Séminaire LFANT

"Recherche de points entiers sur une variété modulaire de dimension 3"

Samuel Le Fourn

Sommaire de l'exposé

Points rationnels et points entiers de variétés algébriques

Notion de hauteurs et méthodes effectives

La méthode de Runge

Application à la variété modulaire $A_2(2)^S$

Points rationnels et points entiers de variétés algébriques

Notion de hauteurs et méthodes effectives

La méthode de Runge

Application à la variété modulaire $A_2(2)^S$

Points rationnels de variétés algébriques

Points rationnels de variétés algébriques

Contexte

On fixe $f_1, \cdots, f_m \in \mathbb{Z}[X_0, \cdots, X_n]$ *homogènes*. On cherche à trouver les $x = (x_0, \cdots, x_n) \in \mathbb{Q}^n$ tels que

$$f_1(x) = \cdots = f_m(x) = 0.$$

Points rationnels de variétés algébriques

Contexte

On fixe $f_1, \cdots, f_m \in \mathbb{Z}[X_0, \cdots, X_n]$ *homogènes*. On cherche à trouver les $x = (x_0, \cdots, x_n) \in \mathbb{Q}^n$ tels que

$$f_1(x) = \cdots = f_m(x) = 0.$$

Points rationnels de variétés algébriques

Contexte

On fixe $f_1, \cdots, f_m \in \mathbb{Z}[X_0, \cdots, X_n]$ *homogènes*. On cherche à trouver les $x = (x_0, \cdots, x_n) \in \mathbb{Q}^n$ tels que

$$f_1(x) = \cdots = f_m(x) = 0.$$

Reformulation

Cela revient à chercher les points $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ de la sous-variété X de $\mathbb{P}^n$ définie par $f_1, \cdots, f_m$.

Points rationnels de variétés algébriques

Contexte

On fixe $f_1, \cdots, f_m \in \mathbb{Z}[X_0, \cdots, X_n]$ *homogènes.* On cherche à trouver les $x = (x_0, \cdots, x_n) \in \mathbb{Q}^n$ tels que

$$f_1(x) = \cdots = f_m(x) = 0.$$

Reformulation

Cela revient à chercher les points $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ de la sous-variété X de $\mathbb{P}^n$ définie par $f_1, \cdots, f_m$.

Notations et hypothèses fixées pour la suite

Points rationnels de variétés algébriques

Contexte

On fixe $f_1, \cdots, f_m \in \mathbb{Z}[X_0, \cdots, X_n]$ *homogènes*. On cherche à trouver les $x = (x_0, \cdots, x_n) \in \mathbb{Q}^n$ tels que

$$f_1(x) = \cdots = f_m(x) = 0.$$

Reformulation

Cela revient à chercher les points $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ de la sous-variété X de $\mathbb{P}^n$ définie par $f_1, \cdots, f_m$.

Notations et hypothèses fixées pour la suite

- $X := Z(f_1, \cdots, f_m) \subset \mathbb{P}^n_{/\mathbb{Q}}$ variété projective irréductible lisse sur $\mathbb{Q}$.

Points rationnels de variétés algébriques

Contexte

On fixe $f_1, \cdots, f_m \in \mathbb{Z}[X_0, \cdots, X_n]$ *homogènes*. On cherche à trouver les $x = (x_0, \cdots, x_n) \in \mathbb{Q}^n$ tels que

$$f_1(x) = \cdots = f_m(x) = 0.$$

Reformulation

Cela revient à chercher les points $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ de la sous-variété X de $\mathbb{P}^n$ définie par $f_1, \cdots, f_m$.

Notations et hypothèses fixées pour la suite

- $X := Z(f_1, \cdots, f_m) \subset \mathbb{P}^n_{/\mathbb{Q}}$ variété projective irréductible lisse sur $\mathbb{Q}$.
- Pour $P \in \mathbb{P}^n(\mathbb{Q})$, $x \in \mathbb{Z}^{n+1}$ désignera un choix de coordonnées *normalisées* ($\mathrm{pgcd}(x_0, \cdots, x_n) = 1$).

Points rationnels de variétés algébriques

Contexte

On fixe $f_1, \cdots, f_m \in \mathbb{Z}[X_0, \cdots, X_n]$ *homogènes.* On cherche à trouver les $x = (x_0, \cdots, x_n) \in \mathbb{Q}^n$ tels que

$$f_1(x) = \cdots = f_m(x) = 0.$$

Reformulation

Cela revient à chercher les points $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ de la sous-variété X de $\mathbb{P}^n$ définie par $f_1, \cdots, f_m$.

Notations et hypothèses fixées pour la suite

- $X := Z(f_1, \cdots, f_m) \subset \mathbb{P}^n_{/\mathbb{Q}}$ variété projective irréductible lisse sur $\mathbb{Q}$.
- Pour $P \in \mathbb{P}^n(\mathbb{Q})$, $x \in \mathbb{Z}^{n+1}$ désignera un choix de coordonnées *normalisées* ($\mathrm{pgcd}(x_0, \cdots, x_n) = 1$).
- $X(\mathbb{Q})$ est l'ensemble des points rationnels de X.

En fait... on va se limiter aux points entiers

En fait... on va se limiter aux points entiers

Problème

Peu de résultats effectifs pour $X(\mathbb{Q})$ en général (même si X est une courbe).

En fait... on va se limiter aux points entiers

Problème

Peu de résultats effectifs pour $X(\mathbb{Q})$ en général (même si X est une courbe).

Remarque

Avec les définitions habituelles, $X(\mathbb{Z}) = X(\mathbb{Q})$.

En fait... on va se limiter aux points entiers

Problème

Peu de résultats effectifs pour $X(\mathbb{Q})$ en général (même si X est une courbe).

Remarque

Avec les définitions habituelles, $X(\mathbb{Z}) = X(\mathbb{Q})$.

Notion d'intégralité : exemple de base

On a $\mathbb{A}^n \subset \mathbb{P}^n$ via $(x_1, \cdots, x_n) \mapsto (1 : x_1 : \cdots x_n)$ et on veut que les points entiers soient ceux venant de $\mathbb{A}^n(\mathbb{Z}) = (\mathbb{P}^n \backslash \{x_0 = 0\})(\mathbb{Z})$.

En fait... on va se limiter aux points entiers

Problème

Peu de résultats effectifs pour $X(\mathbb{Q})$ en général (même si X est une courbe).

Remarque

Avec les définitions habituelles, $X(\mathbb{Z}) = X(\mathbb{Q})$.

Notion d'intégralité : exemple de base

On a $\mathbb{A}^n \subset \mathbb{P}^n$ via $(x_1, \cdots, x_n) \mapsto (1 : x_1 : \cdots x_n)$ et on veut que les points entiers soient ceux venant de $\mathbb{A}^n(\mathbb{Z}) = (\mathbb{P}^n \backslash \{x_0 = 0\})(\mathbb{Z})$. Cela revient pour $P \in X(\mathbb{Q})$ à $\left(\frac{x_i}{x_0}\right) \in \mathbb{Z}$ pour tout i.

En fait... on va se limiter aux points entiers

Problème

Peu de résultats effectifs pour $X(\mathbb{Q})$ en général (même si X est une courbe).

Remarque

Avec les définitions habituelles, $X(\mathbb{Z}) = X(\mathbb{Q})$.

Notion d'intégralité : exemple de base

On a $\mathbb{A}^n \subset \mathbb{P}^n$ via $(x_1, \cdots, x_n) \mapsto (1 : x_1 : \cdots x_n)$ et on veut que les points entiers soient ceux venant de $\mathbb{A}^n(\mathbb{Z}) = (\mathbb{P}^n \backslash \{x_0 = 0\})(\mathbb{Z})$. Cela revient pour $P \in X(\mathbb{Q})$ à $\left(\frac{x_i}{x_0}\right) \in \mathbb{Z}$ pour tout i.

Définition (Intégralité par rapport à un fermé)

Si $Y \subset X$ fixé est défini par $g_1(x) = \cdots = g_s(x) = 0$,

$$(X \backslash Y)(\mathbb{Z}) := \left\{ P \in X(\mathbb{Q}) \;\middle|\; \forall (i,j),\ \frac{x_i^{\deg g_j}}{g_j(x)} \in \mathbb{Z} \right\}.$$

En fait... on va se limiter aux points entiers

Problème

Peu de résultats effectifs pour $X(\mathbb{Q})$ en général (même si X est une courbe).

Remarque

Avec les définitions habituelles, $X(\mathbb{Z}) = X(\mathbb{Q})$.

Notion d'intégralité : exemple de base

On a $\mathbb{A}^n \subset \mathbb{P}^n$ via $(x_1, \cdots, x_n) \mapsto (1 : x_1 : \cdots x_n)$ et on veut que les points entiers soient ceux venant de $\mathbb{A}^n(\mathbb{Z}) = (\mathbb{P}^n \backslash \{x_0 = 0\})(\mathbb{Z})$. Cela revient pour $P \in X(\mathbb{Q})$ à $\left(\frac{x_i}{x_0}\right) \in \mathbb{Z}$ pour tout i.

Définition (Intégralité par rapport à un fermé)

Si $Y \subset X$ fixé est défini par $g_1(x) = \cdots = g_s(x) = 0$,

$$(X \backslash Y)(\mathbb{Z}) := \left\{ P \in X(\mathbb{Q}) \;\middle|\; \forall (i,j),\ \frac{x_i^{\deg g_j}}{g_j(x)} \in \mathbb{Z} \right\}.$$

Remarque

Beaucoup de notations dépendront du choix des polynômes ensuite.

Elargissement de la définition

$$(X\backslash Y)(\mathbb{Z}) := \left\{ P \in X(\mathbb{Q}) \;\middle|\; \forall (i,j),\ \frac{x_i^{\deg g_j}}{g_j(x)} \in \mathbb{Z} \right\}.$$

Elargissement de la définition

$$(X\backslash Y)(\mathbb{Z}) := \left\{ P \in X(\mathbb{Q}) \,\middle|\, \forall (i,j),\ \frac{x_i^{\deg g_j}}{g_j(x)} \in \mathbb{Z} \right\}.$$

Ensemble de mauvaises places

Elargissement de la définition

$$(X\backslash Y)(\mathbb{Z}) := \left\{ P \in X(\mathbb{Q}) \;\middle|\; \forall (i,j),\ \frac{x_i^{\deg g_j}}{g_j(x)} \in \mathbb{Z} \right\}.$$

Ensemble de mauvaises places

- $M_{\mathbb{Q}} = \{\infty, 2, 3, 5, 7, \cdots\}$ est l'ensemble des places de $\mathbb{Q}$ (chaque $v \in M_{\mathbb{Q}}$ définit une norme $|\cdot|_v$ sur $\mathbb{Q}$).

Elargissement de la définition

$$(X\backslash Y)(\mathbb{Z}) := \left\{ P \in X(\mathbb{Q}) \,\middle|\, \forall (i,j),\ \frac{x_i^{\deg g_j}}{g_j(x)} \in \mathbb{Z} \right\}.$$

Ensemble de mauvaises places

- $M_{\mathbb{Q}} = \{\infty, 2, 3, 5, 7, \cdots\}$ est l'ensemble des places de $\mathbb{Q}$ (chaque $v \in M_{\mathbb{Q}}$ définit une norme $|\cdot|_v$ sur $\mathbb{Q}$).
- On fixera $S := \{\infty, p_1, \cdots, p_k\}$ et alors

$$\mathbb{Z}_S := \mathbb{Z}\left[\frac{1}{p_1 \cdots p_k}\right] = \{\alpha \in \mathbb{Q} \,|\, \forall v \in M_{\mathbb{Q}} \backslash S, |\alpha|_v \leq 1\}.$$

- On notera alors

$$(X\backslash Y)(\mathbb{Z}_S) := \left\{ P \in X(\mathbb{Q}) \,\middle|\, \forall (i,j),\ \frac{x_i^{\deg g_j}}{g_j(x)} \in \mathbb{Z}_S \right\}.$$

Hauteur relative à un fermé

Hauteur relative à un fermé

Notations fixées

Hauteur relative à un fermé

Notations fixées

- $X \subset \mathbb{P}^n_{\mathbb{Q}}$ définie par $f_1(x) = \cdots = f_m(x) = 0$.

Hauteur relative à un fermé

Notations fixées

- $X \subset \mathbb{P}^n_{\mathbb{Q}}$ définie par $f_1(x) = \cdots = f_m(x) = 0$.
- $Y \subset X$ fermé défini par $g_1(x) = \cdots = g_s(x) = 0$.

Hauteur relative à un fermé

Notations fixées

- $X \subset \mathbb{P}^n_{\mathbb{Q}}$ définie par $f_1(x) = \cdots = f_m(x) = 0$.
- $Y \subset X$ fermé défini par $g_1(x) = \cdots = g_s(x) = 0$.
- Pour $P \in \mathbb{P}^n(\mathbb{Q})$, et x_P des coordonnées normalisées, $\|x_P\|_v := \max_{0 \leq i \leq n} |x_i|_v$.

Hauteur relative à un fermé

Notations fixées

- $X \subset \mathbb{P}^n_{\mathbb{Q}}$ définie par $f_1(x) = \cdots = f_m(x) = 0$.
- $Y \subset X$ fermé défini par $g_1(x) = \cdots = g_s(x) = 0$.
- Pour $P \in \mathbb{P}^n(\mathbb{Q})$, et x_P des coordonnées normalisées, $\|x_P\|_v := \max_{0 \leq i \leq n} |x_i|_v$.
- Pour $v \in M_{\mathbb{Q}}$ et $g \in \mathbb{Q}[X_0, \cdots, X_n]$, $\|g\|_v := \max |\operatorname{coeffs}(g)|_v$.

Hauteur relative à un fermé

Notations fixées

- $X \subset \mathbb{P}^n_{\mathbb{Q}}$ définie par $f_1(x) = \cdots = f_m(x) = 0$.
- $Y \subset X$ fermé défini par $g_1(x) = \cdots = g_s(x) = 0$.
- Pour $P \in \mathbb{P}^n(\mathbb{Q})$, et x_P des coordonnées normalisées, $\|x_P\|_v := \max_{0 \leq i \leq n} |x_i|_v$.
- Pour $v \in M_{\mathbb{Q}}$ et $g \in \mathbb{Q}[X_0, \cdots, X_n]$, $\|g\|_v := \max |\operatorname{coeffs}(g)|_v$.

Définition (Hauteur relative à Y)

Elle mesure la proximité d'un point à Y pour chaque place possible.

$$h_Y(P) := \sum_{v \in M_{\mathbb{Q}}} h_{Y,v}(P),$$

Hauteur relative à un fermé

Notations fixées

- $X \subset \mathbb{P}^n_{\mathbb{Q}}$ définie par $f_1(x) = \cdots = f_m(x) = 0$.
- $Y \subset X$ fermé défini par $g_1(x) = \cdots = g_s(x) = 0$.
- Pour $P \in \mathbb{P}^n(\mathbb{Q})$, et x_P des coordonnées normalisées, $\|x_P\|_v := \max_{0 \leq i \leq n} |x_i|_v$.
- Pour $v \in M_{\mathbb{Q}}$ et $g \in \mathbb{Q}[X_0, \cdots, X_n]$, $\|g\|_v := \max |\operatorname{coeffs}(g)|_v$.

Définition (Hauteur relative à Y)

Elle mesure la proximité d'un point à Y pour chaque place possible.

$$h_Y(P) := \sum_{v \in M_{\mathbb{Q}}} h_{Y,v}(P), \quad h_{Y,v}(P) := -\min_{1 \leq j \leq s} \log \frac{\|g_j(x_P)\|_v}{\|g_j\|_w \|x_P\|_v^{\deg g_j}}.$$

Intuition de base

$$h_{Y,v}(P) \text{ grand} \Leftrightarrow P \text{ “}v\text{-proche” de } Y.$$

Lien entre hauteur locale et réduction

Réduction d'un point de $\mathbb{P}^n(\mathbb{Q})$ modulo p premier

Lien entre hauteur locale et réduction

Réduction d'un point de $\mathbb{P}^n(\mathbb{Q})$ modulo p premier

Si $P \in \mathbb{P}^n(\mathbb{Q}) = (x_0 : \cdots : x_n)$ avec x_P normalisé et p premier, la *réduction de P modulo p* est

$$\overline{P}_p := (\overline{x_0} : \cdots : \overline{x_n}) \in \mathbb{P}^n(\mathbb{F}_p).$$

Lien entre hauteur locale et réduction

Réduction d'un point de $\mathbb{P}^n(\mathbb{Q})$ modulo p premier

Si $P \in \mathbb{P}^n(\mathbb{Q}) = (x_0 : \cdots : x_n)$ avec x_P normalisé et p premier, la *réduction de P modulo p* est

$$\overline{P}_p := (\overline{x_0} : \cdots : \overline{x_n}) \in \mathbb{P}^n(\mathbb{F}_p).$$

Un procédé similaire définit $\overline{Y_p}$ et $\overline{X}_p$ comme sous-variétés de $\mathbb{P}^n_{\mathbb{F}_p}$.

Lien entre hauteur locale et réduction

Réduction d'un point de $\mathbb{P}^n(\mathbb{Q})$ modulo p premier

Si $P \in \mathbb{P}^n(\mathbb{Q}) = (x_0 : \cdots : x_n)$ avec x_P normalisé et p premier, la *réduction de P modulo p* est

$$\overline{P}_p := (\overline{x_0} : \cdots : \overline{x_n}) \in \mathbb{P}^n(\mathbb{F}_p).$$

Un procédé similaire définit $\overline{Y_p}$ et $\overline{X}_p$ comme sous-variétés de $\mathbb{P}^n_{\mathbb{F}_p}$.

Proposition

Après avoir normalisé les générateurs de Y à $\|g_j\|_p = 1$ pour tout p premier, on a pour tout $P \in X(\mathbb{Q})$,

$$h_{Y,p}(P) > 0 \Leftrightarrow \overline{P}_p \in \overline{Y}_p.$$

Lien entre hauteur locale et réduction

Réduction d'un point de $\mathbb{P}^n(\mathbb{Q})$ modulo p premier

Si $P \in \mathbb{P}^n(\mathbb{Q}) = (x_0 : \cdots : x_n)$ avec x_P normalisé et p premier, la *réduction de P modulo p* est

$$\overline{P}_p := (\overline{x_0} : \cdots : \overline{x_n}) \in \mathbb{P}^n(\mathbb{F}_p).$$

Un procédé similaire définit $\overline{Y_p}$ et $\overline{X}_p$ comme sous-variétés de $\mathbb{P}^n_{\mathbb{F}_p}$.

Proposition

Après avoir normalisé les générateurs de Y à $\|g_j\|_p = 1$ pour tout p premier, on a pour tout $P \in X(\mathbb{Q})$,

$$h_{Y,p}(P) > 0 \Leftrightarrow \overline{P}_p \in \overline{Y}_p.$$

Par construction, on a aussi

$$(X \backslash Y)(\mathbb{Z}_S) = \{P \in X(\mathbb{Q}) \,|\, \forall p \in (M_{\mathbb{Q}} \backslash S), \overline{P}_p \notin \overline{Y}_p\}.$$

Comment utiliser les hauteurs pour une détermination effective ?

Comment utiliser les hauteurs pour une détermination effective ?

Ce qu'on sait déjà

- $h_Y(P) := \sum_{v \in M_{\mathbb{Q}}} h_{Y,v}(P)$.
- $h_{Y,v}(P) = 0$ si $P \in (X \backslash Y)(\mathbb{Z}_S)$ et $v \notin S$.

Comment utiliser les hauteurs pour une détermination effective ?

Ce qu'on sait déjà

- $h_Y(P) := \sum_{v \in M_{\mathbb{Q}}} h_{Y,v}(P)$.
- $h_{Y,v}(P) = 0$ si $P \in (X \backslash Y)(\mathbb{Z}_S)$ et $v \notin S$.

Proposition (propriété de Northcott)

Si Y est un *diviseur effectif ample* (par exemple $Y : g_1(x) = 0$),

$$\{P \in \mathbb{P}^n(\mathbb{Q}) \,|\, h_Y(P) \leq B\}$$

est *fini et effectivement calculable* pour toute borne B. Il "suffit" donc de borner h_Y sur $X(\mathbb{Q})$.

Comment utiliser les hauteurs pour une détermination effective ?

Ce qu'on sait déjà

- $h_Y(P) := \sum_{v \in M_{\mathbb{Q}}} h_{Y,v}(P)$.
- $h_{Y,v}(P) = 0$ si $P \in (X \backslash Y)(\mathbb{Z}_S)$ et $v \notin S$.

Proposition (propriété de Northcott)

Si Y est un *diviseur effectif ample* (par exemple $Y : g_1(x) = 0$),

$$\{P \in \mathbb{P}^n(\mathbb{Q}) \,|\, h_Y(P) \leq B\}$$

est *fini et effectivement calculable* pour toute borne B. Il "suffit" donc de borner h_Y sur $X(\mathbb{Q})$.

Remarque

Pour les points entiers, on a déjà fait une partie du travail !

Le cas des courbes

Ici, X est une courbe de genre g et on prend $Y \subset X(\mathbb{Q})$ de cardinal r.

Le cas des courbes

Ici, X est une courbe de genre g et on prend $Y \subset X(\mathbb{Q})$ de cardinal r.

Théorème (Siegel)

Si $g \geq 1$ et $r \geq 1$ ou $g = 0$ et $r \geq 3$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est fini pour tout S.

Le cas des courbes

Ici, X est une courbe de genre g et on prend $Y \subset X(\mathbb{Q})$ de cardinal r.

Théorème (Siegel)

Si $g \geq 1$ et $r \geq 1$ ou $g = 0$ et $r \geq 3$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est fini pour tout S.

Problème

Même ce théorème n'est pas effectif !

Le cas des courbes

Ici, X est une courbe de genre g et on prend $Y \subset X(\mathbb{Q})$ de cardinal r.

Théorème (Siegel)

Si $g \geq 1$ et $r \geq 1$ ou $g = 0$ et $r \geq 3$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est fini pour tout S.

Problème

Même ce théorème n'est pas effectif !

Deux méthodes effectives intéressantes

Le cas des courbes

Ici, X est une courbe de genre g et on prend $Y \subset X(\mathbb{Q})$ de cardinal r.

Théorème (Siegel)

Si $g \geq 1$ et $r \geq 1$ ou $g = 0$ et $r \geq 3$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est fini pour tout S.

Problème

Même ce théorème n'est pas effectif !

Deux méthodes effectives intéressantes

- Méthode de Baker : suppose l'existence d'assez de fonctions $\phi \in \mathbb{Q}(X)$ avec $\mathrm{div}(\phi) \subset Y$.

Le cas des courbes

Ici, X est une courbe de genre g et on prend $Y \subset X(\mathbb{Q})$ de cardinal r.

Théorème (Siegel)

Si $g \geq 1$ et $r \geq 1$ ou $g = 0$ et $r \geq 3$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est fini pour tout S.

Problème

Même ce théorème n'est pas effectif !

Deux méthodes effectives intéressantes

- Méthode de Baker : suppose l'existence d'assez de fonctions $\phi \in \mathbb{Q}(X)$ avec $\mathrm{div}(\phi) \subset Y$.
- Méthode de Runge : suppose que $|S|$ est petit par rapport à $r = |Y| \quad \Longrightarrow$ notre sujet d'aujourd'hui.

Points rationnels et points entiers de variétés algébriques

Notion de hauteurs et méthodes effectives

La méthode de Runge

Application à la variété modulaire $A_2(2)^S$

La méthode de Runge pour les courbes

La méthode de Runge pour les courbes

Théorème (Bombieri, 1983)

Soit X une courbe et $Y \subset X(\mathbb{Q})$ de cardinal r.
Si $|S| < r$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est *effectivement fini*,

La méthode de Runge pour les courbes

Théorème (Bombieri, 1983)

Soit X une courbe et $Y \subset X(\mathbb{Q})$ de cardinal r.
Si $|S| < r$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est *effectivement fini*,

au sens où on peut borner une certaine hauteur (qui vérifie Northcott) sur cet ensemble.

La méthode de Runge pour les courbes

Théorème (Bombieri, 1983)

Soit X une courbe et $Y \subset X(\mathbb{Q})$ de cardinal r.
Si $|S| < r$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est *effectivement fini*, et c'est même le cas de

$$\bigcup_{S, |S| < r} X(\mathbb{Z}_S),$$

au sens où on peut borner une certaine hauteur (qui vérifie Northcott) sur cet ensemble.

La méthode de Runge pour les courbes

Théorème (Bombieri, 1983)

Soit X une courbe et $Y \subset X(\mathbb{Q})$ de cardinal r.
Si $|S| < r$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est *effectivement fini*, et c'est même le cas de

$$\bigcup_{S, |S| < r} X(\mathbb{Z}_S),$$

au sens où on peut borner une certaine hauteur (qui vérifie Northcott) sur cet ensemble.

Remarque

La version générale admet même des points entiers sur des corps de nombres et le corps qui varie.

La méthode de Runge pour les courbes

Théorème (Bombieri, 1983)

Soit X une courbe et $Y \subset X(\mathbb{Q})$ de cardinal r.
Si $|S| < r$, alors $(X \backslash Y)(\mathbb{Z}_S)$ est *effectivement fini*, et c'est même le cas de

$$\bigcup_{S, |S| < r} X(\mathbb{Z}_S),$$

au sens où on peut borner une certaine hauteur (qui vérifie Northcott) sur cet ensemble.

Remarque

La version générale admet même des points entiers sur des corps de nombres et le corps qui varie.

Idée

Cf. notes manuscrites

Runge en dimension supérieure (selon Levin)

Runge en dimension supérieure (selon Levin)

- Ici, on suppose $Y = D = D_1 \cup \cdots \cup D_r$ avec chaque D_i un diviseur effectif ample de X.

Runge en dimension supérieure (selon Levin)

- Ici, on suppose $Y = D = D_1 \cup \cdots \cup D_r$ avec chaque D_i un diviseur effectif ample de X.
- Contrairement au cas des courbes, on peut avoir $D_i \cap D_j \neq \emptyset$ donc un point P peut être v-près de plusieurs D_i en même temps.

Runge en dimension supérieure (selon Levin)

- Ici, on suppose $Y = D = D_1 \cup \cdots \cup D_r$ avec chaque D_i un diviseur effectif ample de X.
- Contrairement au cas des courbes, on peut avoir $D_i \cap D_j \neq \emptyset$ donc un point P peut être v-près de plusieurs D_i en même temps.
- Adapation de l'idée : cf. notes manuscrites

Runge en dimension supérieure (selon Levin)

- Ici, on suppose $Y = D = D_1 \cup \cdots \cup D_r$ avec chaque D_i un diviseur effectif ample de X.
- Contrairement au cas des courbes, on peut avoir $D_i \cap D_j \neq \emptyset$ donc un point P peut être v-près de plusieurs D_i en même temps.
- Adapation de l'idée : cf. notes manuscrites

Théorème (Levin, 2008)

On note $m := \max\{|I| \,|\, I \subset \{1, \cdots, r\}, \bigcap_{i \in I} D_i \neq \emptyset\}$.

Runge en dimension supérieure (selon Levin)

- Ici, on suppose $Y = D = D_1 \cup \cdots \cup D_r$ avec chaque D_i un diviseur effectif ample de X.
- Contrairement au cas des courbes, on peut avoir $D_i \cap D_j \neq \emptyset$ donc un point P peut être v-près de plusieurs D_i en même temps.
- Adapation de l'idée : cf. notes manuscrites

Théorème (Levin, 2008)

On note $m := \max\{|I| \,|\, I \subset \{1, \cdots, r\}, \bigcap_{i \in I} D_i \neq \emptyset\}$. Si $m|S| < r$, $(X \backslash D)(\mathbb{Z}_S)$ est effectivement fini, et c'est même le cas de

$$\bigcup_{S, m|S| < r} (X \backslash D)(\mathbb{Z}_S).$$

Runge en dimension supérieure (selon Levin)

- Ici, on suppose $Y = D = D_1 \cup \cdots \cup D_r$ avec chaque D_i un diviseur effectif ample de X.
- Contrairement au cas des courbes, on peut avoir $D_i \cap D_j \neq \emptyset$ donc un point P peut être v-près de plusieurs D_i en même temps.
- Adapation de l'idée : cf. notes manuscrites

Théorème (Levin, 2008)

On note $m := \max\{|I| \mid I \subset \{1, \cdots, r\}, \bigcap_{i \in I} D_i \neq \emptyset\}$. Si $m|S| < r$, $(X \backslash D)(\mathbb{Z}_S)$ est effectivement fini, et c'est même le cas de

$$\bigcup_{S, m|S| < r} (X \backslash D)(\mathbb{Z}_S).$$

Problème

Si r/m est trop petit, résultat presque inapplicable.

Améliorer la condition $m|S| < r$

Améliorer la condition $m|S| < r$

On définit un “graphe d’intersection” :

Améliorer la condition $m|S| < r$

On définit un “graphe d’intersection” :

- Sommets : les $Z_I := \cap_{i \in I} D_i$ non vides avec I *optimal* (si $J \supsetneq I$, $Z_J \neq Z_I$).

Améliorer la condition $m|S| < r$

On définit un “graphe d’intersection” :

- Sommets : les $Z_I := \cap_{i\in I} D_i$ non vides avec I *optimal* (si $J \supsetneq I$, $Z_J \neq Z_I$).
- Arêtes : $Z_I \to Z_J$ si $J \supsetneq I$ sans ensemble optimal intermédiaire.

Améliorer la condition $m|S| < r$

On définit un "graphe d'intersection" :

- Sommets : les $Z_I := \cap_{i \in I} D_i$ non vides avec I *optimal* (si $J \supsetneq I$, $Z_J \neq Z_I$).
- Arêtes : $Z_I \to Z_J$ si $J \supsetneq I$ sans ensemble optimal intermédiaire.
- Profondeur d'un Z_I : $|I|$.

Améliorer la condition $m|S| < r$

On définit un “graphe d’intersection” :

- Sommets : les $Z_I := \cap_{i \in I} D_i$ non vides avec I *optimal* (si $J \supsetneq I$, $Z_J \neq Z_I$).
- Arêtes : $Z_I \to Z_J$ si $J \supsetneq I$ sans ensemble optimal intermédiaire.
- Profondeur d’un Z_I : $|I|$.
- Cône au-dessus de Z_I : $\{Z_J,\, Z_J \supset Z_I\}$ (cf. notes).

Améliorer la condition $m|S| < r$

On définit un “graphe d’intersection” :

- Sommets : les $Z_I := \cap_{i \in I} D_i$ non vides avec I *optimal* (si $J \supsetneq I$, $Z_J \neq Z_I$).
- Arêtes : $Z_I \to Z_J$ si $J \supsetneq I$ sans ensemble optimal intermédiaire.
- Profondeur d’un Z_I : $|I|$.
- Cône au-dessus de Z_I : $\{Z_J, \, Z_J \supset Z_I\}$ (cf. notes).

Point crucial

Pour une bonne notion de v-proximité, quel que soit $P \in X(\mathbb{Q})$, l’ensemble des Z_I tels que P est v-proche de Z_I forme un cône (cf. notes).

Améliorer la condition $m|S| < r$

On définit un “graphe d’intersection” :

- Sommets : les $Z_I := \cap_{i \in I} D_i$ non vides avec I *optimal* (si $J \supsetneq I$, $Z_J \neq Z_I$).
- Arêtes : $Z_I \to Z_J$ si $J \supsetneq I$ sans ensemble optimal intermédiaire.
- Profondeur d’un Z_I : $|I|$.
- Cône au-dessus de Z_I : $\{Z_J, Z_J \supset Z_I\}$ (cf. notes).

Point crucial

Pour une bonne notion de v-proximité, quel que soit $P \in X(\mathbb{Q})$, l’ensemble des Z_I tels que P est v-proche de Z_I forme un cône (cf. notes).

Théorème (Corvaja–Sookdeo–Tucker–Zannier, 2015)

Si $|S|$ cônes quelconques ne peuvent pas recouvrir les sommets de profondeur 1, alors la méthode de Runge s’applique et $(X \backslash D)(\mathbb{Z}_S)$ est effectivement fini.

Points rationnels et points entiers de variétés algébriques

Notion de hauteurs et méthodes effectives

La méthode de Runge

Application à la variété modulaire $A_2(2)^S$

Application à une variété modulaire

Application à une variété modulaire

Définitions

Application à une variété modulaire

Définitions

- $A_2(2)$: espace de modules des surfaces abéliennes principalement polarisées (A, λ) avec base symplectique de la 2-torsion.

Application à une variété modulaire

Définitions

- $A_2(2)$: espace de modules des surfaces abéliennes principalement polarisées (A, λ) avec base symplectique de la 2-torsion.
- $X := A_2(2)^{\mathrm{Sa}}$ compactification de Satake de $A_2(2)$.

Application à une variété modulaire

Définitions

- $A_2(2)$: espace de modules des surfaces abéliennes principalement polarisées (A, λ) avec base symplectique de la 2-torsion.
- $X := A_2(2)^{\mathrm{Sa}}$ compactification de Satake de $A_2(2)$.
- $Y := D$ le diviseur des produits de courbes elliptiques dans $A_2(2)^{\mathrm{Sa}}$.

Application à une variété modulaire

Définitions

- $A_2(2)$: espace de modules des surfaces abéliennes principalement polarisées (A, λ) avec base symplectique de la 2-torsion.
- $X := A_2(2)^{\mathrm{Sa}}$ compactification de Satake de $A_2(2)$.
- $Y := D$ le diviseur des produits de courbes elliptiques dans $A_2(2)^{\mathrm{Sa}}$.

Rappel (Oort–Ueno, 1973)

Si (A, λ) est une surface abélienne principalement polarisée sur k algébriquement clos, (A, λ) est soit de la forme $\mathrm{Jac}(C)$ (C courbe de genre 2 sur k) soit un produit de courbes elliptiques.

Application à une variété modulaire

Définitions

- $A_2(2)$: espace de modules des surfaces abéliennes principalement polarisées (A, λ) avec base symplectique de la 2-torsion.
- $X := A_2(2)^{\mathrm{Sa}}$ compactification de Satake de $A_2(2)$.
- $Y := D$ le diviseur des produits de courbes elliptiques dans $A_2(2)^{\mathrm{Sa}}$.

Rappel (Oort–Ueno, 1973)

Si (A, λ) est une surface abélienne principalement polarisée sur k algébriquement clos, (A, λ) est soit de la forme $\mathrm{Jac}(C)$ (C courbe de genre 2 sur k) soit un produit de courbes elliptiques.

Objet d'étude

$$(A_2(2)^{\mathrm{Sa}} \backslash D)(\mathbb{Z}_S),$$

Application à une variété modulaire

Définitions

- $A_2(2)$: espace de modules des surfaces abéliennes principalement polarisées (A, λ) avec base symplectique de la 2-torsion.
- $X := A_2(2)^{\mathrm{Sa}}$ compactification de Satake de $A_2(2)$.
- $Y := D$ le diviseur des produits de courbes elliptiques dans $A_2(2)^{\mathrm{Sa}}$.

Rappel (Oort–Ueno, 1973)

Si (A, λ) est une surface abélienne principalement polarisée sur k algébriquement clos, (A, λ) est soit de la forme $\mathrm{Jac}(C)$ (C courbe de genre 2 sur k) soit un produit de courbes elliptiques.

Objet d'étude

$$(A_2(2)^{\mathrm{Sa}} \backslash D)(\mathbb{Z}_S),$$

qui paramètre l'ensemble des jacobiennes de courbes C de genre 2 sur $\mathbb{Q}$

Application à une variété modulaire

Définitions

- $A_2(2)$: espace de modules des surfaces abéliennes principalement polarisées (A, λ) avec base symplectique de la 2-torsion.
- $X := A_2(2)^{\mathrm{Sa}}$ compactification de Satake de $A_2(2)$.
- $Y := D$ le diviseur des produits de courbes elliptiques dans $A_2(2)^{\mathrm{Sa}}$.

Rappel (Oort–Ueno, 1973)

Si (A, λ) est une surface abélienne principalement polarisée sur k algébriquement clos, (A, λ) est soit de la forme $\mathrm{Jac}(C)$ (C courbe de genre 2 sur k) soit un produit de courbes elliptiques.

Objet d'étude

$$(A_2(2)^{\mathrm{Sa}} \backslash D)(\mathbb{Z}_S),$$

qui paramètre l'ensemble des jacobiennes de courbes C de genre 2 sur $\mathbb{Q}$ (dont tous les points de Weierstrass sont rationnels)

Application à une variété modulaire

Définitions

- $A_2(2)$: espace de modules des surfaces abéliennes principalement polarisées (A, λ) avec base symplectique de la 2-torsion.
- $X := A_2(2)^{\mathrm{Sa}}$ compactification de Satake de $A_2(2)$.
- $Y := D$ le diviseur des produits de courbes elliptiques dans $A_2(2)^{\mathrm{Sa}}$.

Rappel (Oort–Ueno, 1973)

Si (A, λ) est une surface abélienne principalement polarisée sur k algébriquement clos, (A, λ) est soit de la forme $\mathrm{Jac}(C)$ (C courbe de genre 2 sur k) soit un produit de courbes elliptiques.

Objet d'étude

$$(A_2(2)^{\mathrm{Sa}} \backslash D)(\mathbb{Z}_S),$$

qui paramètre l'ensemble des jacobiennes de courbes C de genre 2 sur $\mathbb{Q}$ (dont tous les points de Weierstrass sont rationnels) avec C ayant potentiellement bonne réduction partout sauf pour $p \in S$ (cf. notes).

Description explicite de X

On a (via les "fonctions thêta") un plongement

$$\psi : A_2(2)^{\mathrm{Sa}} \hookrightarrow \mathbb{P}^9$$

dont l'image (renotée X), de dimension 3, vérifie

Description explicite de X

On a (via les “fonctions thêta”) un plongement

$$\psi : A_2(2)^{\mathrm{Sa}} \hookrightarrow \mathbb{P}^9$$

dont l’image (renotée X), de dimension 3, vérifie

- X est défini par une équation quartique et 15 équations linéaires simples, par exemple

$$x_6 - x_7 - x_8 + x_9 = 0.$$

Description explicite de X

On a (via les “fonctions thêta”) un plongement

$$\psi : A_2(2)^{\mathrm{Sa}} \hookrightarrow \mathbb{P}^9$$

dont l’image (renotée X), de dimension 3, vérifie

- X est défini par une équation quartique et 15 équations linéaires simples, par exemple

$$x_6 - x_7 - x_8 + x_9 = 0.$$

- $\psi(D) = \bigcup_i D_i$ avec $D_i : \{x_i = 0\}$ (autrement dit, les produits de courbes elliptiques sont caractérisés par l’annulation d’une des 10 fonctions thêta).

Description explicite de X

On a (via les “fonctions thêta”) un plongement

$$\psi : A_2(2)^{\mathrm{Sa}} \hookrightarrow \mathbb{P}^9$$

dont l’image (renotée X), de dimension 3, vérifie

- X est défini par une équation quartique et 15 équations linéaires simples, par exemple

$$x_6 - x_7 - x_8 + x_9 = 0.$$

- $\psi(D) = \bigcup_i D_i$ avec $D_i : \{x_i = 0\}$ (autrement dit, les produits de courbes elliptiques sont caractérisés par l’annulation d’une des 10 fonctions thêta).

Graphe d’intersection et calculs : cf. notes manuscrites.

Conclusion de la méthode pour $X = A_2(2)^S$

Conclusion de la méthode pour $X = A_2(2)^S$

Théorème (Box-LF)

Si $P \in (A_2(2)^{\mathrm{Sa}} \backslash D)(\mathbb{Z}_S)$ et $|S| \leq 2$ alors $h_{D_1}(\psi(P)) \leq 10$.

Conclusion de la méthode pour $X = A_2(2)^S$

Théorème (Box-LF)

Si $P \in (A_2(2)^{\mathrm{Sa}} \backslash D)(\mathbb{Z}_S)$ et $|S| \leq 2$ alors $h_{D_1}(\psi(P)) \leq 10$.

Corollaire

Il n'existe pas de courbe hyperelliptique C de genre 2 sur $\mathbb{Q}$ dont tous les points de Weierstrass sont rationnels et ayant bonne réduction potentielle en tout nombre premier p sauf au plus un.

Merci de votre attention !