2| - \sum_{i=1}^{N} \langle P_i, P_i \rangle_v$$

## Lemme d'Elkies « pondéré »

Soit $v$ une place archimédienne, et soient $P_1, \ldots, P_N$ des points distincts de $E(L)$ tels que $P_i^\sigma \neq P_j^\tau$ pour tous $(i,\sigma) \neq (j,\tau)$. Soient $m_1, \ldots, m_N$ des réels strictement positifs qui vérifient $3\sum_{i=1}^{N} m_i^2 < 2D\left(\sum_{i=1}^{N} m_i\right)^2$. Alors,

$$\sum_{\substack{1\leqslant i,j\leqslant N\\(i,\sigma)\neq(j,\tau)}} m_i m_j \lambda_v(P_i^\sigma - P_j^\tau) \geqslant -D\sum_{i=1}^{N} m_i^2 \times$$

$$\left(\frac{1}{2}\ln\left(2D\frac{\left(\sum_{i=1}^{N} m_i\right)^2}{\sum_{i=1}^{N} m_i^2} - 2\right) + \frac{1}{12}J_v + \frac{27}{10}\right).$$

Pour résumer,

$$2D^2 n_K \left( \sum_{i=0}^{r} m_i \right) \left( \sum_{j=0}^{r} m_j p_j \right) \hat{h}(P) \geqslant \sum_{0 \leqslant i,j \leqslant r} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle$$

Pour résumer,

$$2D^2 n_K \left( \sum_{i=0}^{r} m_i \right) \left( \sum_{j=0}^{r} m_j p_j \right) \hat{h}(P) \geqslant \sum_{v \in M_K^0} \sum_{\substack{1 \leqslant i,j \leqslant r \\ i \neq j}} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle_v$$
$$+ \sum_{v \in M_K^\infty} \sum_{\substack{1 \leqslant i,j \leqslant r \\ \sigma,\tau : L \hookrightarrow \mathbb{C} \\ \sigma,\tau | v \\ (i,\sigma) \neq (j,\tau)}} n_v m_i m_j \lambda_v(\mathrm{F}_{p_i}(\mathcal{P})^\sigma - \mathrm{F}_{p_j}(\mathcal{P})^\tau)$$

Pour résumer,

$$2D^2 n_K \left( \sum_{i=0}^{r} m_i \right) \left( \sum_{j=0}^{r} m_j p_j \right) \hat{h}(P) \geqslant D n_K m_0 \sum_{i=1}^{r} m_i \ln(p_i) + \sum_{v \in M_K^\infty} \sum_{\substack{1 \leqslant i,j \leqslant r \\ \sigma,\tau : L \hookrightarrow \mathbb{C} \\ \sigma,\tau | v \\ (i,\sigma) \neq (j,\tau)}} n_v m_i m_j \lambda_v (\mathrm{F}_{p_i}(\mathcal{P})^\sigma - \mathrm{F}_{p_j}(\mathcal{P})^\tau)$$

Pour résumer,

$$2D^2 n_K \left( \sum_{i=0}^{r} m_i \right) \left( \sum_{j=0}^{r} m_j p_j \right) \hat{h}(P) \geqslant D n_K m_0 \sum_{i=1}^{r} m_i \ln(p_i)$$

$$- D n_K \sum_{i=0}^{r} m_i^2 \cdot \left( \frac{1}{2} \ln \left( 2D \frac{\left( \sum_{i=0}^{r} m_i \right)^2}{\sum_{i=0}^{r} m_i^2} - 2 \right) + \frac{h(j_E)}{12} + \frac{27}{10} \right)$$

Pour résumer,

$$2D^2 n_K \left( \sum_{i=0}^{r} m_i \right) \left( \sum_{j=0}^{r} m_j p_j \right) \hat{h}(P) \geqslant D n_K m_0 \sum_{i=1}^{r} m_i \ln(p_i)$$
$$- D n_K \sum_{i=0}^{r} m_i^2 \cdot \left( \frac{1}{2} \ln \left( 2D \frac{\left( \sum_{i=0}^{r} m_i \right)^2}{\sum_{i=0}^{r} m_i^2} - 2 \right) + \frac{h(j_E)}{12} + \frac{27}{10} \right)$$

Pour résumer,

$$2D^{\cancel{2}}\cancel{n_K}\left(\sum_{i=0}^{r} m_i\right)\left(\sum_{j=0}^{r} m_j p_j\right)\hat{h}(P) \geqslant \cancel{D}\cancel{n_K} m_0 \sum_{i=1}^{r} m_i \ln(p_i)$$

$$-\cancel{D}\cancel{n_K}\sum_{i=0}^{r} m_i^2 \cdot \left(\frac{1}{2}\ln\left(2D\frac{\left(\sum_{i=0}^{r} m_i\right)^2}{\sum_{i=0}^{r} m_i^2} - 2\right) + \frac{h(j_E)}{12} + \frac{27}{10}\right)$$

Pour résumer,

$$2D\left(\sum_{i=0}^{r} m_i\right)\left(\sum_{j=0}^{r} m_j p_j\right)\hat{h}(P) \geqslant m_0 \sum_{i=1}^{r} m_i \ln(p_i)$$
$$- \sum_{i=0}^{r} m_i^2 \cdot \left(\frac{1}{2}\ln\left(2D\frac{\left(\sum_{i=0}^{r} m_i\right)^2}{\sum_{i=0}^{r} m_i^2} - 2\right) + \frac{h(j_E)}{12} + \frac{27}{10}\right)$$

Pour résumer,

$$2D\left(\sum_{i=0}^{r} m_i\right)\left(\sum_{j=0}^{r} m_j p_j\right)\hat{h}(P) \geqslant m_0 \sum_{i=1}^{r} m_i \ln(p_i)$$
$$- \sum_{i=0}^{r} m_i^2 \cdot \left(\frac{1}{2}\ln\left(2D\frac{\left(\sum_{i=0}^{r} m_i\right)^2}{\sum_{i=0}^{r} m_i^2} - 2\right) + \frac{h(j_E)}{12} + \frac{27}{10}\right)$$

On pose $m_i = 1$ pour $i > 0$, et $m_0 = \sqrt{r}$.

Pour résumer,

$$2D\,(m_0+r)\left(m_0+\sum_{j=0}^{r}p_j\right)\hat{h}(P)\geqslant m_0\sum_{i=1}^{r}\ln(p_i)$$
$$-\,(m_0^2+r)\cdot\left(\frac{1}{2}\ln\left(2D\frac{(m_0+r)^2}{m_0^2+r}-2\right)+\frac{h(j_E)}{12}+\frac{27}{10}\right)$$

On pose $m_i = 1$ pour $i > 0$, et $m_0 = \sqrt{r}$.

Pour résumer,

$$2D\,(m_0+r)\left(m_0+\sum_{j=0}^{r}p_j\right)\hat{h}(P)\geqslant m_0\sum_{i=1}^{r}\ln(p_i)$$
$$-\,(m_0^2+r)\cdot\left(\frac{1}{2}\ln\left(2D\frac{(m_0+r)^2}{m_0^2+r}-2\right)+\frac{h(j_E)}{12}+\frac{27}{10}\right)$$

On pose $m_i = 1$ pour $i > 0$, et $m_0 = \sqrt{r}$. On a :

$$\sum_{i=1}^{r}\ln(p_i)\sim r\ln(r),\ \text{et}\ \sum_{i=1}^{r}p_i\sim\frac{r^2}{2}\ln(r)\ \text{quand}\ r\to\infty.$$

# Plan

Soit $L/K$ une extension galoisienne de corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ qui ne se ramifie pas dans $L$, et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de $G$ qui relève $\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \to & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \end{array}$, et $\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right); \mathfrak{P}|\mathfrak{p}\right\}$. Si $C$ est une classe de conjugaison, soit $\pi_C(x)$ la fonction de décompte des idéaux premiers de norme inférieure à $x$ tels que $\left(\frac{L/K}{\mathfrak{p}}\right) = C$.

**Théorème de Chebotarev explicite inconditionnel (W. (2014))**

Soit $\beta$ l'éventuel zéro de $\zeta_L$ « près de 1 ». Alors, pour tout $x \geqslant \exp\left(110000 n_L (\ln(9 d_L^8))^2\right)$,

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant \frac{|C|}{|G|}\left(\mathrm{Li}\left(x^\beta\right) + 3,37 \cdot 10^{13} x \exp\left(-\frac{1}{12}\sqrt{\frac{\ln(x)}{n_L}}\right)\right).$$

Soit $L/K$ une extension galoisienne de corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ qui ne se ramifie pas dans $L$, et $\mathfrak{P}|\mathfrak{p}$. On appelle automorphisme de Frobenius, noté $\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right)$, l'élément de $G$ qui relève $\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \to & \mathcal{O}_L/\mathfrak{P} \\ x & \mapsto & x^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \end{array}$, et $\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{\left(\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right); \mathfrak{P}|\mathfrak{p}\right\}$. Si $C$ est une classe de conjugaison, soit $\pi_C(x)$ la fonction de décompte des idéaux premiers de norme inférieure à $x$ tels que $\left(\frac{L/K}{\mathfrak{p}}\right) = C$.

**Théorème de Chebotarev explicite avec HRG (W. (2014))**

Supposons que HRG est vraie pour $\zeta_L$. Alors, pour tout $x \geqslant 2$,

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\left[1,2\ln(d_L) + 0,6\ln(x)n_L + \text{reste}\right].$$

On pose $G = \mathrm{Gal}(L/K)$. Soient $\rho$ ses représentations irréductibles, et $\Phi$ les caractères associés. Fixons $g \in C$.

On pose $G = \mathrm{Gal}(L/K)$. Soient $\rho$ ses représentations irréductibles, et $\Phi$ les caractères associés. Fixons $g \in C$.

$$\mathrm{L}(s, \Phi) = \prod_{\mathfrak{p} \text{ non ram.}} \det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1} \times \prod_{\mathfrak{p} \text{ ram.}} (\cdots).$$

On pose $G = \mathrm{Gal}(L/K)$. Soient $\rho$ ses représentations irréductibles, et $\Phi$ les caractères associés. Fixons $g \in C$.

$$\mathrm{L}(s,\Phi) = \prod_{\mathfrak{p} \text{ non ram.}} \det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1} \times \prod_{\mathfrak{p} \text{ ram.}} (\cdots).$$

- on a $F_C(s) := -\sum_{\Phi} \frac{|C|}{|G|}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi) \simeq s\int_0^\infty \psi_C(x)x^{-s}\frac{\mathrm{d}x}{x}$ ;

On pose $G = \mathrm{Gal}(L/K)$. Soient $\rho$ ses représentations irréductibles, et $\Phi$ les caractères associés. Fixons $g \in C$.

$$\mathrm{L}(s,\Phi) = \prod_{\mathfrak{p} \text{ non ram.}} \det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1} \times \prod_{\mathfrak{p} \text{ ram.}} (\cdots).$$

- on a $F_C(s) := -\sum_{\Phi} \frac{|C|}{|G|}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi) \simeq s\int_0^\infty \psi_C(x)x^{-s}\frac{\mathrm{d}x}{x}$ ;
- on en déduit $\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s}$ ;

On pose $G = \mathrm{Gal}(L/K)$. Soient $\rho$ ses représentations irréductibles, et $\Phi$ les caractères associés. Fixons $g \in C$.

$$\mathrm{L}(s,\Phi) = \prod_{\mathfrak{p} \text{ non ram.}} \det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1} \times \prod_{\mathfrak{p} \text{ ram.}} (\cdots).$$

- on a $F_C(s) := -\sum_{\Phi} \frac{|C|}{|G|}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi) \simeq s\int_0^\infty \psi_C(x)x^{-s}\frac{\mathrm{d}x}{x}$ ;
- on en déduit
  $\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s} = \int_{c-i\infty}^{c+i\infty}\sum_{\chi}\frac{\mathrm{L}'}{\mathrm{L}}(\chi,s)x^s\frac{\mathrm{d}s}{s}$ ;

On pose $G = \mathrm{Gal}(L/K)$. Soient $\rho$ ses représentations irréductibles, et $\Phi$ les caractères associés. Fixons $g \in C$.

$$\mathrm{L}(s,\Phi) = \prod_{\mathfrak{p} \text{ non ram.}} \det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1} \times \prod_{\mathfrak{p} \text{ ram.}} (\cdots).$$

- on a $F_C(s) := -\sum_{\Phi} \frac{|C|}{|G|}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi) \simeq s\int_0^\infty \psi_C(x)x^{-s}\frac{\mathrm{d}x}{x}$ ;
- on en déduit
  $\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s} = \int_{c-i\infty}^{c+i\infty}\sum_{\chi}\frac{\mathrm{L}'}{\mathrm{L}}(\chi,s)x^s\frac{\mathrm{d}s}{s}$ ;
- le théorème des résidus implique
  $\psi_C(x) = \frac{|C|}{|G|}\sum_{\chi}\bar{\chi}(g)\left(-\sum_{\rho}\frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)}\right) + o(x)$ ;

On pose $G = \mathrm{Gal}(L/K)$. Soient $\rho$ ses représentations irréductibles, et $\Phi$ les caractères associés. Fixons $g \in C$.

$$\mathrm{L}(s,\Phi) = \prod_{\mathfrak{p} \text{ non ram.}} \det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1} \times \prod_{\mathfrak{p} \text{ ram.}} (\cdots).$$

- on a $F_C(s) := -\sum_{\Phi} \frac{|C|}{|G|}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi) \simeq s\int_0^\infty \psi_C(x)x^{-s}\frac{\mathrm{d}x}{x}$ ;
- on en déduit
  $\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s} = \int_{c-i\infty}^{c+i\infty}\sum_{\chi}\frac{\mathrm{L}'}{\mathrm{L}}(\chi,s)x^s\frac{\mathrm{d}s}{s}$ ;
- le théorème des résidus implique
  $\psi_C(x) = \frac{|C|}{|G|}\sum_{\chi}\bar{\chi}(g)\left(-\sum_{\rho}\frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)}\right) + o(x)$ ;
- le caractère principal contribue avec un $x$, et $\psi_C(x) \sim \frac{|C|}{|G|}x$ ;

On pose $G = \mathrm{Gal}(L/K)$. Soient $\rho$ ses représentations irréductibles, et $\Phi$ les caractères associés. Fixons $g \in C$.

$$\mathrm{L}(s,\Phi) = \prod_{\mathfrak{p} \text{ non ram.}} \det\left(\mathrm{I} - \rho\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]\right)(\mathrm{N}(\mathfrak{p}))^{-s}\right)^{-1} \times \prod_{\mathfrak{p} \text{ ram.}} (\cdots).$$

- on a $F_C(s) := -\sum_{\Phi} \frac{|C|}{|G|}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi) \simeq s\int_0^\infty \psi_C(x)x^{-s}\frac{\mathrm{d}x}{x}$ ;
- on en déduit
  $\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s} = \int_{c-i\infty}^{c+i\infty}\sum_{\chi}\frac{\mathrm{L}'}{\mathrm{L}}(\chi,s)x^s\frac{\mathrm{d}s}{s}$ ;
- le théorème des résidus implique
  $\psi_C(x) = \frac{|C|}{|G|}\sum_{\chi}\bar{\chi}(g)\left(-\sum_{\rho}\frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)}\right) + o(x)$ ;
- le caractère principal contribue avec un $x$, et $\psi_C(x) \sim \frac{|C|}{|G|}x$ ;
- on en déduit $\pi_C(x) \sim \frac{|C|}{|G|}\mathrm{Li}(x) \sim \frac{|C|}{|G|}\frac{x}{\ln(x)}$.

# Étape 1 : $F_C(s) \simeq s \int_0^\infty \psi_C(x) x^{-s} \frac{\mathrm{d}x}{x}$

# Étape 1 : $F_C(s) \simeq s \int_0^\infty \psi_C(x) x^{-s} \frac{\mathrm{d}x}{x}$

Pour tout $\Phi$, on pose $\Phi_K(\mathfrak{p}^m) = \frac{1}{e} \sum_{\alpha \in \mathrm{I}_{\mathfrak{P}}} \Phi\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m \alpha\right)$.

# Étape 1 : $F_C(s) \simeq s \int_0^\infty \psi_C(x) x^{-s} \frac{\mathrm{d}x}{x}$

Pour tout $\Phi$, on pose $\Phi_K(\mathfrak{p}^m) = \frac{1}{e} \sum_{\alpha \in \mathrm{I}_{\mathfrak{P}}} \Phi\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m \alpha\right)$. Alors,

$$-\frac{\mathrm{L}'}{\mathrm{L}}(s, \Phi, L/K) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \Phi_K(\mathfrak{p}^m) \frac{\ln(\mathrm{N}(\mathfrak{p}))}{(\mathrm{N}(\mathfrak{p}))^{ms}}.$$

# Étape 1 : $F_C(s) \simeq s\int_0^\infty \psi_C(x)x^{-s}\frac{\mathrm{d}x}{x}$

Pour tout $\Phi$, on pose $\Phi_K(\mathfrak{p}^m) = \frac{1}{e}\sum_{\alpha\in \mathrm{I}_{\mathfrak{P}}} \Phi\left(\left[\frac{L/K}{\mathfrak{P},\mathfrak{p}}\right]^m \alpha\right)$. Alors,

$$-\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi,L/K) = \sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\Phi_K(\mathfrak{p}^m)\frac{\ln(\mathrm{N}(\mathfrak{p}))}{(\mathrm{N}(\mathfrak{p}))^{ms}}.$$

Donc, si $g \in C$ :

$$F_C(s) = -\frac{|C|}{|G|}\sum_{\Phi}\bar{\Phi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\Phi,L/K) = \sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\theta(\mathfrak{p}^m)\frac{\ln(\mathrm{N}(\mathfrak{p}))}{(\mathrm{N}(\mathfrak{p}))^{ms}}$$

où, pour $\mathfrak{p}$ non ramifié dans $L$, on a $\theta(\mathfrak{p}^m) = 1$ si $\left[\frac{L/K}{\mathfrak{p}}\right]^m = C$, $\theta(\mathfrak{p}^m) = 0$ sinon, et $|\theta(\mathfrak{p}^m)| \leqslant 1$ si $\mathfrak{p}$ se ramifie dans $L$.

# Étape 2 : $\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s}$

$$\left|\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} F_C(s)\frac{x^s}{s}\mathrm{d}s - \sum_{\substack{\mathfrak{p},m\\ \mathrm{N}(\mathfrak{p})^m\leqslant x}} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\right| \leqslant R_0(x,T),$$

où $R_0(x,T) \leqslant 20n_K\ln(x) + 17n_K T^{-1}x(\ln(x))^2$.

# Étape 2 : $\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s}$

$$\left|\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} F_C(s)\frac{x^s}{s}\mathrm{d}s - \sum_{\substack{\mathfrak{p},m\\ \mathrm{N}(\mathfrak{p})^m\leqslant x}} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p}))\right| \leqslant R_0(x,T),$$

où $R_0(x,T) \leqslant 20n_K\ln(x) + 17n_K T^{-1}x(\ln(x))^2$.

Or $\left|\sum_{\substack{\mathfrak{p},m\\ \mathrm{N}(\mathfrak{p}^m)\leqslant x}} \theta(\mathfrak{p}^m)\ln(\mathrm{N}(\mathfrak{p})) - \psi_C(x)\right| \leqslant \frac{2}{\ln(2)}\frac{\ln(x)\ln(d_L)}{|G|}$

# Étape 2 :

$$\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s} = \int_{c-i\infty}^{c+i\infty}\sum_{\chi}\frac{\mathrm{L}'}{\mathrm{L}}(\chi,s)x^s\frac{\mathrm{d}s}{s}$$

Soit $g \in C$, et soit $H$ le sous-groupe de $G$ engendré par $g$, $E$ le corps fixé par $H$, et notons $\chi$ les caractères irréductibles de $H$.

# Étape 2 :

$$\psi_C(x) \simeq -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F_C(s)x^s\frac{\mathrm{d}s}{s} = \int_{c-i\infty}^{c+i\infty}\sum_{\chi}\frac{\mathrm{L}'}{\mathrm{L}}(\chi,s)x^s\frac{\mathrm{d}s}{s}$$

Soit $g \in C$, et soit $H$ le sous-groupe de $G$ engendré par $g$, $E$ le corps fixé par $H$, et notons $\chi$ les caractères irréductibles de $H$.

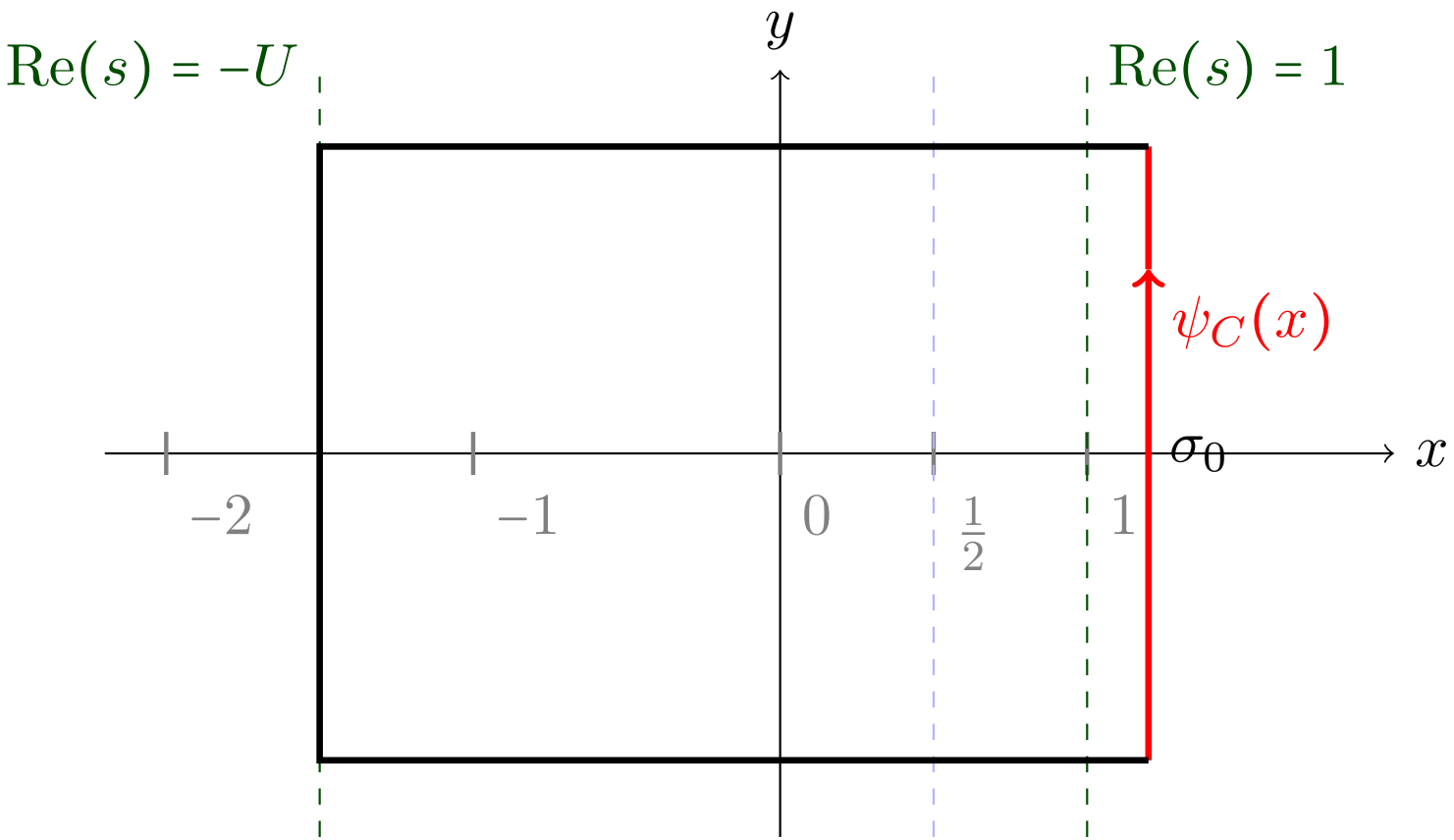
On a

$$F_C(s) = -\frac{|C|}{|G|}\sum_{\chi}\bar{\chi}(g)\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi,L/E).$$

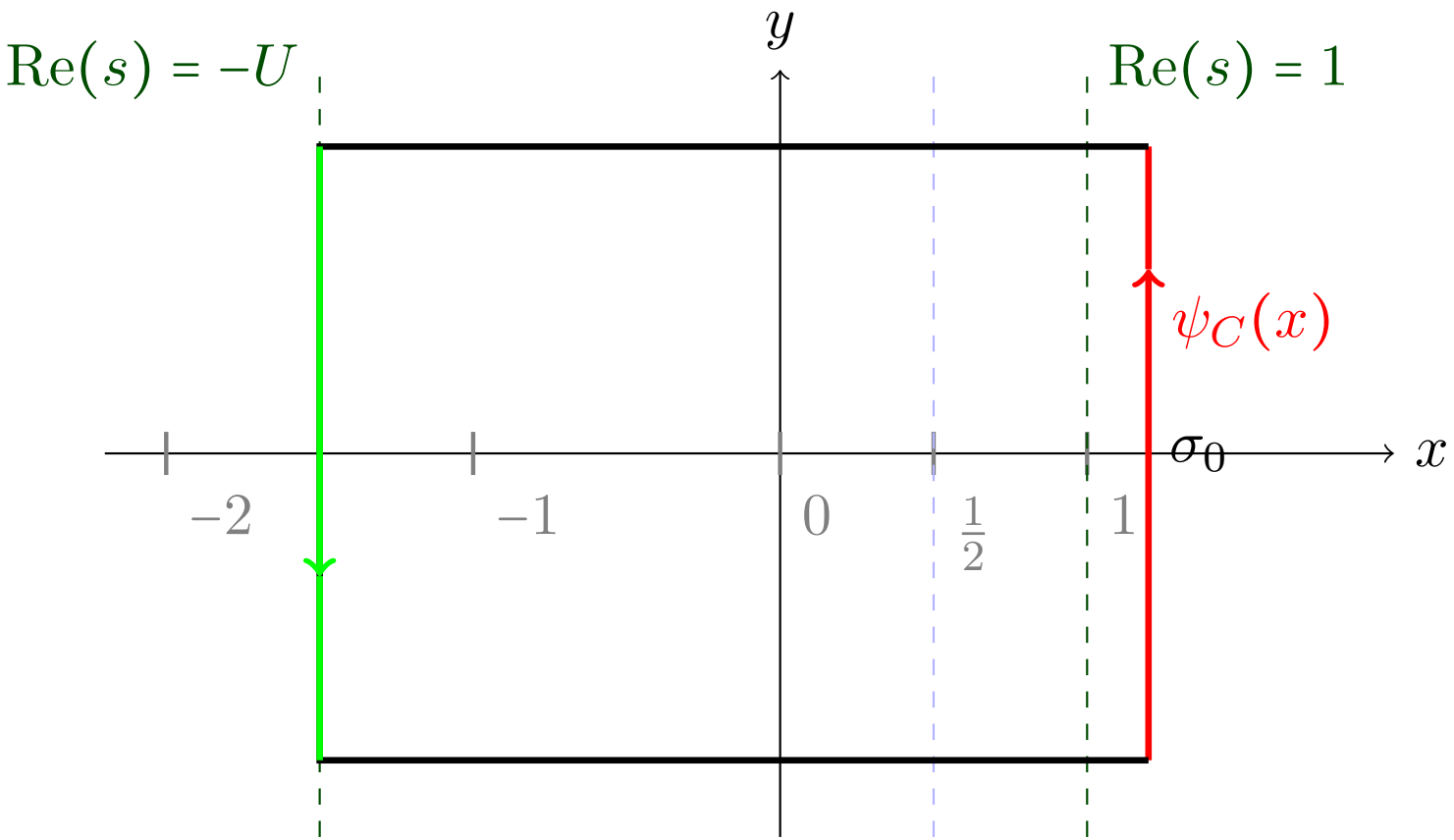
# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_\chi \bar{\chi}(g) \left( - \sum_\rho \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$

Problème : approcher $\int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} \frac{\mathrm{L}'}{\mathrm{L}}(s, \chi, L/E) \mathrm{d}s$ par une intégrale sur un contour.

# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left( - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$



# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left( - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$



# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_\chi \bar{\chi}(g) \left( - \sum_\rho \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$

Posons $\gamma_\chi(s) = \left(\pi^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)\right)^{b(\chi)} \left(\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\right)^{a(\chi)}$. La fonction $\xi(s,\chi) = (s(s-1))^{\delta_{\chi=1}(\chi)} A(\chi)^{s/2} \gamma_\chi(s) \mathrm{L}(s,\chi)$ est *entière*, et vérifie l'équation fonctionnelle

$$\xi(1-s,\bar{\chi}) = W(\chi)\xi(s,\chi),$$

# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_\chi \bar{\chi}(g) \left( - \sum_\rho \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$

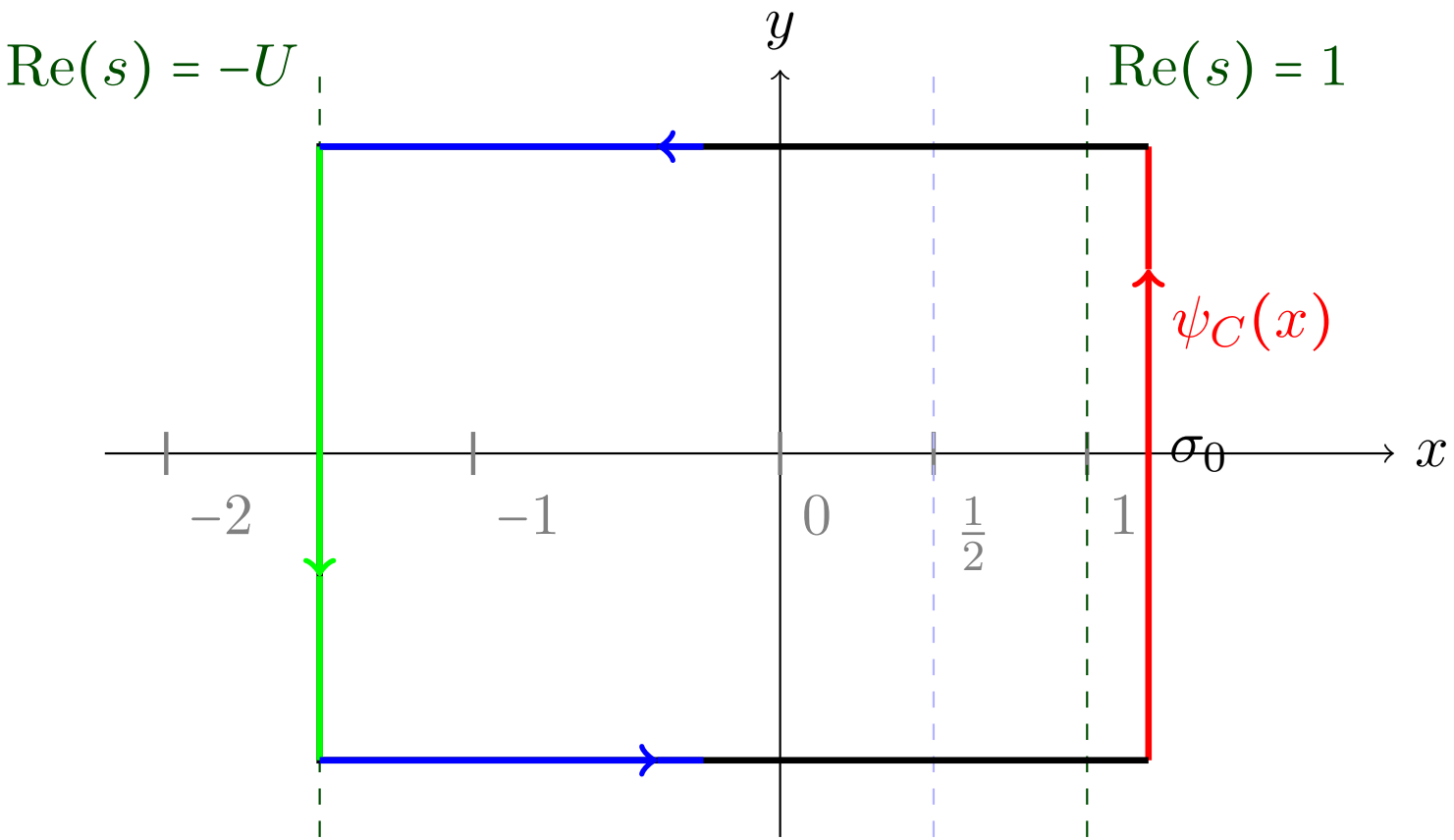
Posons $\gamma_\chi(s) = \left(\pi^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)\right)^{b(\chi)} \left(\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\right)^{a(\chi)}$. La fonction $\xi(s,\chi) = (s(s-1))^{\delta_{\chi=1}(\chi)} A(\chi)^{s/2} \gamma_\chi(s) \mathrm{L}(s,\chi)$ est *entière*, et vérifie l'équation fonctionnelle

$$\xi(1-s,\bar{\chi}) = W(\chi)\xi(s,\chi),$$

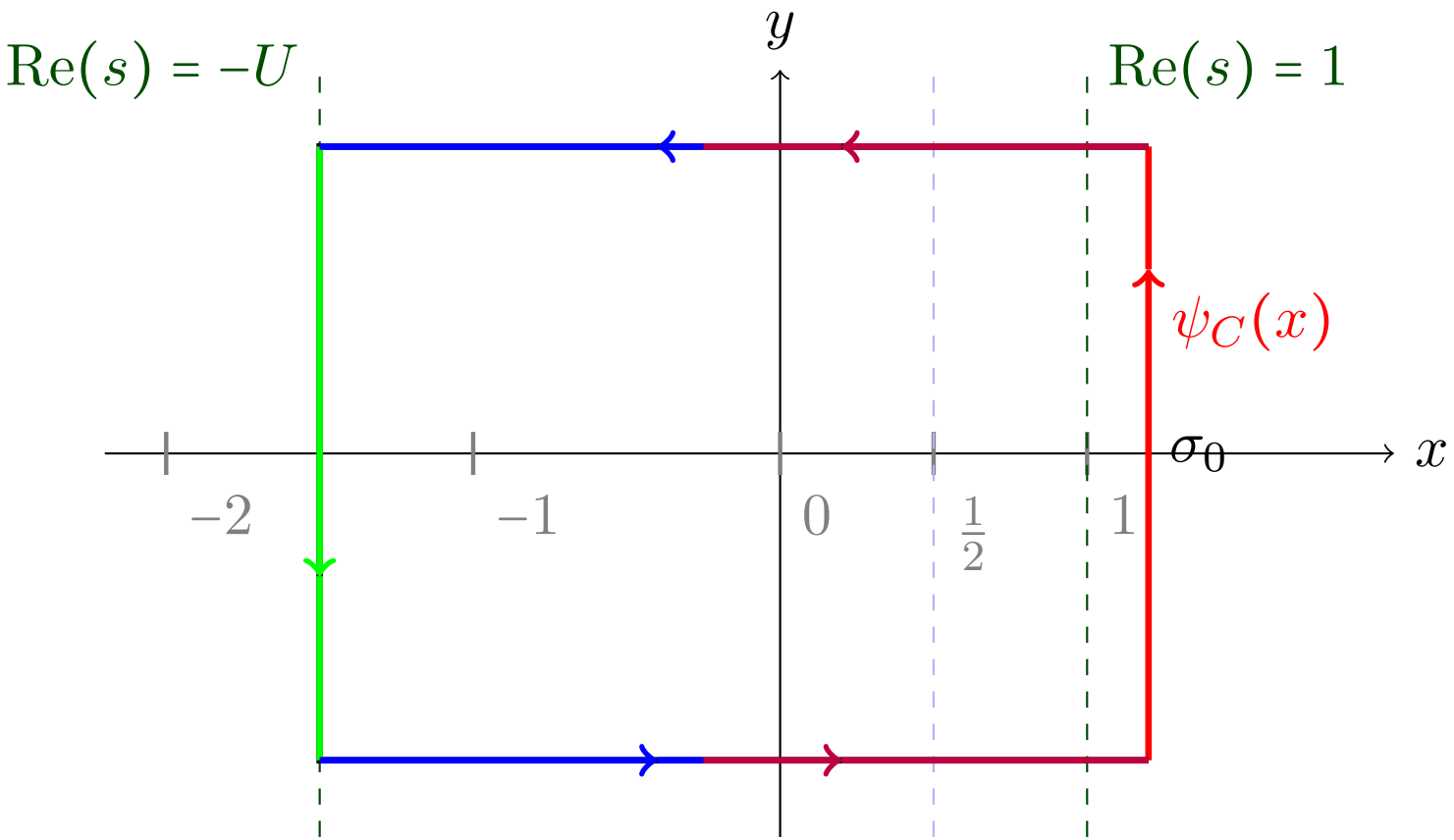
donc en particulier :

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = -\frac{\mathrm{L}'}{\mathrm{L}}(1-s,\bar{\chi}) - \ln(A(\chi)) - \frac{\gamma'_\chi}{\gamma_\chi}(1-s) - \frac{\gamma'_\chi}{\gamma_\chi}(s).$$

# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left( - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$



# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left( - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$



# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_\chi \bar{\chi}(g) \left( - \sum_\rho \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$

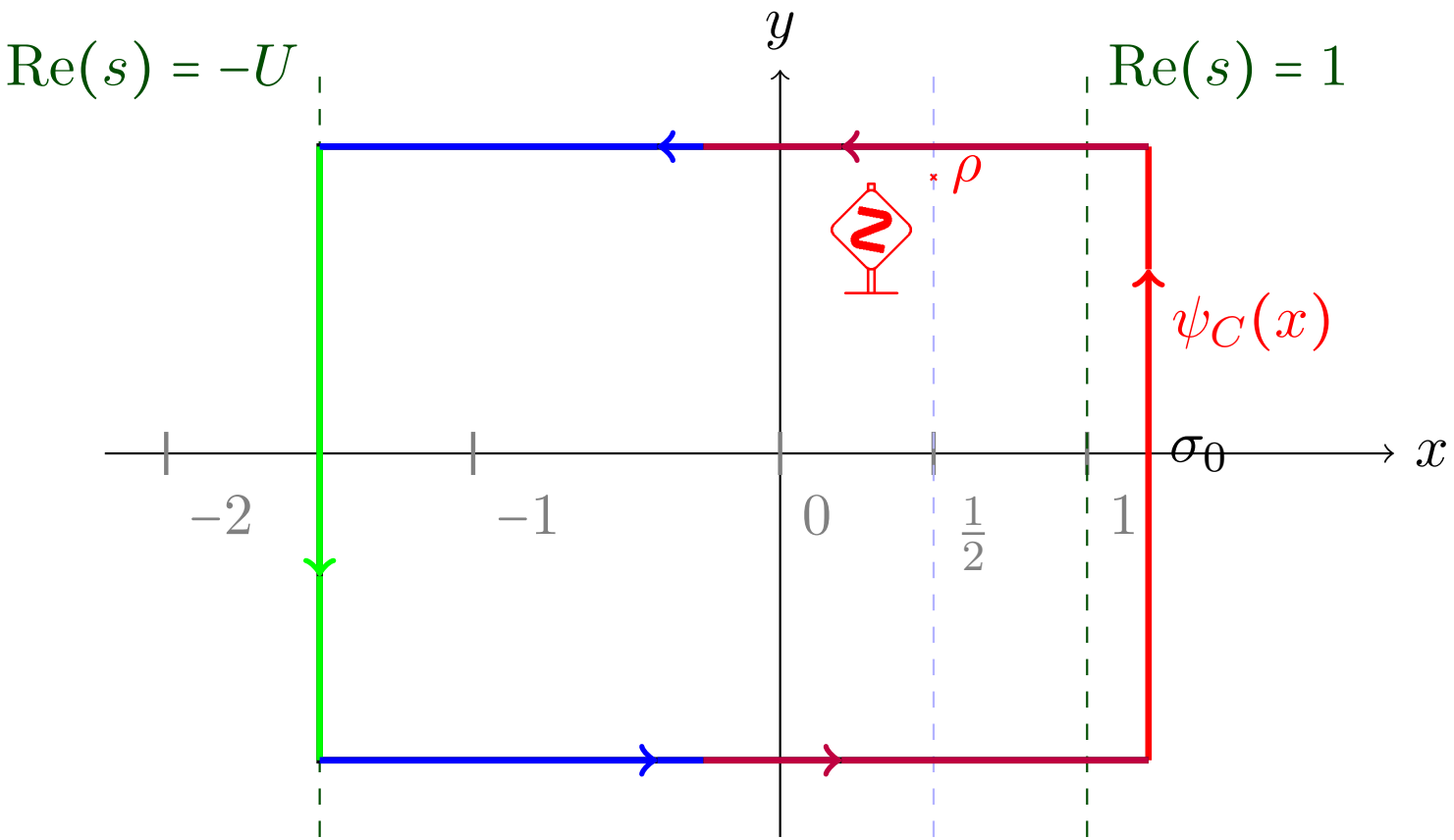
On a :

$$\xi(s,\chi) = e^{B_1(\chi)+B(\chi)s} \prod_\rho \left(1 - \frac{s}{\rho}\right) e^{s/\rho},$$

et donc :

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) + \frac{\mathrm{L}'}{\mathrm{L}}(s,\bar{\chi}) = \sum_\rho \left( \frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}} \right) - \ln(A(\chi))$$
$$-2\delta_{\chi=1}(\chi) \left( \frac{1}{s} + \frac{1}{s-1} \right) - 2\frac{\gamma'_\chi}{\gamma_\chi}(s).$$

# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left( - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$



# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left( - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$

## Densité des zéros

Soit $n_\chi(t)$ le nombre de zéros $\rho = \beta + i\gamma$ de $\mathrm{L}(\cdot, \chi)$ avec $0 < \beta < 1$ et $|\gamma - t| \leqslant 1$. Pour tout $t$, on a

$$n_\chi(t) + n_\chi(-t) \leqslant \frac{5}{2} \Big[ \ln(A(\chi)) + 2\delta_{\chi=1}(\chi) \left( \frac{2}{4+t^2} + \frac{1}{1+t^2} \right) + n_E \left( \ln \left( \frac{|t|+3}{2\pi} \right) + 2 \right) \Big].$$

# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_\chi \bar{\chi}(g) \left( - \sum_\rho \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$

Résidus de $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\frac{x^s}{s}$ :

- en chaque zéro $\rho$ de $\mathrm{L}(s,\chi)$, de résidu $\frac{x^\rho}{\rho}$ ;
- en chaque pôle de $\gamma_\chi$, *i.e.* de $\Gamma$, *i.e.* en les entiers négatifs $-m$, de résidu $a(\chi)\frac{x^{-m}}{-m}$ ou $b(\chi)\frac{x^{-m}}{-m}$ ;
- un résidu éventuellement en 0, plus compliqué, mais en $o(x)$ ;
- en $s = 1$ si $L(s,\chi) = \zeta_L(s)$, de résidu $-x$.

# Étape 3 : $\psi_C(x) = \frac{|C|}{|G|} \sum_\chi \bar{\chi}(g) \left( - \sum_\rho \frac{x^\rho}{\rho} - \frac{\mathrm{L}'(\chi,0)}{\mathrm{L}(\chi,0)} \right) + o(x)$

Résidus de $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\frac{x^s}{s}$ :

- en chaque zéro $\rho$ de $\mathrm{L}(s,\chi)$, de résidu $\frac{x^\rho}{\rho}$ ;
- en chaque pôle de $\gamma_\chi$, *i.e.* de $\Gamma$, *i.e.* en les entiers négatifs $-m$, de résidu $a(\chi)\frac{x^{-m}}{-m}$ ou $b(\chi)\frac{x^{-m}}{-m}$ ;
- un résidu éventuellement en 0, plus compliqué, mais en $o(x)$ ;
- en $s = 1$ si $L(s,\chi) = \zeta_L(s)$, de résidu $-x$.

Donc $\psi_C(x) \simeq \frac{|C|}{|G|}x + \frac{|C|}{|G|} \sum_\chi \sum_\rho \frac{x^\rho}{\rho}$.

# Étape 4 : $\psi_C(x) \sim \frac{|C|}{|G|}x$

## Formule explicite pour $\psi_C$

Si $x \geqslant 2$ et $T \geqslant 2$, alors

$$\left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T)\right| \leqslant \frac{|C|}{|G|}\Big(24,2n_L\frac{x(\ln(x))^2}{T} + 7,1\frac{x\ln(x)}{T-1}\Big[\ln(d_L)+0,9 + n_L\left(\ln(T+5)+2\right)\Big] + \text{etc.}\Big),$$

où $S(x,T) = \frac{|C|}{|G|}\sum_{\chi}\bar{\chi}(g)\left(\sum_{\substack{\rho \\ |\gamma|<T}}\frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho|<\frac{1}{2}}}\frac{1}{\rho}\right)$.

# Étape 4 : $\psi_C(x) \sim \frac{|C|}{|G|}x$

## Formule explicite pour $\psi_C$

Si $x \geqslant 2$ et $T \geqslant 2$, alors

$$\left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T)\right| \leqslant \frac{|C|}{|G|}\Big(24,2n_L\frac{x(\ln(x))^2}{T} + 7,1\frac{x\ln(x)}{T-1}\Big[\ln(d_L)+0,9 + n_L\left(\ln(T+5)+2\right)\Big] + \text{etc.}\Big),$$

où $S(x,T) \leqslant \frac{5}{2}\sqrt{x}\left(\left(2+\frac{\ln(T)}{2}\right)\left(\ln(A(\chi))+n_E\right)+\text{etc.}\right)$ si HRG.

# Étape 4 : $\psi_C(x) \sim \frac{|C|}{|G|}x$

## Formule explicite pour $\psi_C$

Si $x \geqslant 2$ et $T \geqslant 2$, alors

$$\left|\psi_C(x) - \frac{|C|}{|G|}x + S(x,T)\right| \leqslant \frac{|C|}{|G|}\Big(24,2n_L\frac{x(\ln(x))^2}{T} + 7,1\frac{x\ln(x)}{T-1}\Big[\ln(d_L)+0,9 + n_L\left(\ln(T+5)+2\right)\Big] + \text{etc.}\Big),$$

où $S(x,T) \leqslant \frac{5}{2}\sqrt{x}\left(\left(2+\frac{\ln(T)}{2}\right)\left(\ln(A(\chi))+n_E\right)+\text{etc.}\right)$. On pose alors $T = \frac{\sqrt{2}}{\ln(2)}\sqrt{x}\ln(x)$.

# Étape 5 : $\pi_C(x) \sim \frac{|C|}{|G|}\mathrm{Li}(x) \sim \frac{|C|}{|G|}\frac{x}{\ln(x)}$

Posons $\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) \leqslant x \\ \left[\frac{L/K}{\mathfrak{p}}\right] = C}} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}))$.

# Étape 5 : $\pi_C(x) \sim \frac{|C|}{|G|}\mathrm{Li}(x) \sim \frac{|C|}{|G|}\frac{x}{\ln(x)}$

Posons $\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) \leqslant x \\ \left[\frac{L/K}{\mathfrak{p}}\right]=C}} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}))$.

Alors, $\psi_C(x) - \theta_C(x) \leqslant \frac{22}{15} n_K \sqrt{x} \ln(x)$.

# Étape 5 : $\pi_C(x) \sim \frac{|C|}{|G|}\mathrm{Li}(x) \sim \frac{|C|}{|G|}\frac{x}{\ln(x)}$

Posons $\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) \leqslant x \\ \left[\frac{L/K}{\mathfrak{p}}\right]=C}} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}))$.

Alors, $\psi_C(x) - \theta_C(x) \leqslant \frac{22}{15} n_K \sqrt{x} \ln(x)$. Donc $\psi_C(x) \simeq \theta_C(x)$.

# Étape 5 : $\pi_C(x) \sim \frac{|C|}{|G|}\mathrm{Li}(x) \sim \frac{|C|}{|G|}\frac{x}{\ln(x)}$

Posons $\theta_C(x) = \sum_{\substack{\mathfrak{p} \text{ non ramifié} \\ \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) \leqslant x \\ \left[\frac{L/K}{\mathfrak{p}}\right]=C}} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}))$.

Alors, $\psi_C(x) - \theta_C(x) \leqslant \frac{22}{15} n_K \sqrt{x} \ln(x)$. Donc $\psi_C(x) \simeq \theta_C(x)$. On conclut avec

$$\pi_C(x) = \frac{\theta_C(x)}{\ln(x)} + \int_2^x \frac{\theta_C(t)}{t(\ln(t))^2} \mathrm{d}t.$$

On a donc :

$$\hat{h}(P) \geqslant \frac{1}{D} \frac{\sum_{i=1}^{r} \ln(p_i) - 2\sqrt{r}\left(\frac{1}{2}\ln\left(D(\sqrt{r}+1)^2-2\right) + \frac{1}{12}h(j_E) + \frac{27}{10}\right)}{2\left(\sqrt{r} + \sum_{i=1}^{r} p_i\right)\left(\sqrt{r}+1\right)}$$

On a donc :

$$\hat{h}(P) \geqslant \frac{1}{D} \frac{\sum_{i=1}^{r} \ln(p_i) - 2\sqrt{r}\left(\frac{1}{2}\ln\left(D(\sqrt{r}+1)^2-2\right) + \frac{1}{12}h(j_E) + \frac{27}{10}\right)}{2\left(\sqrt{r} + \sum_{i=1}^{r} p_i\right)\left(\sqrt{r}+1\right)}$$

Si $s \geqslant 2^{20}(59,07 + 1,44\ln(|d_K|) + 76,88 n_K)^4$, alors :

$$\frac{1}{2n_K} s \leqslant \sum_{i=1}^{r} \ln(p_i) \leqslant \frac{3}{2n_K} s, \quad \sum_{p=1}^{r} p_i \leqslant \frac{1}{2n_K}\left[\frac{8}{3} + \frac{3}{\ln(s)}\right]\frac{s^2}{\ln(s)}, \text{ et}$$

$$\frac{1}{2n_K}\frac{s}{\ln(s)} \leqslant r \leqslant \frac{3}{2n_K}\left(1 + \frac{1,3}{\ln(s)}\right)\frac{s}{\ln(s)}.$$

On a donc :

$$\hat{h}(P) \geqslant \frac{1}{D} \frac{\frac{s}{2n_K} - 2\sqrt{\frac{3}{2n_K}\frac{s}{\ln(s)}\left(1+\frac{1,3}{5\ln(10)}\right)}\left(\frac{1}{2}\ln(4Ds)+\frac{1}{12}h(j_E)+2\right)}{2\left(\sqrt{\frac{s}{2n_K}}+\frac{s^2}{2n_K\ln(s)}\left[\frac{8}{3}+\frac{3}{\ln(s)}\right]\right)\left(\sqrt{\frac{s}{2n_K}}+1\right)}$$

Si $s \geqslant 2^{20}(59,07+1,44\ln(|d_K|)+76,88n_K)^4$, alors :

$$\frac{1}{2n_K}s \leqslant \sum_{i=1}^{r}\ln(p_i) \leqslant \frac{3}{2n_K}s, \quad \sum_{p=1}^{r} p_i \leqslant \frac{1}{2n_K}\left[\frac{8}{3}+\frac{3}{\ln(s)}\right]\frac{s^2}{\ln(s)}, \text{ et}$$

$$\frac{1}{2n_K}\frac{s}{\ln(s)} \leqslant r \leqslant \frac{3}{2n_K}\left(1+\frac{1,3}{\ln(s)}\right)\frac{s}{\ln(s)}.$$

On a donc :

$$\hat{h}(P) \geqslant \frac{1}{D} \frac{\frac{s}{2n_K} - 2\sqrt{\frac{3}{2n_K}\frac{s}{\ln(s)}\left(1+\frac{1{,}3}{5\ln(10)}\right)}\left(\frac{1}{2}\ln(4Ds)+\frac{1}{12}h(j_E)+2\right)}{2\left(\sqrt{\frac{s}{2n_K}}+\frac{s^2}{2n_K\ln(s)}\left[\frac{8}{3}+\frac{3}{\ln(s)}\right]\right)\left(\sqrt{\frac{s}{2n_K}}+1\right)}$$

Si $s \geqslant 2^{20}(59{,}07 + 1{,}44\ln(|d_K|) + 76{,}88n_K)^4$

On a donc :

$$\hat{h}(P) \geqslant \frac{1}{D} \frac{\frac{s}{2n_K} - 2\sqrt{\frac{3}{2n_K}\frac{s}{\ln(s)}\left(1+\frac{1{,}3}{5\ln(10)}\right)}\left(\frac{1}{2}\ln(4Ds)+\frac{1}{12}h(j_E)+2\right)}{20n_K s^{3/2}}$$

Si $s \geqslant 2^{20}(59{,}07 + 1{,}44\ln(|d_K|) + 76{,}88n_K)^4 \dfrac{\left[\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right]^2}{\left[\ln\left(\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right)\right]^{-1}}$

On a donc :

$$\hat{h}(P) \geqslant \frac{1}{D} \frac{(\ln(s))^{3/2}}{20 n_K s^{3/2}}$$

Si $s \geqslant 2^{20}(59,07 + 1,44\ln(|d_K|) + 76,88 n_K)^4 \dfrac{\left[\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right]^2}{\left[\ln\left(\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right)\right]^{-1}}$

On a donc :

$$\hat{h}(P) \geqslant \frac{1}{D} \frac{(\ln(s))^{3/2}}{20 n_K s^{3/2}}$$

Si $s = 2^{20}(59,07 + 1,44 \ln(|d_K|) + 76,88 n_K)^4 \dfrac{\left[\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right]^2}{\left[\ln\left(\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right)\right]^{-1}}$

On a donc :

$$\hat{h}(P) \geqslant \frac{1}{D} \frac{(\ln(s))^{3/2}}{20 n_K s^{3/2}} \quad \text{CQFD.}$$

Si $s = 2^{20}(59,07 + 1,44 \ln(|d_K|) + 76,88 n_K)^4 \dfrac{\left[\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right]^2}{\left[\ln\left(\ln\left(4De^{4+\frac{h(j_E)}{6}}\right)\right)\right]^{-1}}$

# Plan

## Perspectives

## Perspectives

- améliorer les résultats analytiques obtenus (idéal premier de petite norme, *etc.*) ;

## Perspectives

- améliorer les résultats analytiques obtenus (idéal premier de petite norme, *etc.*) ;
- les étendre à une classe de fonctions L plus grande ;

## Perspectives

- améliorer les résultats analytiques obtenus (idéal premier de petite norme, *etc.*) ;
- les étendre à une classe de fonctions L plus grande ;
- réemployer l'approche arakelovienne pour d'autres études de points algébriques sur une courbe elliptique ;

## Perspectives

- améliorer les résultats analytiques obtenus (idéal premier de petite norme, *etc.*) ;
- les étendre à une classe de fonctions L plus grande ;
- réemployer l'approche arakelovienne pour d'autres études de points algébriques sur une courbe elliptique ;
- songer à la dimension supérieure.