Intersection arithmétique

Bruno Winckler

Université Lyon 1, 17 octobre 2017

17 octobre 2016

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

Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$. On pose $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, avec $X, Y, Z \in \mathbb{Z}$.

Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$. On pose $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, avec $X, Y, Z \in \mathbb{Z}$.

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 $x^2 + y^2 = 1$. On pose $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, avec $X, Y, Z \in \mathbb{Z}$.

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 $x^2 + y^2 = 1$. On pose $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, avec $X, Y, Z \in \mathbb{Z}$.

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 $x^2 + y^2 = 1$. On pose $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, avec $X, Y, Z \in \mathbb{Z}$.

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

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

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

- si p divise $X + iY$ et $X - iY$, alors il divise $2X$ et $2iY$, donc divise 2 : impossible ;

Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$. On pose $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, avec $X, Y, Z \in \mathbb{Z}$.

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

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

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

- si p divise $X + iY$ et $X - iY$, alors il divise $2X$ et $2iY$, donc divise 2 : impossible ;
- alors, $X + iY = (u + iv)^2$, et $(X, Y, Z) = (u^2 - v^2, 2uv, u^2 + v^2)$.

Exemple introductif

Considérons l'équation $x^2 + y^2 = 1$. On pose $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, avec $X, Y, Z \in \mathbb{Z}$.

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

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

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

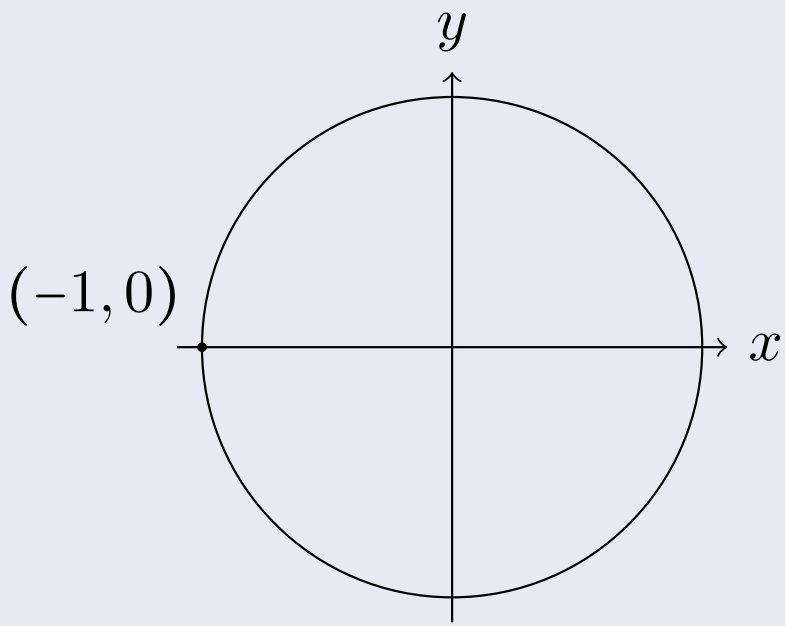
- si p divise $X + iY$ et $X - iY$, alors il divise $2X$ et $2iY$, donc divise 2 : impossible ;
- alors, $X + iY = (u + iv)^2$, et $(X, Y, Z) = (u^2 - v^2, 2uv, u^2 + v^2)$.

On trouve : $(x, y) = \left(\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, $t = \frac{v}{u} \in \mathbb{Q}$.

Exemple introductif

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

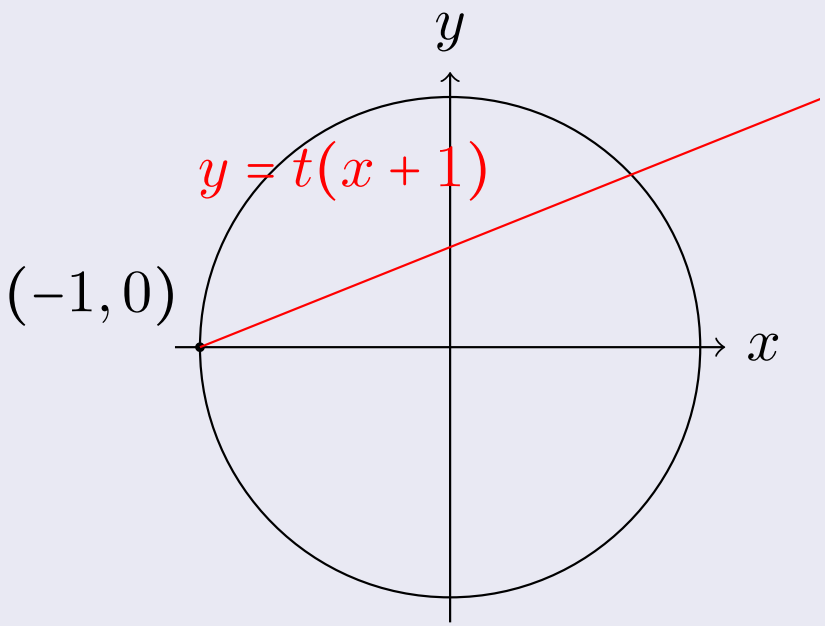
Résolution dans $\mathbb{Q}$: méthode 2



Exemple introductif

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

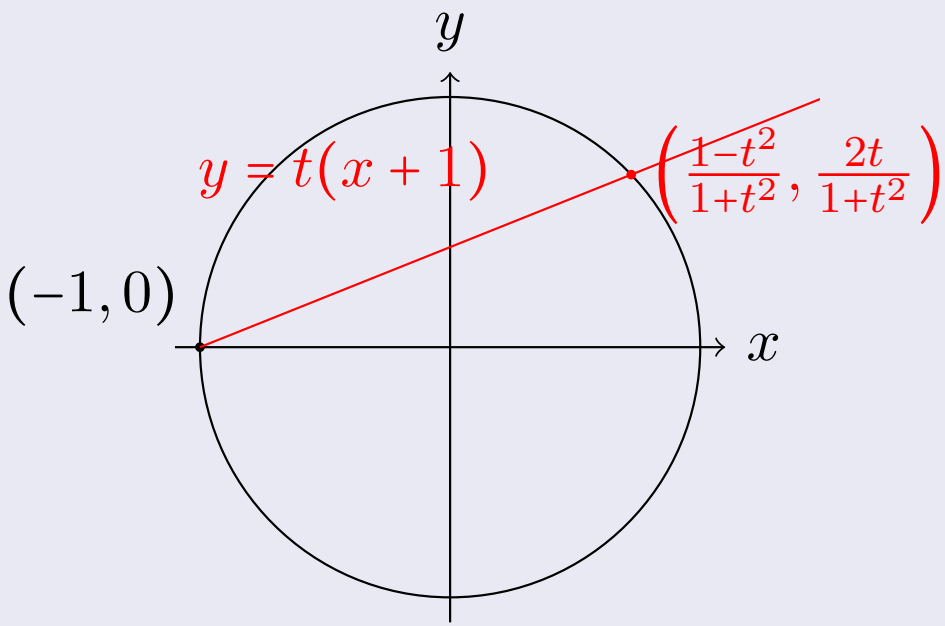
Résolution dans $\mathbb{Q}$: méthode 2



Exemple introductif

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

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



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

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 :

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

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 :

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

Pour tout $c > 0$, l'ensemble

$$\{x \in \mathbb{Q} \mid h(x) \leqslant c\}$$

est fini. La fonction h s'étend à $\bar{\mathbb{Q}}$.

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 ;
- 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 tous $c, d > 0$, l'ensemble

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

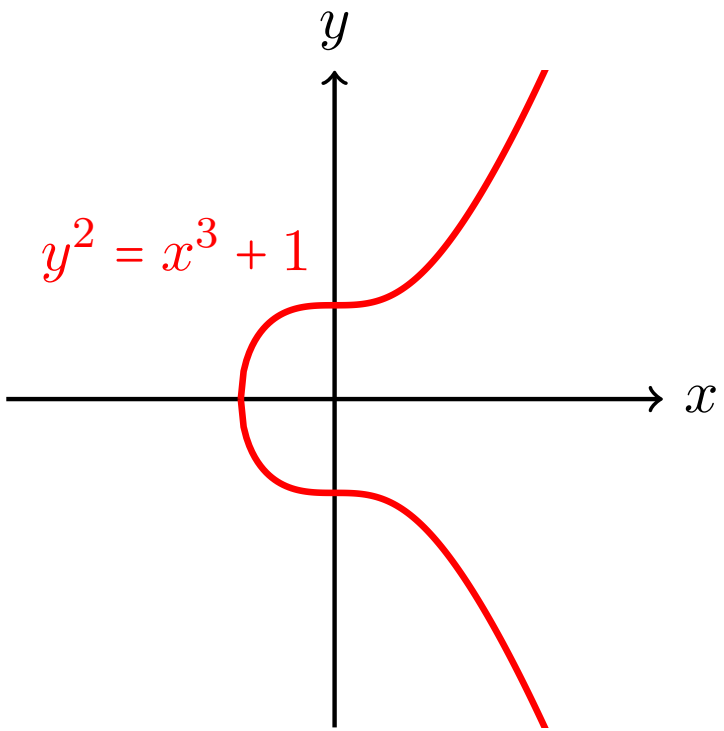
est fini. La fonction h s'étend à $\bar{\mathbb{Q}}$.

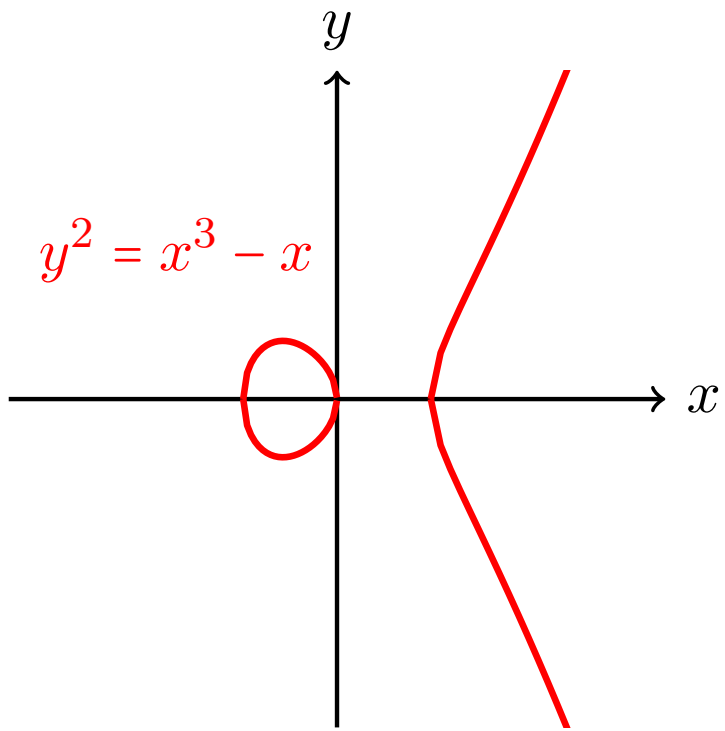
Plan

Courbes elliptiques

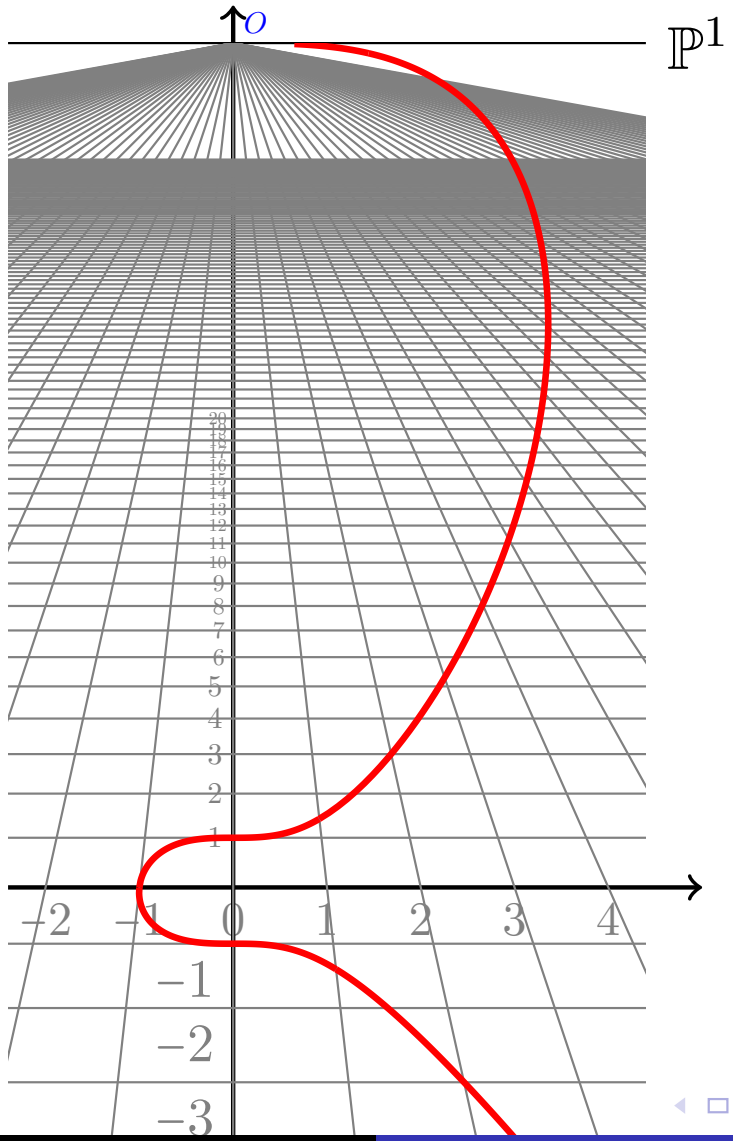
Définition

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





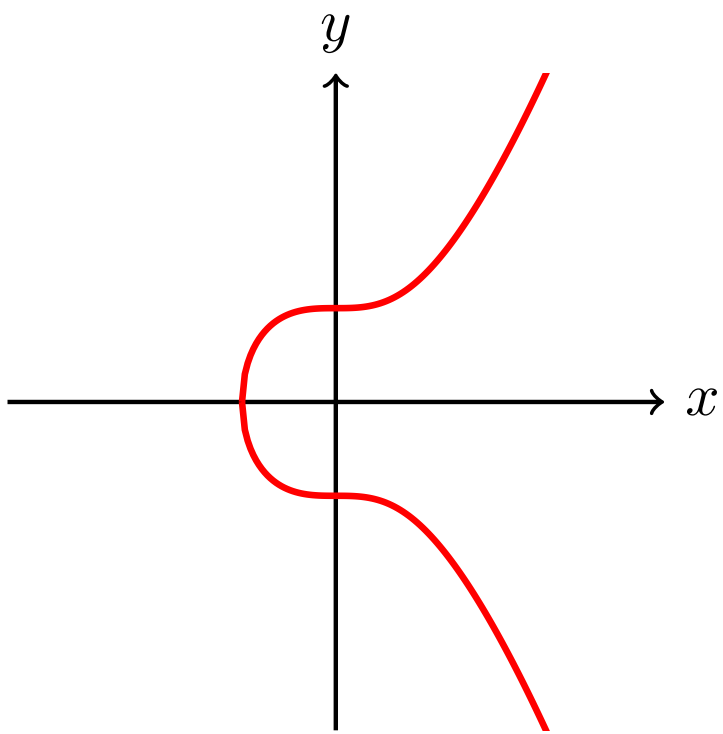
Courbe elliptique projective : $Y^2Z = X^3 + Z^3$.



Courbes elliptiques

loi de groupe et points rationnels

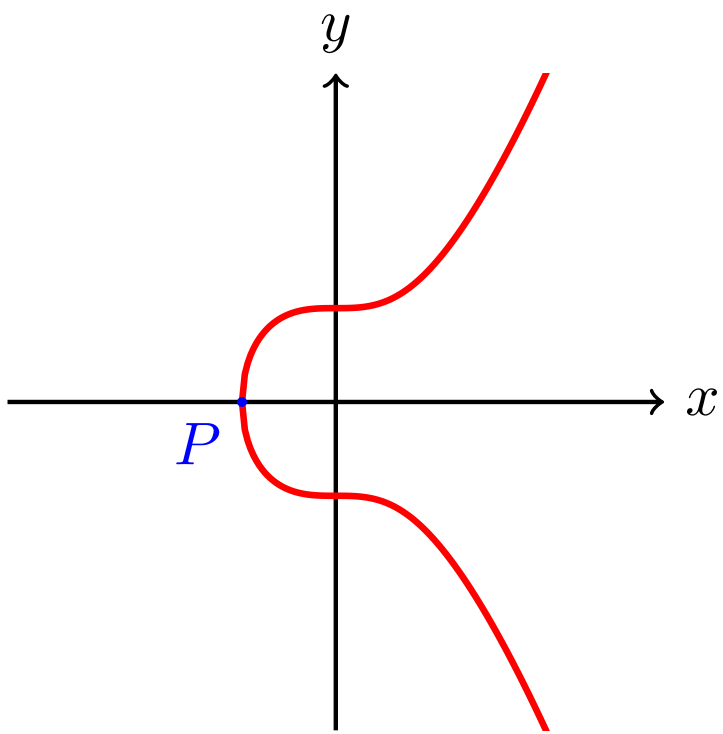
Soit K un corps de nombres. Une courbe elliptique E/K est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ est tel que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



Courbes elliptiques

loi de groupe et points rationnels

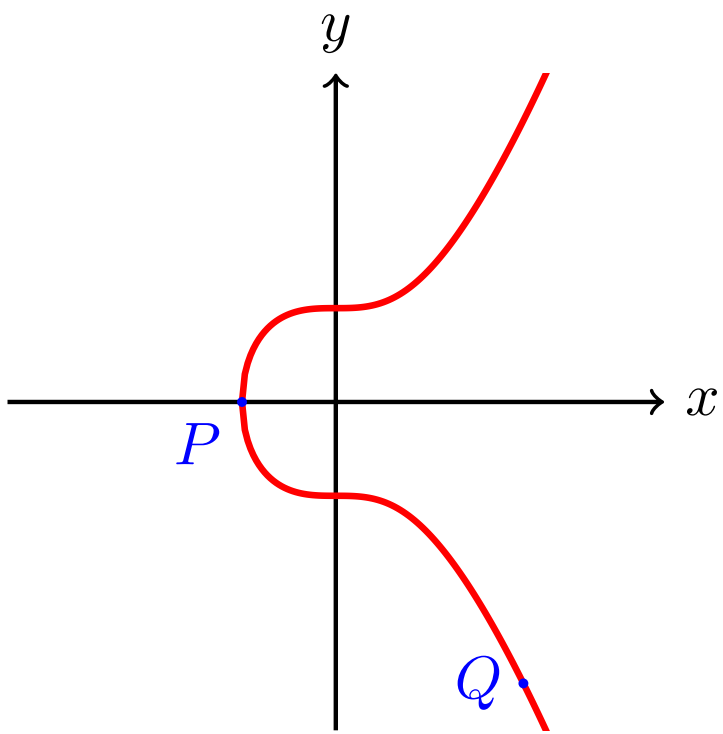
Soit K un corps de nombres. Une courbe elliptique E/K est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ est tel que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



Courbes elliptiques

loi de groupe et points rationnels

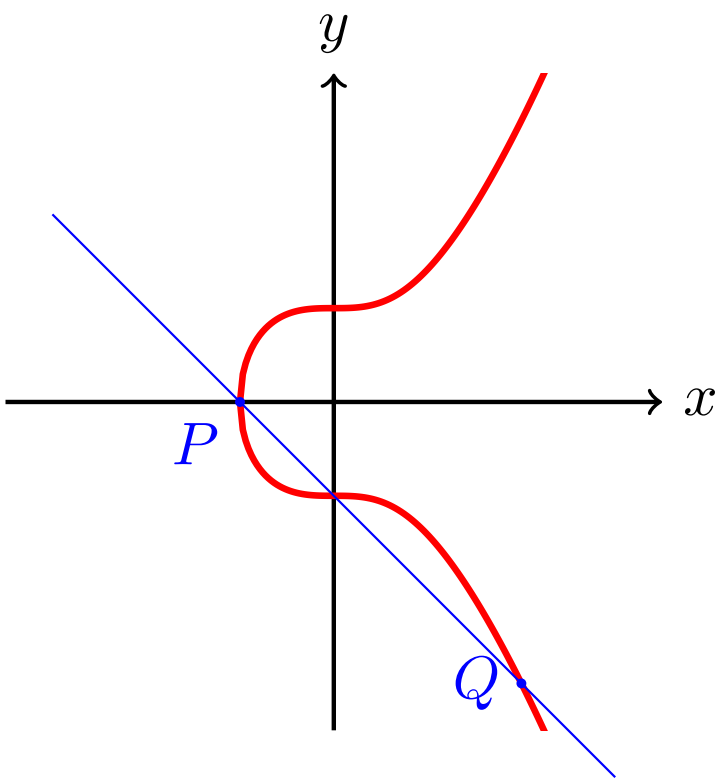
Soit K un corps de nombres. Une courbe elliptique E/K est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ est tel que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



Courbes elliptiques

loi de groupe et points rationnels

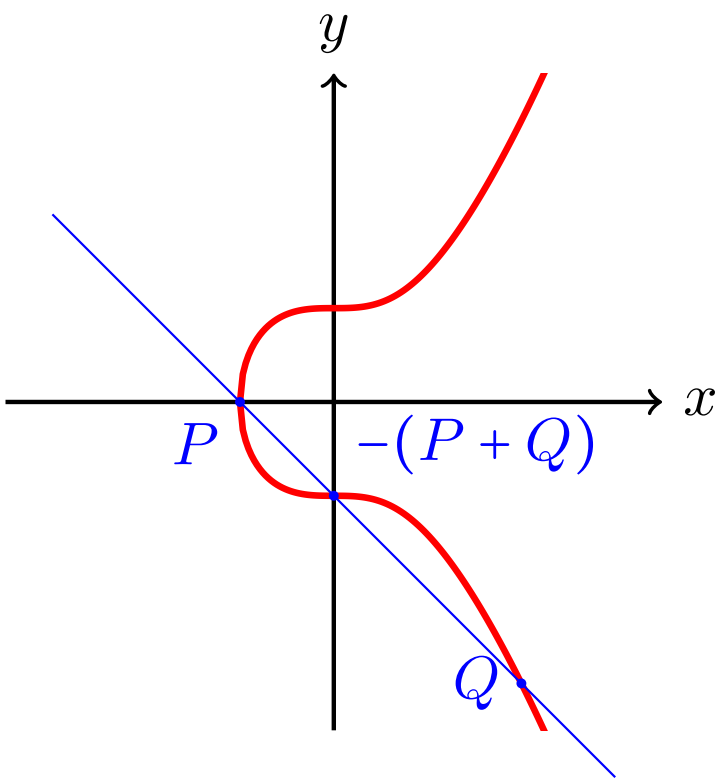
Soit K un corps de nombres. Une courbe elliptique E/K est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ est tel que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



Courbes elliptiques

loi de groupe et points rationnels

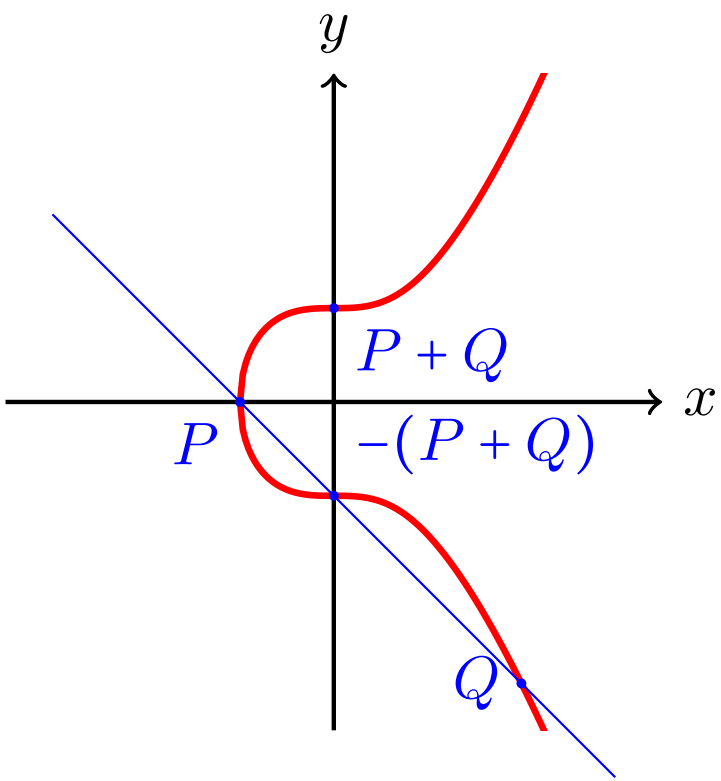
Soit K un corps de nombres. Une courbe elliptique E/K est une courbe d'équation affine $y^2 = x^3 + ax + b$, où $(a, b) \in K^2$ est tel que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



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 $(a, b) \in K^2$ est tel que $4a^3 + 27b^2 \neq 0$, avec en plus un point à l'infini.



Structure

Théorème de Mordell-Weil

Le groupe $(E(K), +)$ a un nombre fini de générateurs : on a $E(K) \simeq \mathbb{Z}^r \times \{\text{torsion}\}$.

Structure

Théorème de Mordell-Weil

Le groupe $(E(K), +)$ a un nombre fini de générateurs : on a $E(K) \simeq \mathbb{Z}^r \times \{\text{torsion}\}$.

Théorème de Siegel

L'ensemble $E(\mathcal{O}_K)$ est fini.

Structure

Théorème de Mordell-Weil

Le groupe $(E(K), +)$ a un nombre fini de générateurs : on a $E(K) \simeq \mathbb{Z}^r \times \{\text{torsion}\}$.

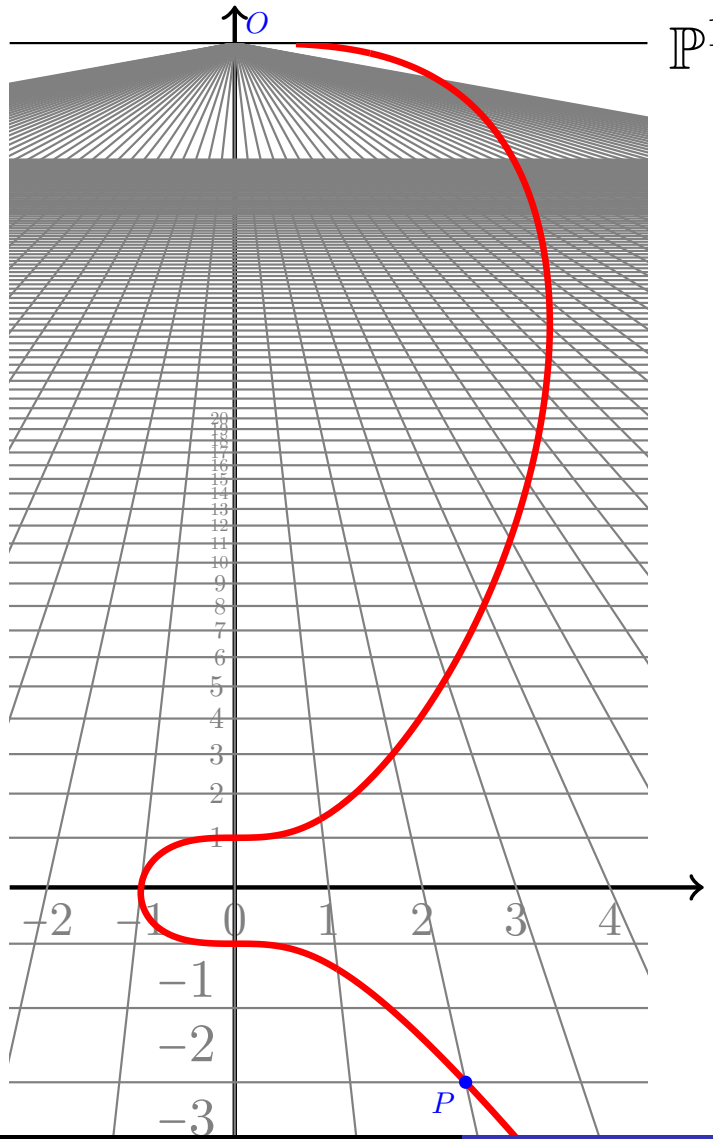
Théorème de Siegel

L'ensemble $E(\mathcal{O}_K)$ est fini.

Théorème d'uniformisation complexe

Le groupe topologique $(E(\mathbb{C}), +)$ est isomorphe à un tore complexe, donc à $\frac{\mathbb{C}}{\mathbb{Z}+\tau\mathbb{Z}}$ pour τ bien choisi tel que $\mathrm{Im}(\tau) > 0$.

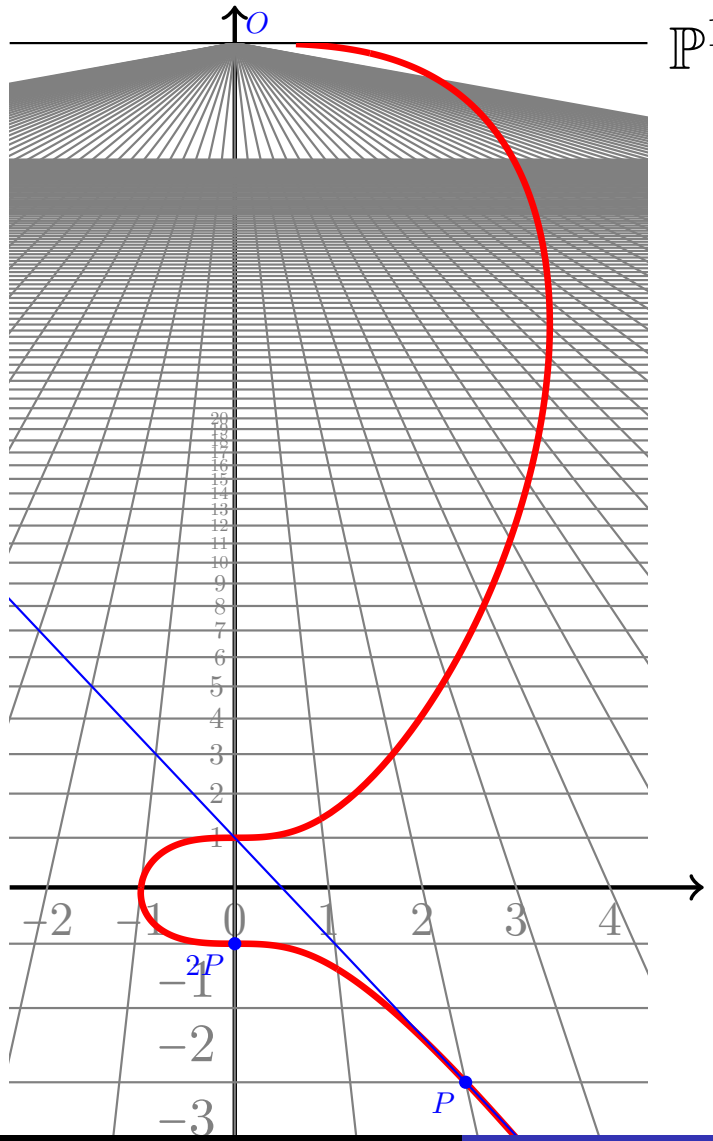
Courbe elliptique d'équation affine $y^2 = x^3 + 1$.



$\mathbb{P}^1$

$(2, -3)$

Courbe elliptique d'équation affine $y^2 = x^3 + 1$.

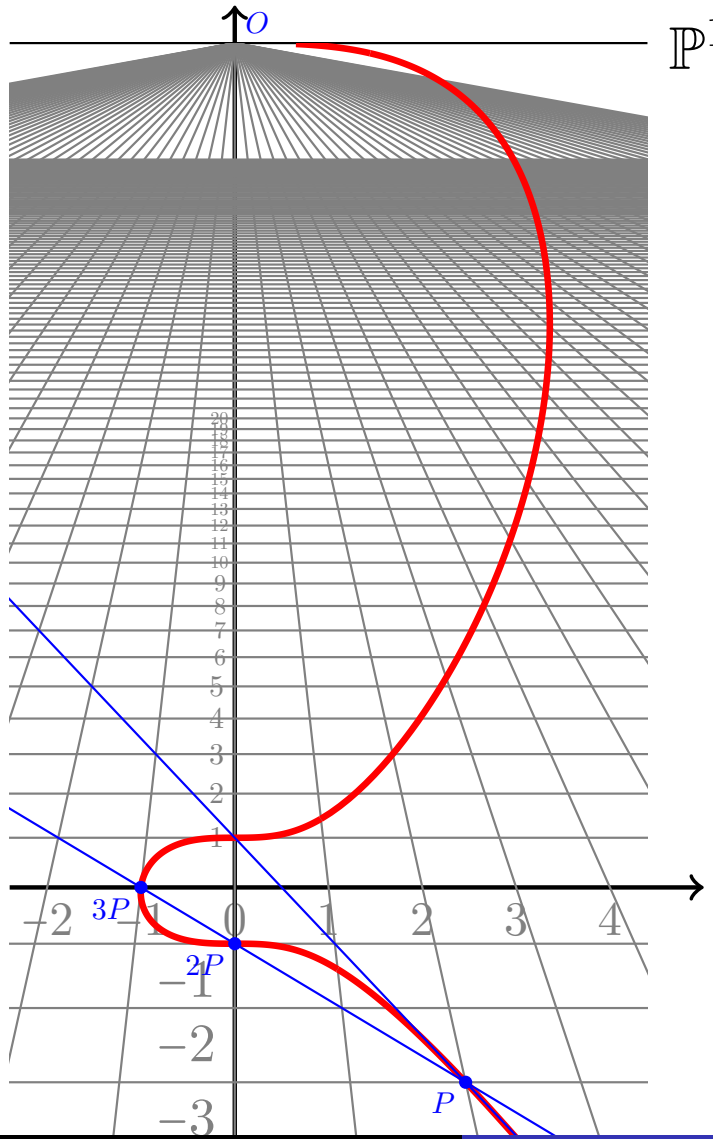


$\mathbb{P}^1$

$(2, -3)$

$(0, -1)$

Courbe elliptique d'équation affine $y^2 = x^3 + 1$.



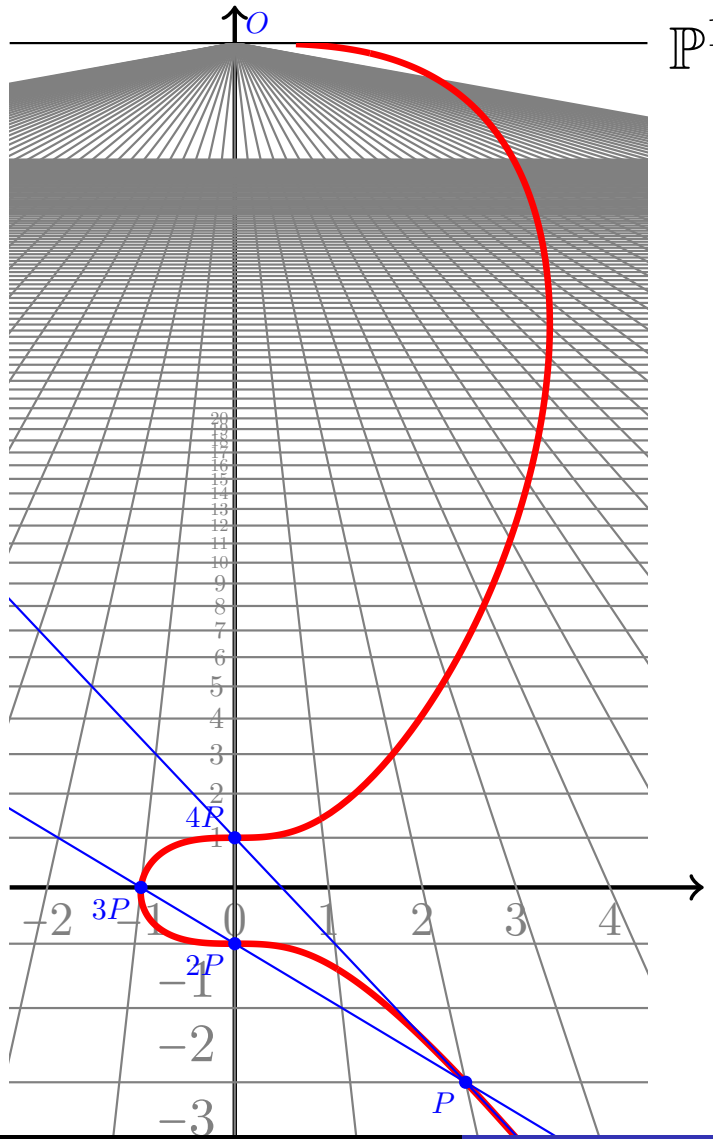
$\mathbb{P}^1$

$(2, -3)$

$(0, -1)$

$(-1, 0)$

Courbe elliptique d'équation affine $y^2 = x^3 + 1$.



$\mathbb{P}^1$

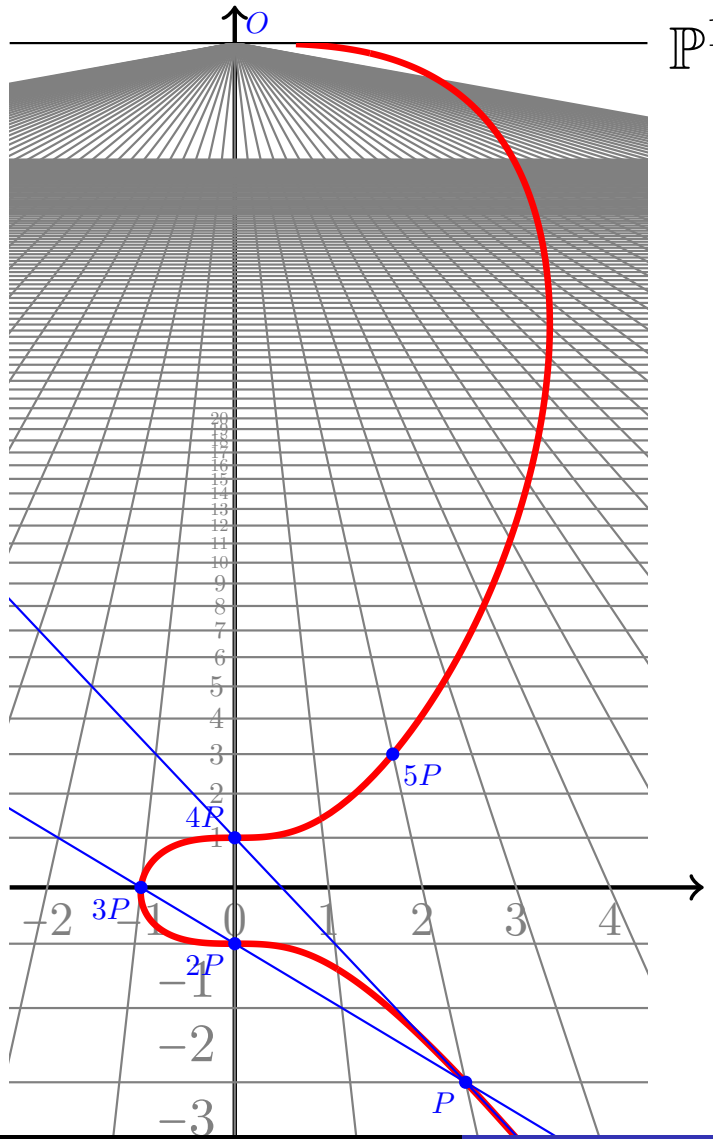
$(2, -3)$

$(0, -1)$

$(-1, 0)$

$(0, 1)$

Courbe elliptique d'équation affine $y^2 = x^3 + 1$.



$\mathbb{P}^1$

$(2, -3)$

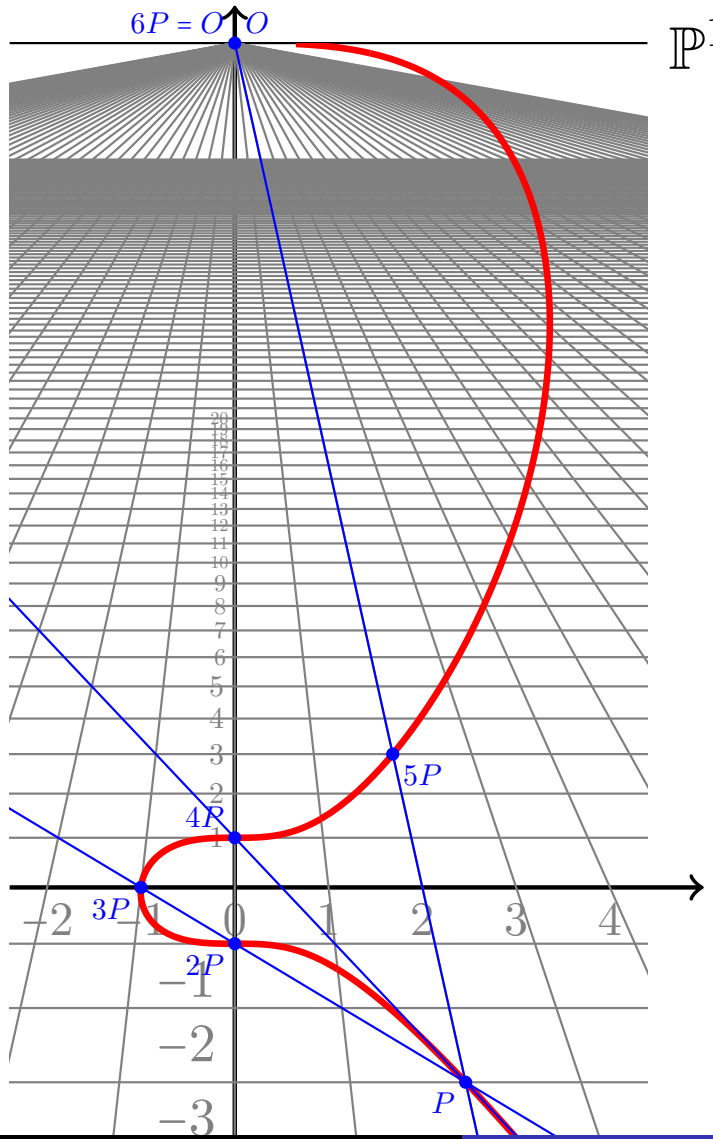
$(0, -1)$

$(-1, 0)$

$(0, 1)$

$(2, 3)$

Courbe elliptique d'équation affine $y^2 = x^3 + 1$.



$\mathbb{P}^1$

$(2, -3)$

$(0, -1)$

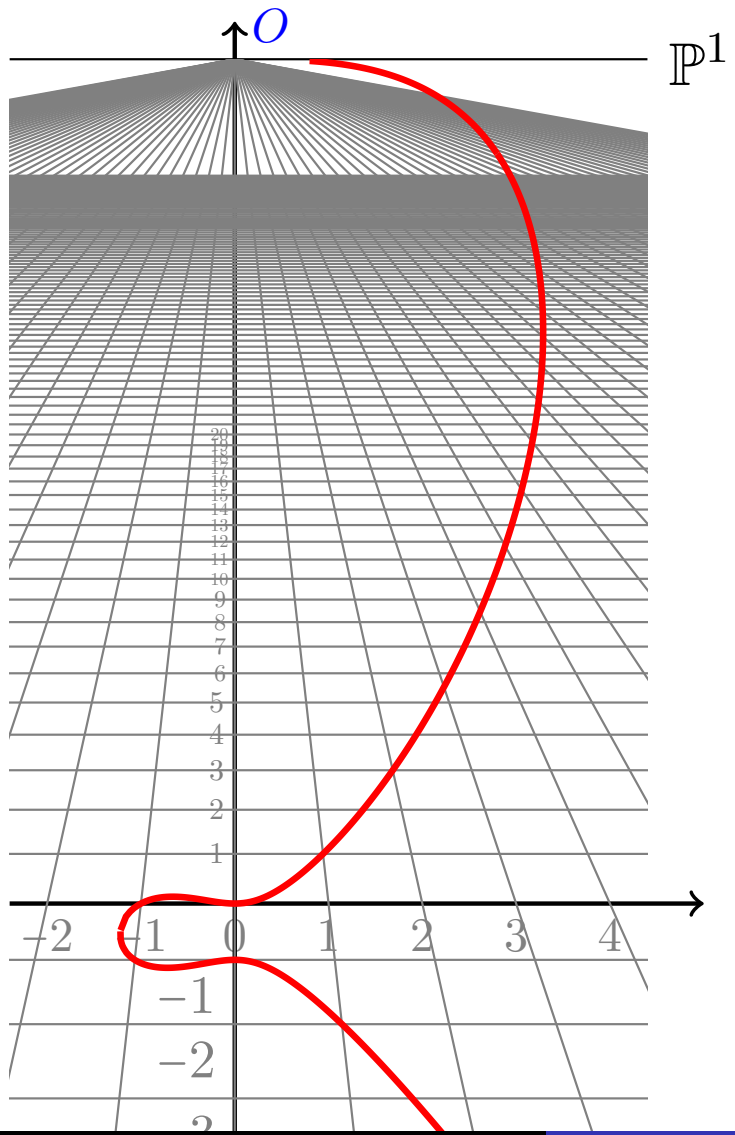
$(-1, 0)$

$(0, 1)$

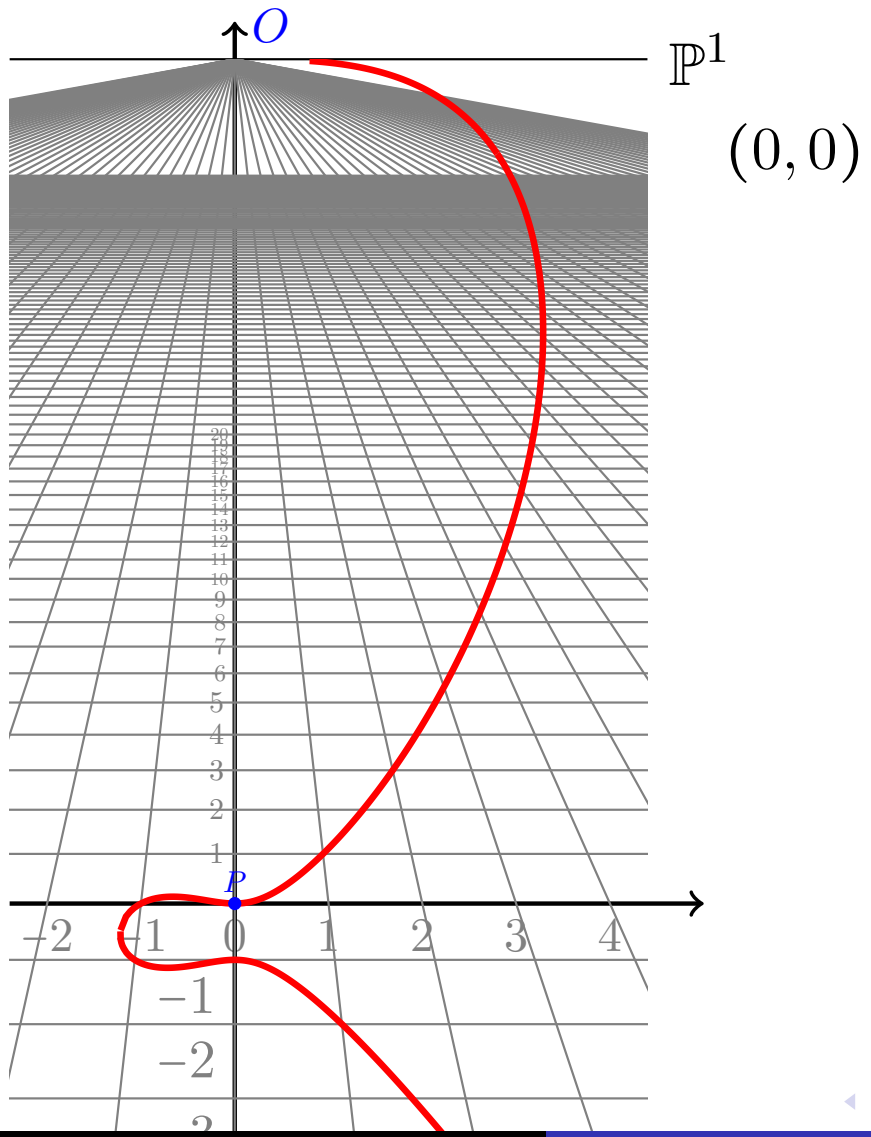
$(2, 3)$

∞

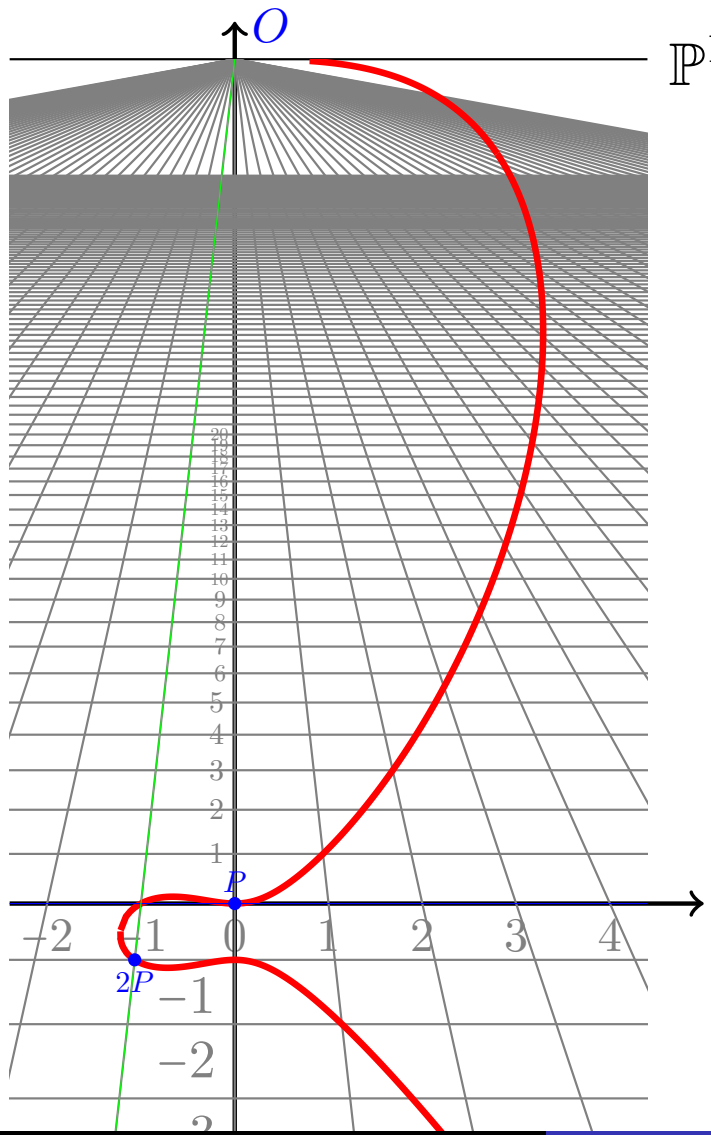
Courbe elliptique d'équation affine $y^2 + y = x^3 + x^2$.



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



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

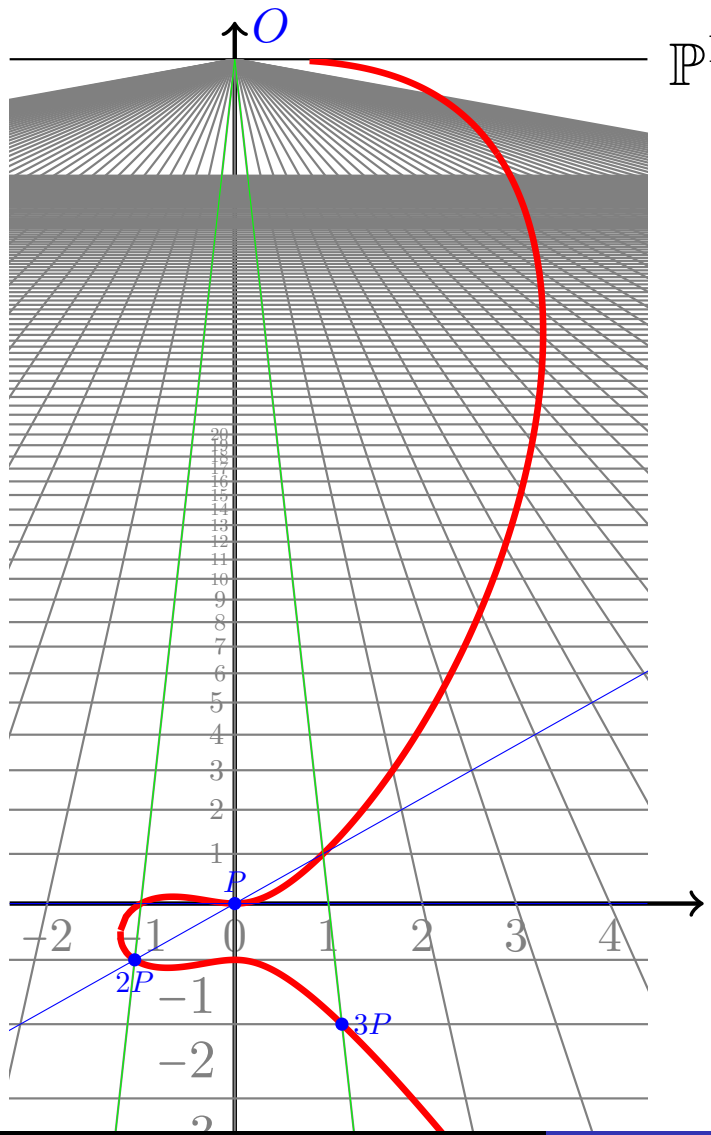


$\mathbb{P}^1$

$(0, 0)$

$(-1, -1)$

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



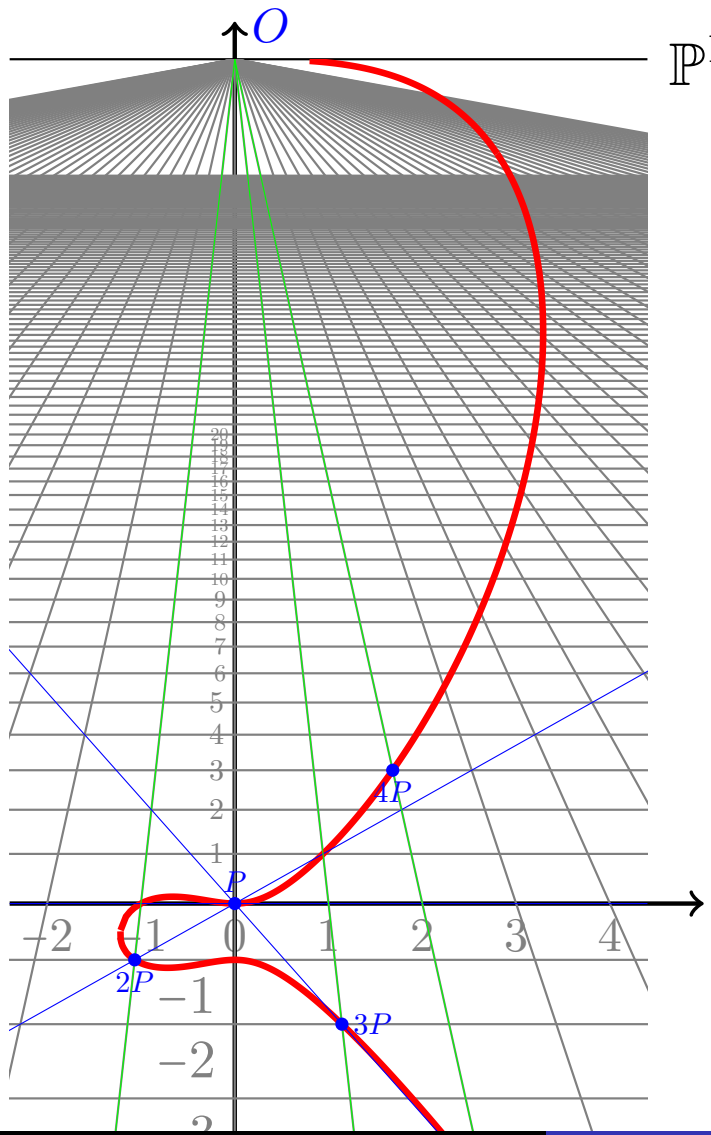
$\mathbb{P}^1$

$(0, 0)$

$(-1, -1)$

$(1, -2)$

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



$\mathbb{P}^1$

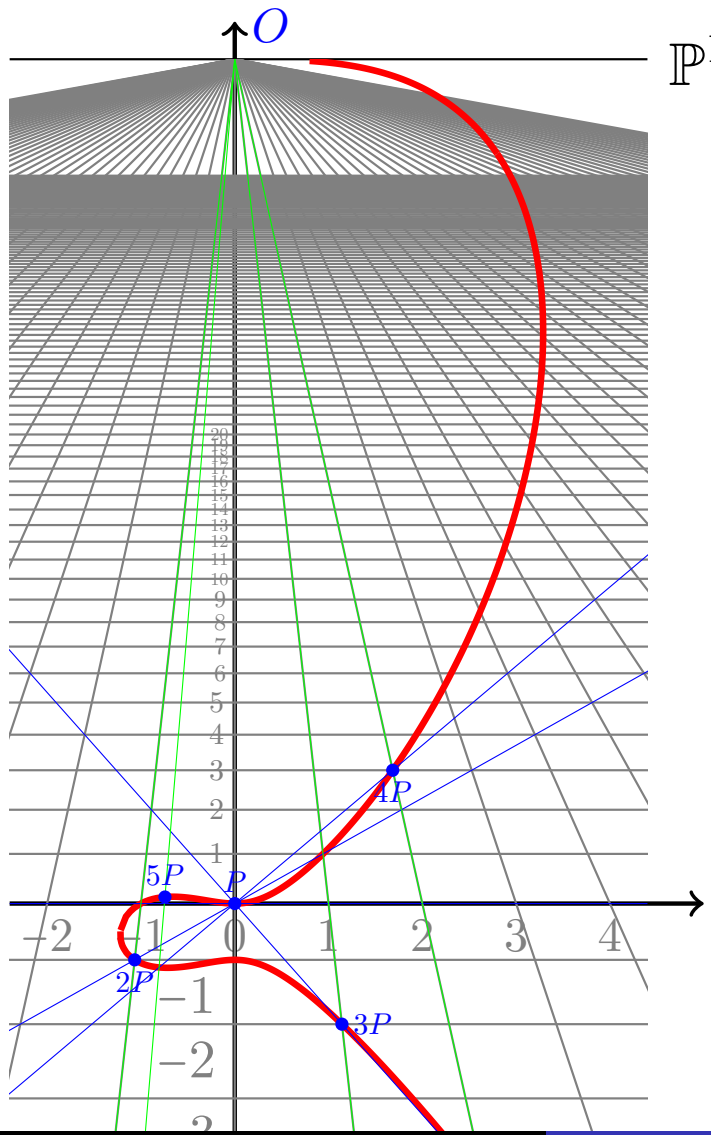
$(0, 0)$

$(-1, -1)$

$(1, -2)$

$(2, 3)$

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



$(0, 0)$

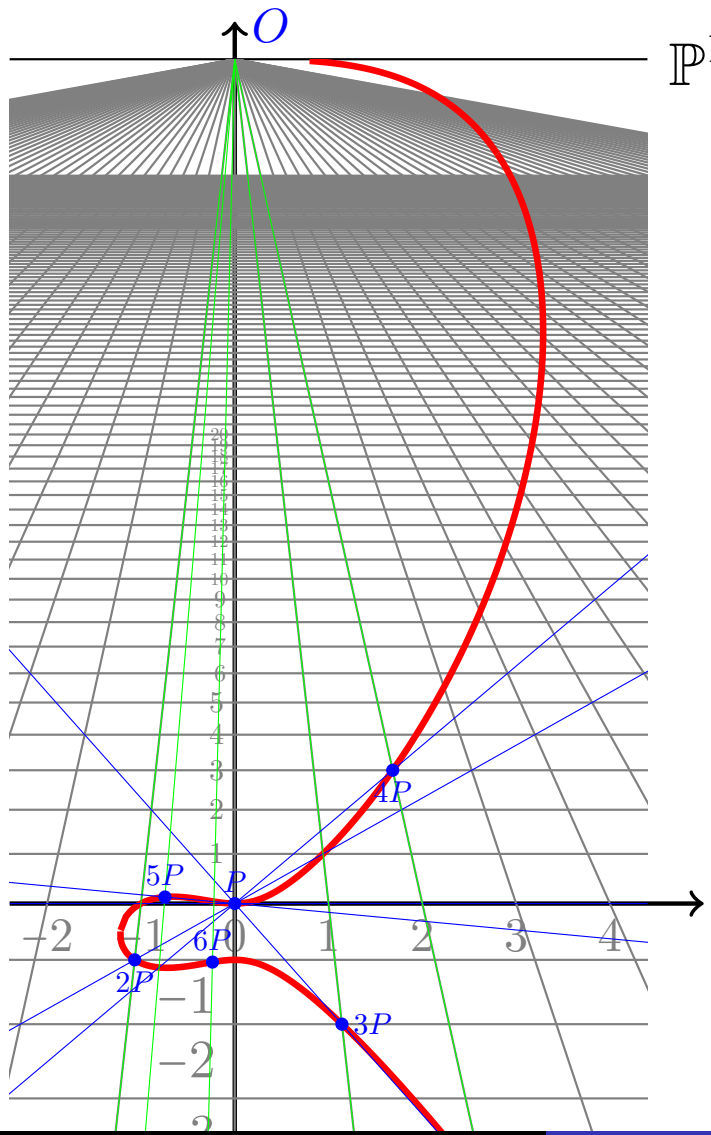
$(-1, -1)$

$(1, -2)$

$(2, 3)$

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

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



$(0, 0)$

$(-1, -1)$

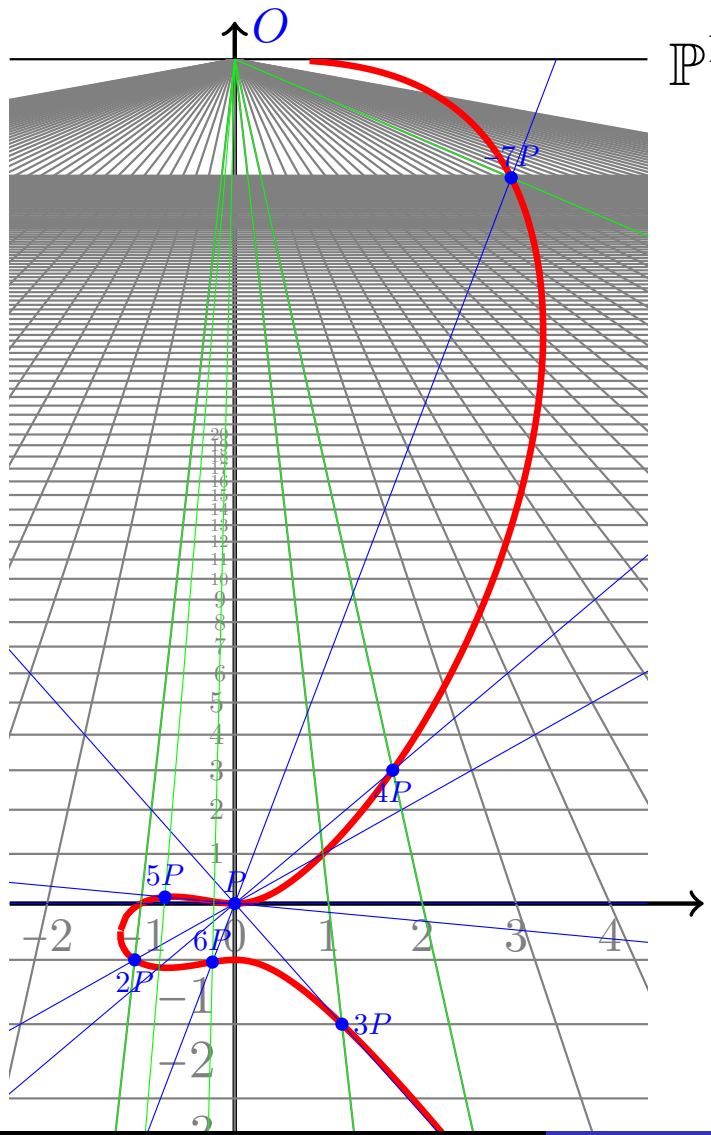
$(1, -2)$

$(2, 3)$

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

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

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



$\mathbb{P}^1$

$(0,0)$

$(-1,-1)$

$(1,-2)$

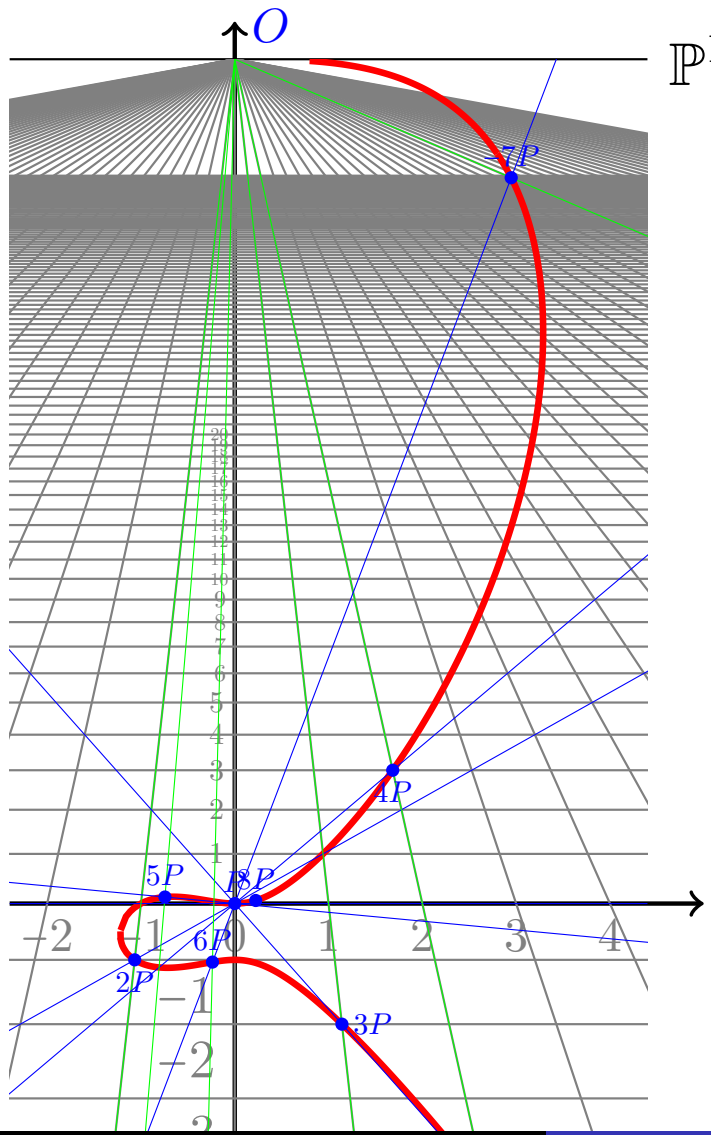
$(2,3)$

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

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

$(21,98)$

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



$\mathbb{P}^1$

$(0, 0)$

$(-1, -1)$

$(1, -2)$

$(2, 3)$

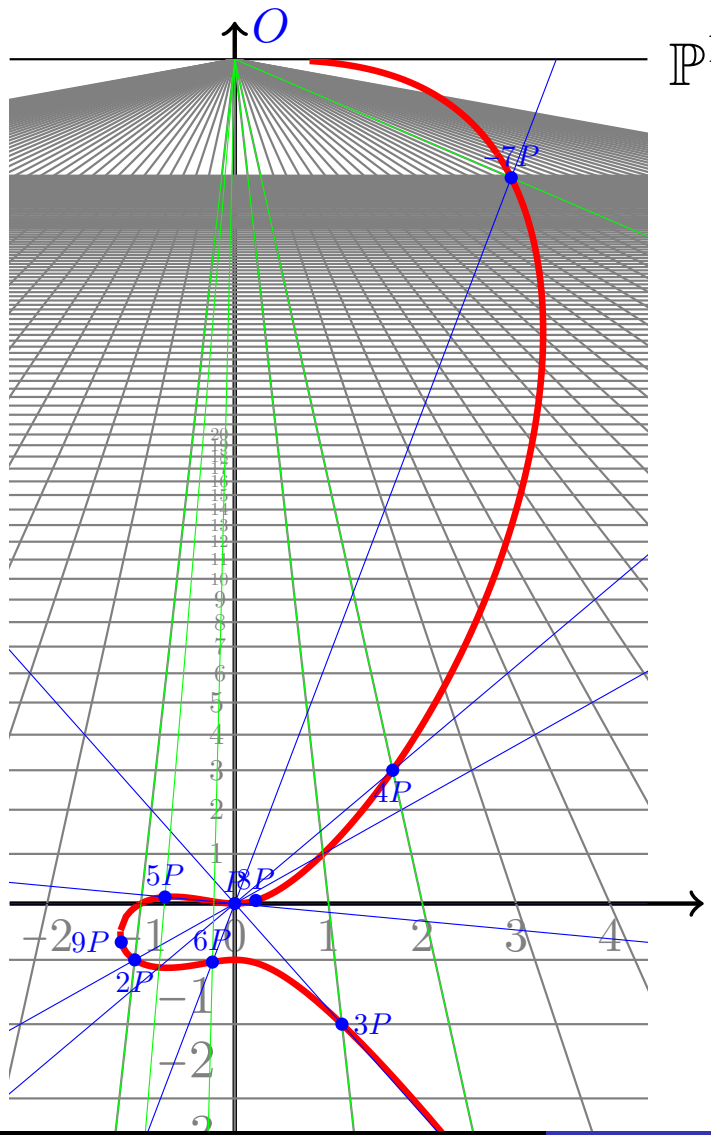
$\left(-\frac{3}{4}, \frac{1}{8}\right)$

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

$(21, 98)$

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

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



$\mathbb{P}^1$

$(0, 0)$

$(-1, -1)$

$(1, -2)$

$(2, 3)$

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

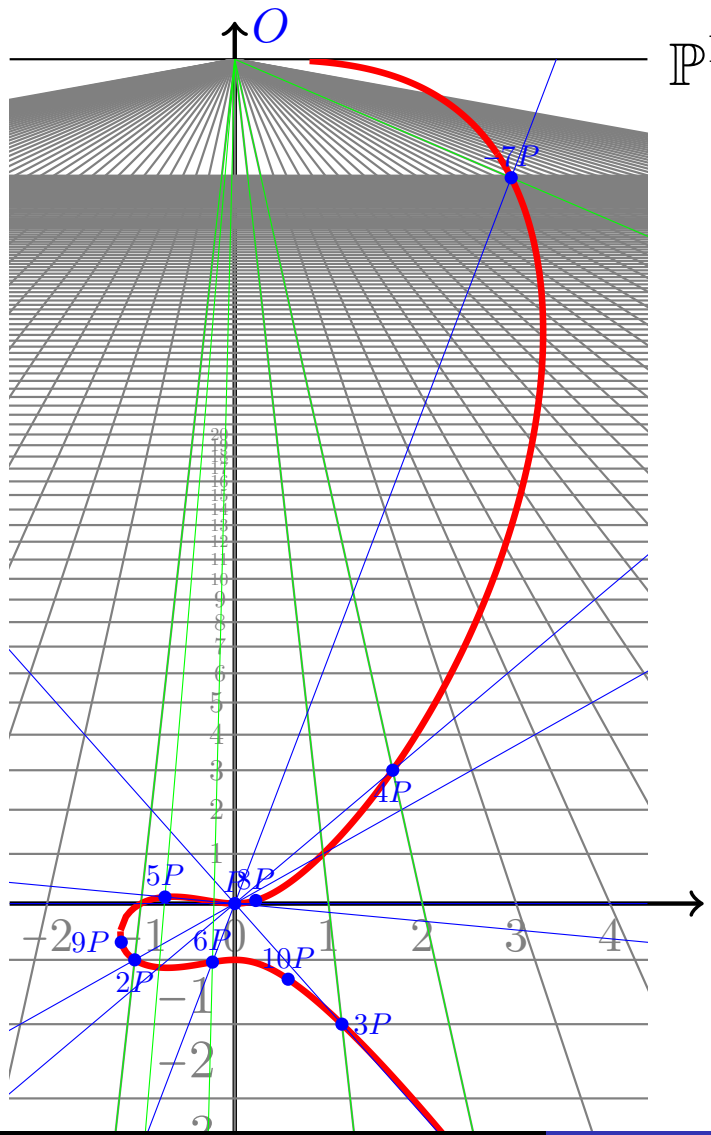
$\left(-\frac{2}{9}, -\frac{28}{27}\right)$

$(21, 98)$

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

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

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 $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, et $h(O) = 0$.

Soit $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, et $h(O) = 0$.

On a :

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

Soit $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, 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 $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, 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 tout $c > 0$, l'ensemble $\{P \in E(\mathbb{Q}) \mid h(P) \leqslant c\}$ est fini ;

Soit $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, 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 tout $c > 0$, l'ensemble $\{P \in E(\mathbb{Q}) \mid h(P) \leqslant c\}$ est fini ;

Soit $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, 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 tout $c > 0$, l'ensemble $\{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leqslant c\}$ est fini ;

Soit $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, 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 tout $c > 0$, l'ensemble $\{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leqslant c\}$ est fini ;
- $\hat{h}(P) = 0$ si, et seulement si P est de torsion.

Soit $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, et $h(O) = 0$. On peut étendre h à $E(\bar{K})$. 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 tout $c > 0$, l'ensemble $\{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leqslant c\}$ est fini ;
- $\hat{h}(P) = 0$ si, et seulement si P est de torsion.

Soit $E/\mathbb{Q}$ une courbe elliptique. Pour $P\left(\frac{a}{b}, \frac{c}{d}\right) \in E(\mathbb{Q})$, on pose $h(P) = \ln(\max(|a|, |b|))$, et $h(O) = 0$. On peut étendre h à $E(\bar{K})$. On définit alors la hauteur canonique comme suit :

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

On a :

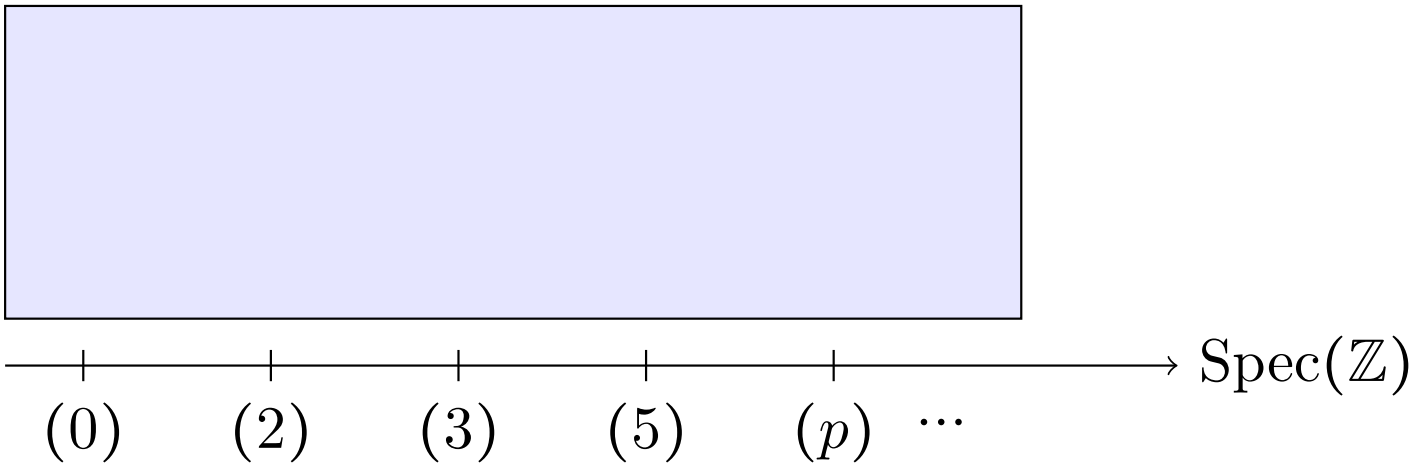
- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2(\hat{h}(P) + \hat{h}(Q))$;
- $\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P)$ pour $\phi \in \mathrm{End}(E)$;
- $\hat{h}(nP) = n^2 \cdot \hat{h}(P)$ pour $n \in \mathbb{Z}$;
- pour tous $c, d > 0$, l'ensemble $\{P \in E(\bar{K}) \mid \hat{h}(P) \leqslant c, [K(P) : K] \leqslant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

Plan

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

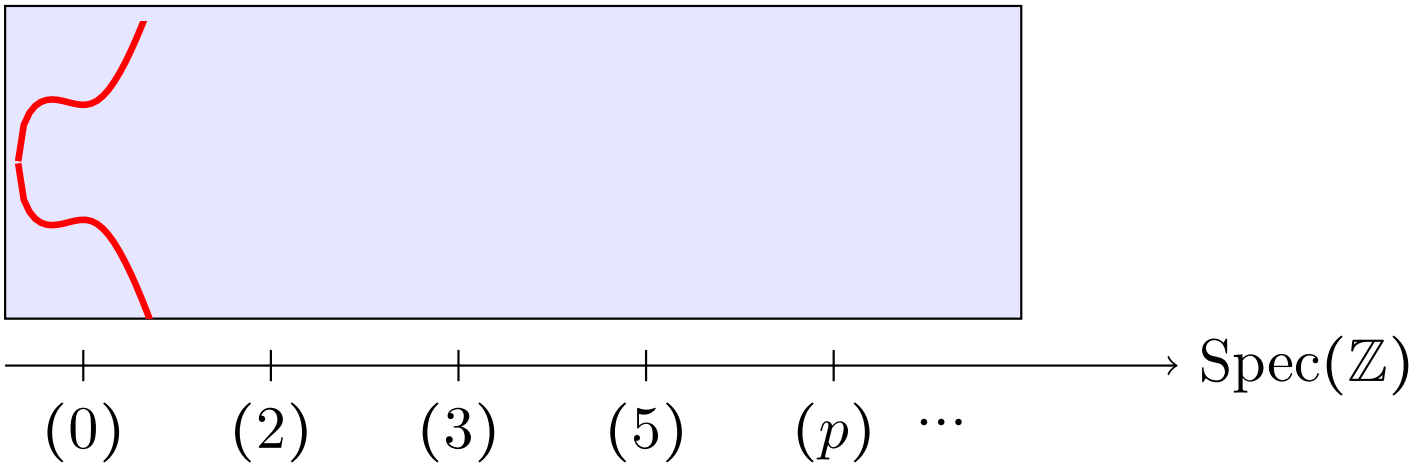
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

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



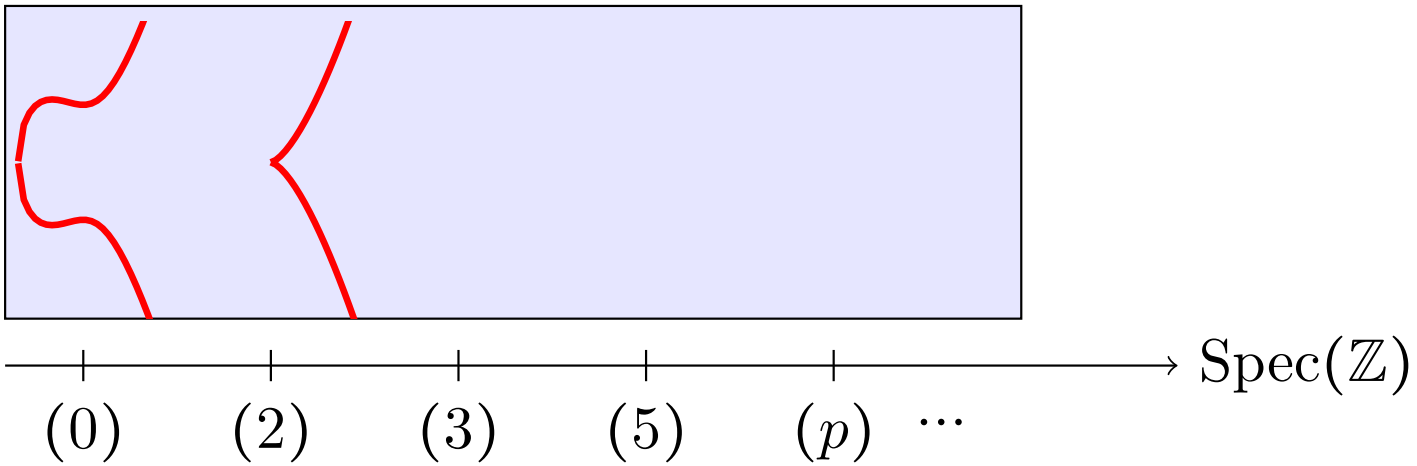
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

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



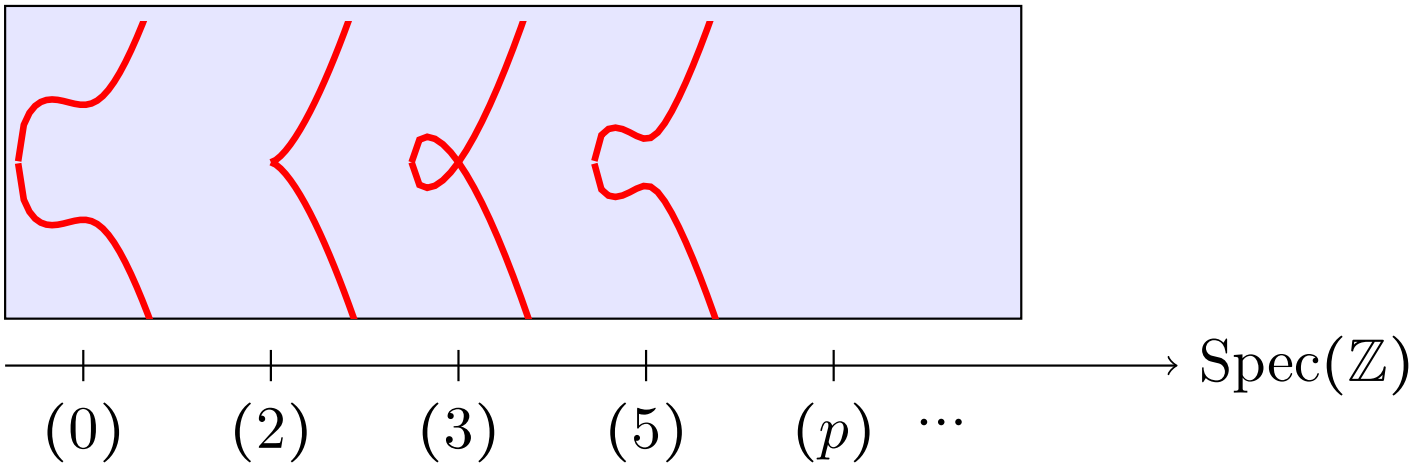
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

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



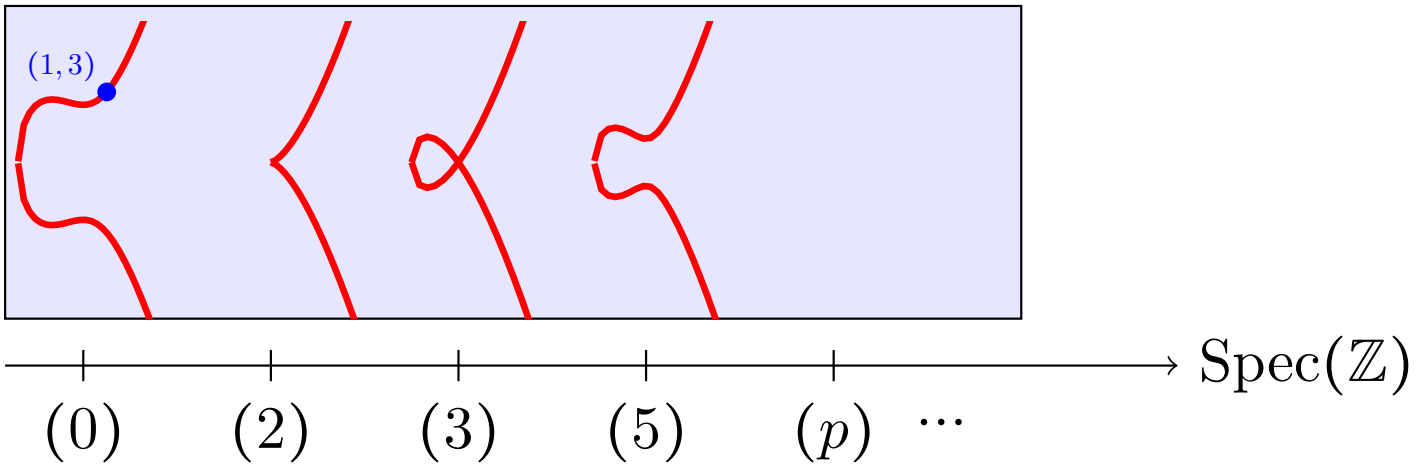
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

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



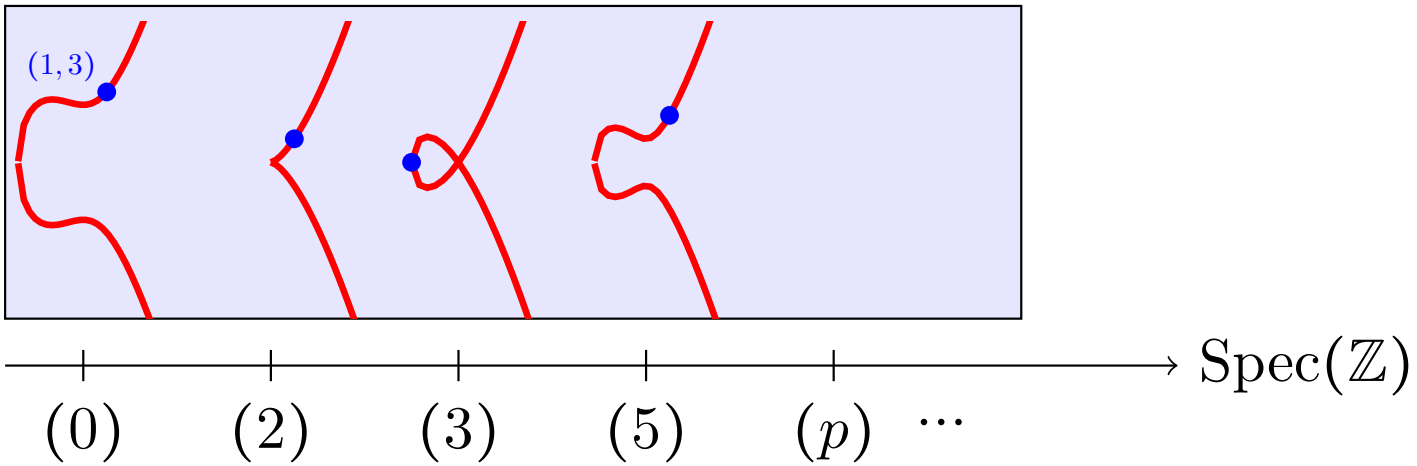
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

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



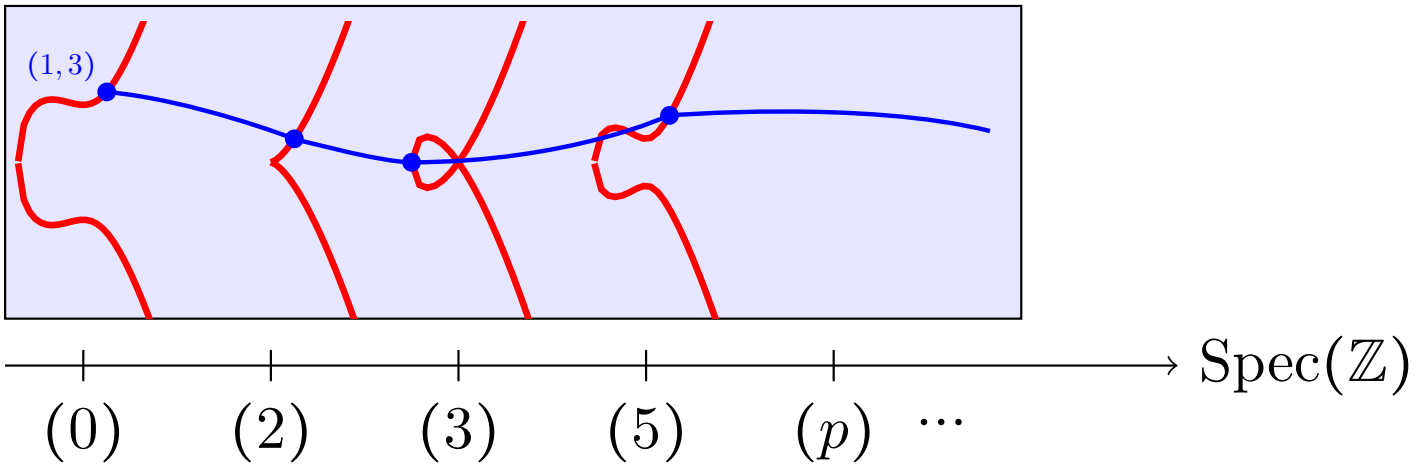
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

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



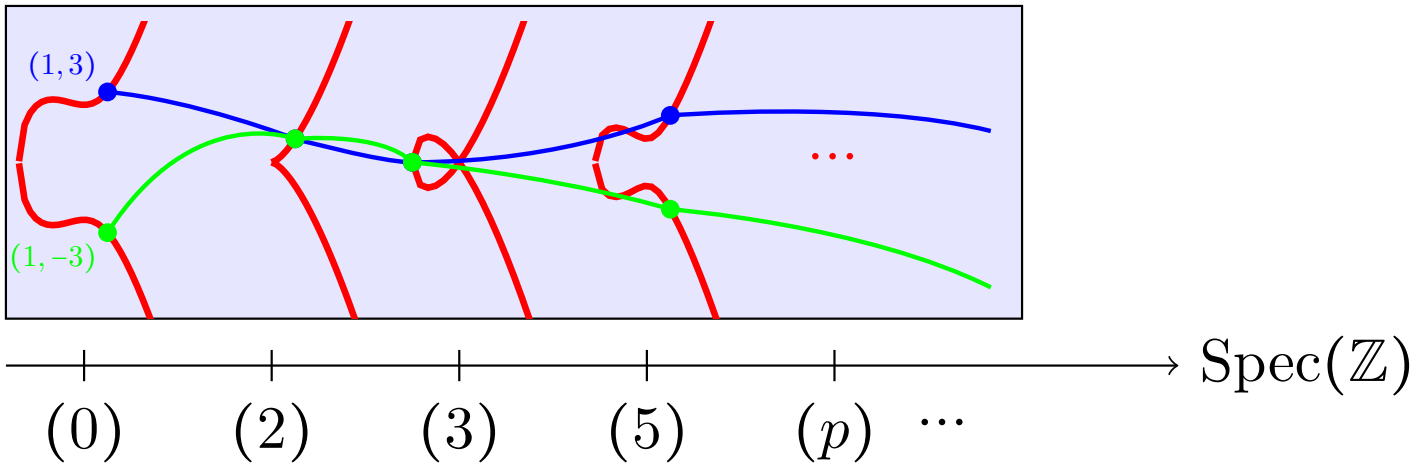
Soit $\mathcal{X}/\mathcal{O}_K$ une surface arithmétique.

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



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

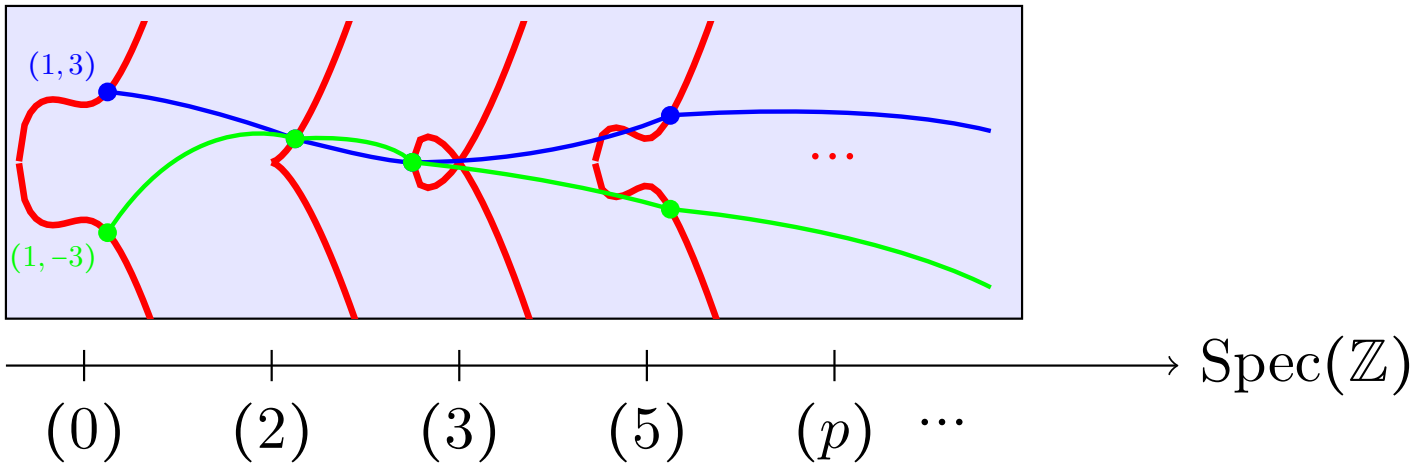
Soient $\mathcal{P}_1$ et $\mathcal{P}_2$ deux sections distinctes de $\mathcal{X}/\mathcal{O}_K$, soient $\mathfrak{p}$ un idéal premier et $x \in \mathcal{X}_\mathfrak{p}$. On pose :

- $\langle \mathcal{P}_1, \mathcal{P}_2 \rangle_x = (\text{mult. d'intersection en } x) \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}))$;
- $\langle \mathcal{P}_1, \mathcal{P}_2 \rangle_\mathfrak{p} = \sum_{x \in \mathcal{X}_\mathfrak{p}} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_x$.

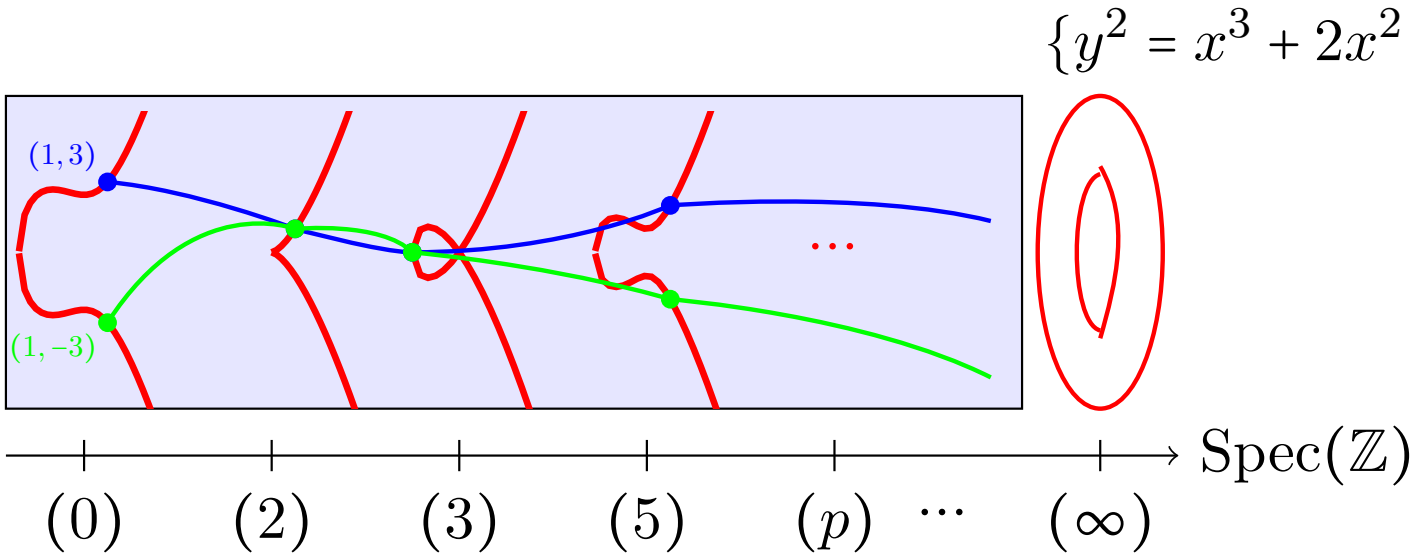
On pose alors $\langle \mathcal{P}_1, \mathcal{P}_2 \rangle = \sum_{\mathfrak{p} \subseteq K} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_\mathfrak{p}$.

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

Si $\mathcal{P}_1$ et $\mathcal{P}_2$ sont deux sections distinctes, alors :

$$\langle \mathcal{P}_1, \mathcal{P}_2 \rangle_\sigma = -g_\sigma(P_1^\sigma, P_2^\sigma)$$

où g_σ est la fonction de Green-Arakelov sur la surface de Riemann $(\mathcal{X} \otimes_\sigma \mathbb{C})(\mathbb{C})$ (on a $g_\sigma(P_1^\sigma, P_2^\sigma) \sim \ln(|P_1^\sigma - P_2^\sigma|_\sigma)$).

Intersection aux places infinies

Si $\mathcal{P}_1$ et $\mathcal{P}_2$ sont deux sections distinctes, alors :

$$\langle \mathcal{P}_1, \mathcal{P}_2 \rangle_\sigma = -g_\sigma(P_1^\sigma, P_2^\sigma)$$

où g_σ est la fonction de Green-Arakelov sur la surface de Riemann $(\mathcal{X} \otimes_\sigma \mathbb{C})(\mathbb{C})$ (on a $g_\sigma(P_1^\sigma, P_2^\sigma) \sim \ln(|P_1^\sigma - P_2^\sigma|_\sigma)$).

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 symétrique, continue (pour la topologie v-adique), localement bornée et diverge ainsi quand $\mathcal{P}_1$ tend vers $\mathcal{P}_2$:

$$\langle \mathcal{P}_1, \mathcal{P}_2 \rangle_v \sim -n_v \ln(|P_1 - P_2|_v).$$

On pose alors :

$$\langle \mathcal{P}_1, \mathcal{P}_2 \rangle = \sum_{\mathfrak{p} \subseteq K} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_{\mathfrak{p}} + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_{\sigma}$$

On pose alors :

$$\begin{aligned}\langle \mathcal{P}_1, \mathcal{P}_2 \rangle &= \sum_{\mathfrak{p} \subseteq K} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_{\mathfrak{p}} + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_{\sigma} \\ &= \sum_{v \in M_K^0} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_v + \sum_{v \in M_K^\infty} n_v \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_v .\end{aligned}$$

On pose alors :

$$\begin{aligned}\langle \mathcal{P}_1, \mathcal{P}_2 \rangle &= \sum_{\mathfrak{p} \subseteq K} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_{\mathfrak{p}} + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_{\sigma} \\ &= \sum_{v \in M_K^0} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_v + \sum_{v \in M_K^\infty} n_v \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_v .\end{aligned}$$

Cet accouplement bilinéaire se prolonge, et définit un accouplement d'intersection $\langle \cdot, \cdot \rangle : \widehat{\mathrm{Cl}(\mathcal{X})} \times \widehat{\mathrm{Cl}(\mathcal{X})} \to \mathbb{R}$.

Lien entre hauteur et intersection

Soient E/K avec bonne réduction partout, et $\mathcal{E} \to B$ son modèle minimal régulier. Pour tout point $P \in E(K)$ d'adhérence $\mathcal{P}$ dans $\mathcal{E}$, on a :

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

Deux applications

Soit E/K une courbe elliptique ayant bonne réduction partout.

Deux applications

Soit E/K une courbe elliptique ayant bonne réduction partout.

Hindry-Silverman (1999)

On a $\mathrm{card}(E(K)_{\mathrm{tors}}) \leqslant 1977408 n_K \ln(n_K)$, où $n_K = [K : \mathbb{Q}]$.

Deux applications

Soit E/K une courbe elliptique ayant bonne réduction partout.

Hindry-Silverman (1999)

On a $\mathrm{card}(E(K)_{\mathrm{tors}}) \leqslant 1977408 n_K \ln(n_K)$, où $n_K = [K : \mathbb{Q}]$.

Laurent (1979), W. (2015)

Supposons que $\mathbb{Z} \subsetneq \mathrm{End}(E)$. Pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré relatif $D = [K(P) : K]$, on a :

$$\hat{h}(P) \geqslant \frac{c_K}{D} \left(\frac{\ln(\ln(4D))}{\ln(4D)} \right)^3$$

où $c_K \gg n_K^{-20}$ si HRG (il existe une version inconditionnelle).

Plan

Nous voulons montrer qu'il existe un entier $N \geqslant 1$ tel que :

$$(\forall k \in [\![1, N]\!] \quad kP \neq O) \Rightarrow \hat{h}(P) > 0.$$

Nous voulons montrer qu'il existe un entier $N \geqslant 1$ tel que :

$$(\forall k \in [\![1, N]\!] \quad kP \neq O) \Rightarrow \hat{h}(P) > 0.$$

Nous avons vu que $\hat{h}(P) = 0 \Leftrightarrow P$ est de torsion.

Corollaire

Si P est de torsion, alors son ordre de torsion est inférieur à N.

Nous voulons montrer qu'il existe un entier $N \geqslant 1$ tel que :

$$(\forall k \in [\![1, N]\!] \quad kP \neq O) \Rightarrow \hat{h}(P) > 0.$$

Nous avons vu que $\hat{h}(P) = 0 \Leftrightarrow P$ est de torsion.

Corollaire

Si P est de torsion, alors son ordre de torsion est inférieur à N.

Point de départ : pour tout $k \in [\![1, N]\!]$, on a

$$k^2 \hat{h}(P) = \hat{h}(kP) = \frac{\langle k\mathcal{P}, \mathcal{O} \rangle}{[K : \mathbb{Q}]} \geqslant \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma : K \hookrightarrow \mathbb{C}} \langle k\mathcal{P}, \mathcal{O} \rangle_\sigma,$$

car $\langle k\mathcal{P}, \mathcal{O} \rangle_{\mathfrak{p}} \geqslant 0$ pour $\mathfrak{p}$ idéal premier, par définition.

Points « proches » sur le tore $E(\bar{K}_v)$

Soit v une place archimédienne. On a vu que $E(\bar{K}_v) \simeq \mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z})$ pour un certain $\tau_v \in \mathbb{C}$. Pour tout $P \in E(\bar{K}_v)$, notons $z_v(P) = x_v(P) + y_v(P)\tau_v$ son image dans $\mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z})$.

Si $0 \leqslant x(P-Q), y(P-Q) \leqslant \frac{1}{24}$, alors :

$$\langle P, Q\rangle_v \geqslant \frac{1}{288} J_v,$$

où $J_v = \max(\ln(|j_E|_v, 1))$.

Démonstration du théorème de Hindry-Silverman (1/2)

Soit

$$\mathcal{E} = \{kP \mid 1 \leqslant k \leqslant 24^{2n_K}(M+1)\} \subseteq E(K).$$

Si $kP \neq O$ pour tout $k \in [\![1, 2 \cdot 24^{2n_K}]\!]$, Il existe $k, l \leqslant 2 \cdot 24^{2n_K}$ tels pour toute place v archimédienne :

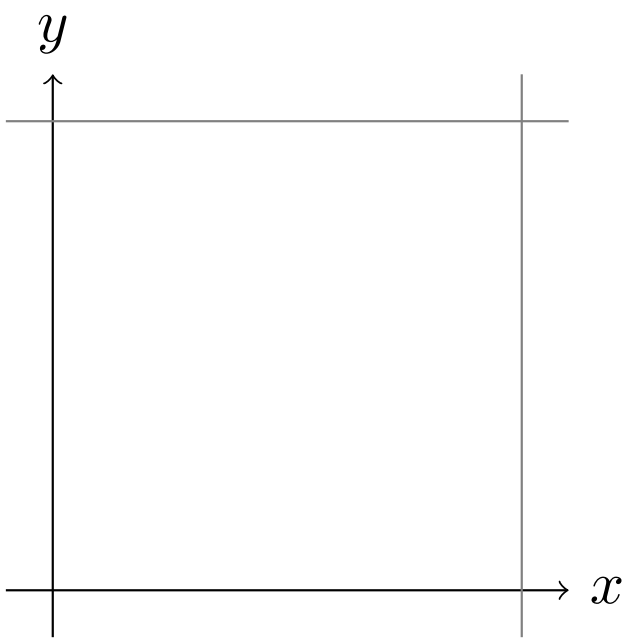
$$\langle kP, lP \rangle_v \geqslant \frac{J_v}{288}$$

Démonstration du théorème de Hindry-Silverman (1/2)

Soit

$$\mathcal{E} = \{kP \mid 1 \leqslant k \leqslant 24^{2n_K}(M+1)\} \subseteq E(K).$$

FIGURE: Exemple avec $\{(x,y) \in \mathbb{C}^2 \mid y^2 = x^3 + x\} \simeq \mathbb{C}/(\mathbb{Z} + i\mathbb{Z})$ $(n_K = 1)$.

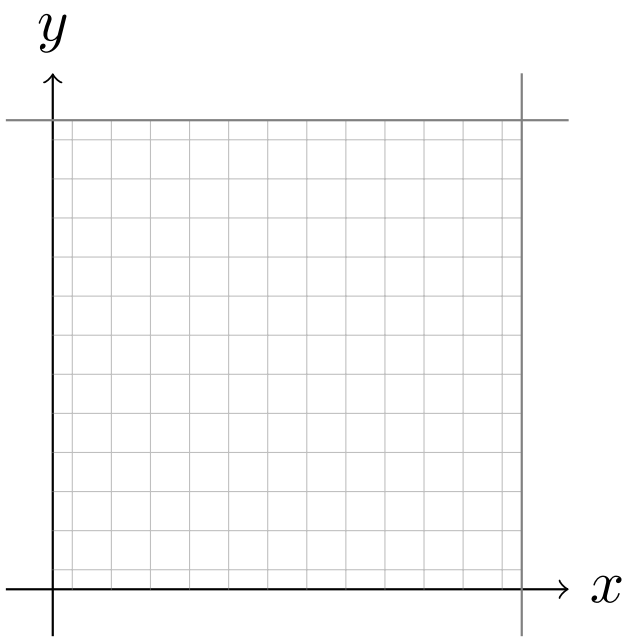


Démonstration du théorème de Hindry-Silverman (1/2)

Soit

$$\mathcal{E} = \{kP \mid 1 \leqslant k \leqslant 24^{2n_K}(M+1)\} \subseteq E(K).$$

FIGURE: Exemple avec $\{(x,y) \in \mathbb{C}^2 \mid y^2 = x^3 + x\} \simeq \mathbb{C}/(\mathbb{Z} + i\mathbb{Z})$ $(n_K = 1)$.

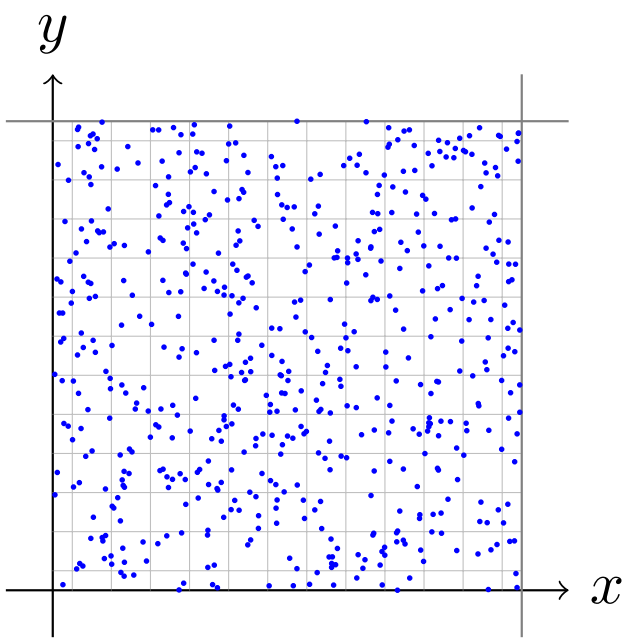


Démonstration du théorème de Hindry-Silverman (1/2)

Soit

$$\mathcal{E} = \{kP \mid 1 \leqslant k \leqslant 24^{2n_K}(M+1)\} \subseteq E(K).$$

FIGURE: Exemple avec $\{(x,y) \in \mathbb{C}^2 \mid y^2 = x^3 + x\} \simeq \mathbb{C}/(\mathbb{Z} + i\mathbb{Z})$ $(n_K = 1)$.



Démonstration du théorème de Hindry-Silverman (1/2)

Soit

$$\mathcal{E} = \{kP \mid 1 \leqslant k \leqslant 24^{2n_K}(M+1)\} \subseteq E(K).$$

Si $kP \neq O$ pour tout $k \in [\![1, 2 \cdot 24^{2n_K}]\!]$, Il existe $k, l \leqslant 2 \cdot 24^{2n_K}$ tels pour toute place v archimédienne :

$$\langle kP, lP \rangle_v \geqslant \frac{J_v}{288}$$

Démonstration du théorème de Hindry-Silverman (1/2)

Soit

$$\mathcal{E} = \{kP \mid 1 \leqslant k \leqslant 24^{2n_K}(M+1)\} \subseteq E(K).$$

Si $kP \neq O$ pour tout $k \in [\![1, 2 \cdot 24^{2n_K}]\!]$, Il existe $k, l \leqslant 2 \cdot 24^{2n_K}$ tels pour toute place v archimédienne :

$$\langle kP, lP \rangle_v \geqslant \frac{J_v}{288}$$

Alors :

$$\hat{h}((k-l)P) \geqslant \frac{1}{n_K} \sum_{v \in M_K^\infty} n_v \langle kP, lP \rangle_v$$

Démonstration du théorème de Hindry-Silverman (1/2)

Soit

$$\mathcal{E} = \{kP \mid 1 \leqslant k \leqslant 24^{2n_K}(M+1)\} \subseteq E(K).$$

Si $kP \neq O$ pour tout $k \in [\![1, 2 \cdot 24^{2n_K}]\!]$, Il existe $k, l \leqslant 2 \cdot 24^{2n_K}$ tels pour toute place v archimédienne :

$$\langle kP, lP \rangle_v \geqslant \frac{J_v}{288}$$

Alors :

$$\begin{aligned}\hat{h}((k-l)P) &\geqslant \frac{1}{n_K} \sum_{v \in M_K^\infty} n_v \langle kP, lP \rangle_v \\ &\geqslant \frac{1}{288}\end{aligned}$$

Démonstration du théorème de Hindry-Silverman (2/2)

On a :

$$\hat{h}((k-l)P) \geqslant \frac{1}{288}$$

Démonstration du théorème de Hindry-Silverman (2/2)

On a :

$$\hat{h}((k-l)P) \geqslant \frac{1}{288}$$

Or $\hat{h}((k-l)P) \leqslant 4 \cdot (2 \cdot 24^{2n_K})\hat{h}(P)$, donc $\hat{h}(P) > 0$.

Démonstration du théorème de Hindry-Silverman (2/2)

On a :

$$\hat{h}((k-l)P) \geqslant \frac{1}{288}$$

Or $\hat{h}((k-l)P) \leqslant 4 \cdot (2 \cdot 24^{2n_K})\hat{h}(P)$, donc $\hat{h}(P) > 0$.

Corollaire

Si P est de torsion, alors son ordre de torsion est inférieur à $2 \cdot 24^{n_K}$.

Théorème

On a :

$$\operatorname{card}\left(\left\{P \in E(K) \mid \hat{h}(P) \leqslant A/n_K\right\}\right) \leqslant 19977408 n_K \ln(n_K),$$

avec $A = 1/164736$.

Théorème

On a :

$$\operatorname{card}\left(\left\{P \in E(K) \mid \hat{h}(P) \leqslant A/n_K\right\}\right) \leqslant 19977408 n_K \ln(n_K),$$

avec $A = 1/164736$.

Corollaire 1

On a $\operatorname{card}(E(K)_{\mathrm{tors}}) \leqslant 1977408 n_K \ln(n_K)$.

Théorème

On a :

$$\operatorname{card}\left(\left\{P \in E(K) \mid \hat{h}(P) \leqslant A/n_K\right\}\right) \leqslant 19977408 n_K \ln(n_K),$$

avec $A = 1/164736$.

Corollaire 1

On a $\operatorname{card}(E(K)_{\mathrm{tors}}) \leqslant 1977408 n_K \ln(n_K)$.

Corollaire 2

Pour tout $P \in E(K)$ d'ordre infini, on a :

$$\hat{h}(P) \geqslant \frac{1}{10^{18} n_K^3 (\ln(n_K))^2}.$$

Plan

Laurent (1979), W. (2015)

Supposons que $\mathbb{Z} \subsetneq \mathrm{End}(E)$. Pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré relatif $D = [K(P) : K]$, on a :

$$\hat{h}(P) \geqslant \frac{c_K}{D} \left(\frac{\ln(\ln(4D))}{\ln(4D)} \right)^3$$

où $c_K \gg n_K^{-20}$ si HRG.

Relèvements de Frobenius

Soit E/K à multiplications complexes par $\mathcal{O}_F$ (c'est-à-dire $\mathrm{End}(E) \simeq \mathcal{O}_F$, où F est un corps quadratique imaginaire), ayant bonne réduction partout, et tel que $F \subseteq K$.

Relèvements de Frobenius

Soit E/K à multiplications complexes par $\mathcal{O}_F$ (c'est-à-dire $\mathrm{End}(E) \simeq \mathcal{O}_F$, où F est un corps quadratique imaginaire), ayant bonne réduction partout, et tel que $F \subseteq K$. Prenons $P \in E(K)$ d'ordre infini.

Relèvements de Frobenius

Soit E/K à multiplications complexes par $\mathcal{O}_F$ (c'est-à-dire $\mathrm{End}(E) \simeq \mathcal{O}_F$, où F est un corps quadratique imaginaire), ayant bonne réduction partout, et tel que $F \subseteq K$. Prenons $P \in E(K)$ d'ordre infini. Soit $s \geqslant 3$, et soit $\Pi_s = \{p_1, \ldots, p_r\}$ l'ensemble des nombres premiers qui se décomposent complètement dans K.

Relèvements de Frobenius

Soit E/K à multiplications complexes par $\mathcal{O}_F$ (c'est-à-dire $\mathrm{End}(E) \simeq \mathcal{O}_F$, où F est un corps quadratique imaginaire), ayant bonne réduction partout, et tel que $F \subseteq K$. Prenons $P \in E(K)$ d'ordre infini. Soit $s \geqslant 3$, et soit $\Pi_s = \{p_1, \ldots, p_r\}$ l'ensemble des nombres premiers qui se décomposent complètement dans K.

Relèvements de Frobenius

Supposons que K contient F. Pour tout $p_i \in \Pi_s$, soit $\mathfrak{p}_i | p_i$ fixé ; alors $(x, y) \bmod \mathfrak{p}_i \mapsto (x^{p_i}, y^{p_i}) \bmod \mathfrak{p}_i$ se relève en $\mathrm{F}_{p_i} : E \to E$.

Relèvements de Frobenius

Soit E/K à multiplications complexes par $\mathcal{O}_F$ (c'est-à-dire $\mathrm{End}(E) \simeq \mathcal{O}_F$, où F est un corps quadratique imaginaire), ayant bonne réduction partout, et tel que $F \subseteq K$. Prenons $P \in E(K)$ d'ordre infini. Soit $s \geqslant 3$, et soit $\Pi_s = \{p_1, \ldots, p_r\}$ l'ensemble des nombres premiers qui se décomposent complètement dans K.

Relèvements de Frobenius

Supposons que K contient F. Pour tout $p_i \in \Pi_s$, soit $\mathfrak{p}_i | p_i$ fixé ; alors $(x, y) \bmod \mathfrak{p}_i \mapsto (x^{p_i}, y^{p_i}) \bmod \mathfrak{p}_i$ se relève en $\mathrm{F}_{p_i} : E \to E$.

On pose $p_0 = 1$ et $\mathrm{F}_1 = \mathrm{Id}$.

On pose :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - (\mathcal{O})),$$

On pose :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - (\mathcal{O})),$$

Par le théorème de l'indice de Hodge :

$$0 \geqslant \langle \mathcal{L}, \mathcal{L} \rangle = \sum_{0 \leqslant i,j \leqslant r} m_i m_j (\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle + \langle \mathcal{O}, \mathcal{O} \rangle - \langle (\mathrm{F}_{p_i} + \mathrm{F}_{p_j})(\mathcal{P}), \mathcal{O} \rangle).$$

On pose :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - (\mathcal{O})),$$

Par le théorème de l'indice de Hodge :

$$0 \geqslant \langle \mathcal{L}, \mathcal{L} \rangle = \sum_{0 \leqslant i,j \leqslant r} m_i m_j (\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle + \langle \mathcal{O}, \mathcal{O} \rangle$$
$$- \langle (\mathrm{F}_{p_i} + \mathrm{F}_{p_j})(\mathcal{P}), \mathcal{O} \rangle).$$

On pose :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - (\mathcal{O})),$$

Par le théorème de l'indice de Hodge :

$$0 \geqslant \langle \mathcal{L}, \mathcal{L} \rangle = \sum_{0 \leqslant i,j \leqslant r} m_i m_j (\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle + \langle \mathcal{O}, \mathcal{O} \rangle - n_K(p_i + p_j)\hat{h}(P)).$$

On pose :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - (\mathcal{O})),$$

Par le théorème de l'indice de Hodge :

$$0 \geqslant \langle \mathcal{L}, \mathcal{L} \rangle = \sum_{0 \leqslant i,j \leqslant r} m_i m_j (\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle + \langle \mathcal{O}, \mathcal{O} \rangle$$
$$- n_K(p_i + p_j)\hat{h}(P)).$$

On pose :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - (\mathcal{O})),$$

Par le théorème de l'indice de Hodge :

$$0 \geqslant \langle \mathcal{L}, \mathcal{L} \rangle = \sum_{0 \leqslant i,j \leqslant r} m_i m_j (\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle - n_K(p_i + p_j)\hat{h}(P)).$$

On pose :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - (\mathcal{O})),$$

Par le théorème de l'indice de Hodge :

$$0 \geqslant \langle \mathcal{L}, \mathcal{L} \rangle = \sum_{0 \leqslant i,j \leqslant r} m_i m_j (\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle - n_K(p_i + p_j)\hat{h}(P)).$$

On a donc

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

Contributions aux places finies

On a, en conservant les notations précédentes,

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

Contributions aux places finies

On a, en conservant les notations précédentes,

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

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,

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

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,

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

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, comme $P \in E(K)$, sa réduction est dans $\tilde{E}(\mathbb{F}_{p_i})$, et ses coordonnées sont fixées par l'automorphisme de Frobenius.

Contributions aux places finies

On a, en conservant les notations précédentes,

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

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, comme $P \in E(K)$, sa réduction est dans $\tilde{E}(\mathbb{F}_{p_i})$, et ses coordonnées sont fixées par l'automorphisme de Frobenius.

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

Contribution aux places infinies

Lemme d'Elkies

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

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

Contribution aux places infinies

Lemme d'Elkies

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

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

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

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

Contribution aux places infinies

Lemme d'Elkies

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

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

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

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

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

Contribution aux places infinies

Lemme d'Elkies « pondéré »

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

$$\sum_{1\leqslant i\neq j\leqslant N} m_i m_j \langle P_i, P_i\rangle_v \geqslant -\sum_{i=1}^{N} m_i^2 \times \left(\frac{1}{2}\ln\left(2\frac{\left(\sum_{i=1}^{N} m_i\right)^2}{\sum_{i=1}^{N} m_i^2} - 2\right) + \frac{1}{12}J_v + \frac{27}{10}\right).$$

Pour résumer,

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

Pour résumer,

$$2n_K\left(\sum_{i=0}^{r} m_i\right)\left(\sum_{j=0}^{r} m_j p_j\right)\hat{h}(P) \geqslant \sum_{v\in M_K^0}\sum_{\substack{1\leqslant i,j\leqslant r\\ i\neq j}} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v + \sum_{v\in M_K^\infty}\sum_{1\leqslant i\neq j\leqslant r} n_v m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v$$

Pour résumer,

$$2n_K\left(\sum_{i=0}^{r} m_i\right)\left(\sum_{j=0}^{r} m_j p_j\right)\hat{h}(P) \geqslant n_K m_0 \sum_{i=1}^{r} m_i \ln(p_i) + \sum_{v\in M_K^\infty}\sum_{1\leqslant i\neq j\leqslant r} n_v m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v$$

Pour résumer,

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

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

Pour résumer,

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

Pour résumer,

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

Pour résumer,

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

Pour résumer,

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

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

Pour résumer,

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

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

Pour résumer,

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

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

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

On a :

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

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

On a :

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

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

On a :

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

$$\hat{h}(P) \gtrsim \frac{r^{3/2} \ln(r) - (m_0^2 + r) \cdot \left(\frac{1}{2} \ln \left(2 \frac{(m_0+r)^2}{m_0^2+r} - 2 \right) + \frac{h(j_E)}{12} + \frac{27}{10} \right)}{2 (m_0 + r) \left(m_0 + \sum_{j=0}^{r} p_j \right)}$$

On a :

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

$$\hat{h}(P) \gtrsim \frac{r^{3/2} \ln(r) - (m_0^2 + r) \cdot \left(\frac{1}{2} \ln \left(2 \frac{(m_0+r)^2}{m_0^2+r} - 2 \right) + \frac{h(j_E)}{12} + \frac{27}{10} \right)}{2 (m_0 + r) \left(m_0 + \sum_{j=0}^{r} p_j \right)}$$

On a :

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

$$\hat{h}(P) \gtrsim \frac{r^{3/2} \ln(r) - r \ln(r)}{2 (m_0 + r) \left(m_0 + \sum_{j=0}^{r} p_j \right)}$$

On a :

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

$$\hat{h}(P) \gtrsim \frac{r^{3/2} \ln(r) - r \ln(r)}{2 (m_0 + r) \left(m_0 + \sum_{j=0}^{r} p_j \right)}$$

On a :

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

$$\hat{h}(P) \gtrsim \frac{r^{3/2} \ln(r) - r \ln(r)}{r^3 \ln(r)}$$

On a :

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

$$\hat{h}(P) \gtrsim \frac{1}{r^{3/2}}$$

On a :

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

$$\hat{h}(P) \gtrsim \left(\frac{\ln(s)}{s} \right)^{3/2}$$

On a :

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

$$\hat{h}(P) \gtrsim \left(\frac{\ln(s)}{s} \right)^{3/2}$$

En adaptant la démonstration à $P \in E'(\bar{K})$ avec E' aux bonnes propriétés, et avec un bon choix de s (Chebotarev explicite), on obtient $\hat{h}(P) \geqslant \frac{c(K,\varepsilon)}{[K(P):K]^{1+\varepsilon}}$.