L'équation aux S-unités

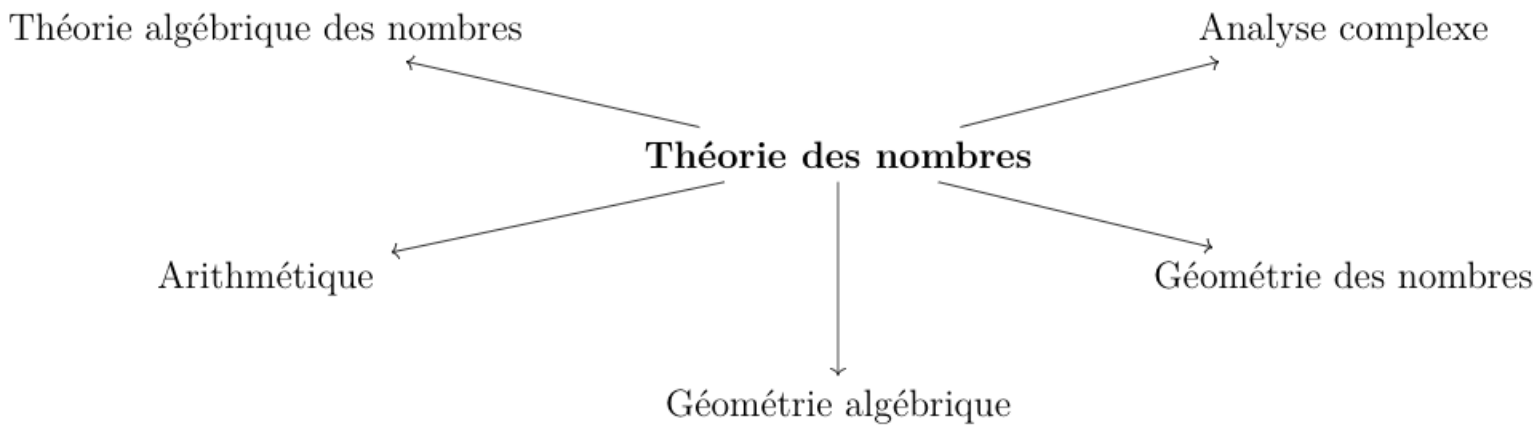
Khalil Bendriss, Paul Boisseau, Adam David, Félix Rebotier, Louis Rustenholz

20 mai 2020

Introduction

Thème du PSC : la théorie des nombres

Notre PSC porte sur un problème de *théorie des nombres*. Ce domaine de mathématiques est à l'interface de beaucoup de champs de recherches.



Quelques thèmes du PSC

L'objectif du PSC : l'équation aux S-unités

- Nous avons étudié *l'équation aux S-unités*, plus précisément un résultat de finitude sur l'ensemble des solutions, obtenu par Beukers et Schlickewei en 1996.

L'objectif du PSC : l'équation aux S-unités

- Nous avons étudié *l'équation aux S-unités*, plus précisément un résultat de finitude sur l'ensemble des solutions, obtenu par Beukers et Schlickewei en 1996.
- L'objectif était de rendre la preuve accessible à un étudiant en mathématiques de niveau L3, en introduisant tous les concepts et outils nécessaires à sa compréhension.

Plan de la présentation

- Approche historique et conceptuelle : quelle est la place du problème en arithmétique ?

Plan de la présentation

- Approche historique et conceptuelle : quelle est la place du problème en arithmétique ?
- Description précise de l'équation des S-unités, annonce du résultat principal de Beukers et Schlickewei (1996).

Plan de la présentation

- Approche historique et conceptuelle : quelle est la place du problème en arithmétique ?
- Description précise de l'équation des S-unités, annonce du résultat principal de Beukers et Schlickewei (1996).
- Quelques idées et outils de la preuve.

Plan de la présentation

- Approche historique et conceptuelle : quelle est la place du problème en arithmétique ?
- Description précise de l'équation des S-unités, annonce du résultat principal de Beukers et Schlickewei (1996).
- Quelques idées et outils de la preuve.
- Une application : le théorème de Siegel.

Contexte historique et scientifique

Balbutiements, grands problèmes et ad-hoc

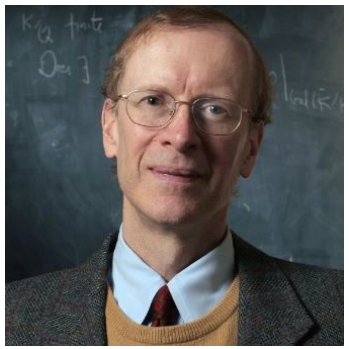
Équation de Pell–Fermat (Antiquité, Fermat XVII^{e}, Gauss XVIII^{e}, Dedekind XIX^{e})

$$x^2 + ny^2 = m$$

Théorème de Fermat–Wiles (Fermat XVII^{e}, ..., Wiles 1994)

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

Pierre de Fermat (1601–1665)



Andrew Wiles (1953–)

XVIII^{e} : renaissance de la théorie des nombres

- Nouveaux outils, essor de l'arithmétique modulaire
- Loi de réciprocité quadratique
- Théorie analytique des nombres
- ...

Euler
(1707–1783)

Lagrange
(1736–1813)

Legendre
(1752–1833)

Gauss
(1777-1855)

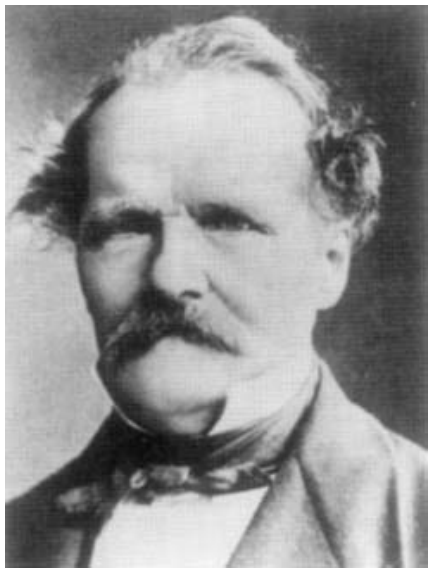
Nouvelle profondeur au XIX^{e} siècle

- Théorie analytique des nombres
  Théorème de la progression arithmétique
- Question de l'approximation diophantienne
- Théorie algébrique des nombres
  Entiers de Gauss $\mathbb{Z}[i]$, d'Eisenstein $\mathbb{Z}[j]$, quadratiques...
  Théorème des unités de Dirichlet : $\mathcal{O}_K$

Gustav Lejeune Dirichlet (1805-1859)

XIX^{e} siècle – Généraliser les nombres et les entiers

Arithmétique des idéaux



Ernst Kummer (1810–1893)

Richard Dedekind (1831–1916)

Début XX^{e} – Résultats généraux de finitude diophantienne

- Approximabilité diophantienne – Thue-Mahler-Roth
- Formes binaires – équations de Thue-Mahler
- Équation aux S-unités – Théorème de Mahler.

Début XX^{e} – Résultats généraux de finitude diophantienne

- Approximabilité diophantienne – Thue-Mahler-Roth

Degré d'irrationnalité de $\alpha \in \mathbb{R}$

$$\sup\left\{\beta \in \mathbb{R}_+ \,\middle|\, |\alpha - \frac{p}{q}| \leq q^{-\beta} \text{ pour une infinité de } p \wedge q = 1\right\}.$$

  - 1 pour rationnels (Dirichlet, milieu XIX^{e})
  - 2 pour algébriques non rationnels (Thue-Mahler-Roth, 1955)
- Formes binaires – équations de Thue-Mahler
- Équation aux S-unités – Théorème de Mahler.

Début XX^{e} – Résultats généraux de finitude diophantienne

- Approximabilité diophantienne – Thue-Mahler-Roth
- Formes binaires – équations de Thue-Mahler

Théorème (Thue, 1909)

Soit $F = a_0X^n + a_1X^{n-1}Y + \cdots + Y^n \in \mathbb{Q}[X, Y]$, irréductible, de degré $n \geq 3$.
Pour tout $m \in \mathbb{N}^*$, l'équation

$$F(p, q) = m$$

n'admet qu'un nombre fini de solutions $p, q \in \mathbb{Z}$.

- Équation aux S-unités – Théorème de Mahler.

Début XX^{e} – Résultats généraux de finitude diophantienne

- Approximabilité diophantienne – Thue-Mahler-Roth
- Formes binaires – équations de Thue-Mahler
- Équation aux S-unités – Théorème de Mahler.

Théorème (Mahler, 1933)

Pour tous premiers distincts $p_1, ..., p_a, p_{a+1}, ..., p_b, p_{b+1}, ..., p_c$, l'équation

$$p_1^{e_1} \cdots p_a^{e_a} \pm p_{a+1}^{e_{a+1}} \cdots p_b^{e_b} = \pm p_{b+1}^{e_{b+1}} \cdots p_c^{e_c}$$

n'admet qu'un nombre fini de solutions en les exposants $e_1, ..., e_c \in \mathbb{Z}$.

Début XX^{e} – Résultats généraux de finitude diophantienne

- Approximabilité diophantienne – Thue-Mahler-Roth
- Formes binaires – équations de Thue-Mahler
- Équation aux S-unités – Théorème de Mahler.

Théorème (Mahler, 1933)

Soit $S = \{p_1, ..., p_s\}$ un ensemble de nombres premiers distincts. Notons $\mathbb{Z}_S = \mathbb{Z}[p_1^{-1}, ..., p_s^{-1}]$. L'équation d'inconnues $x, y \in \mathbb{Z}_S^{\times}$

$$x + y = 1$$

admet un nombre fini de solutions.

Morale moderne : la géométrie gouverne l'arithmétique

Théorème (Faltings, 1983)

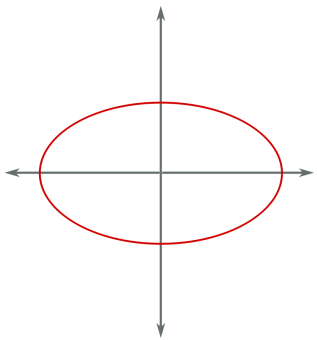
Soient $P \in \mathbb{Q}[Y, Z]$ et C la courbe définie par

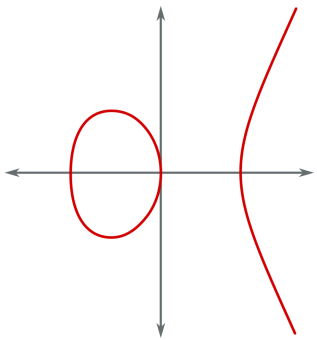
$$C = \{y, z \in \mathbb{Q} \mid P(y, z) = 0\},$$

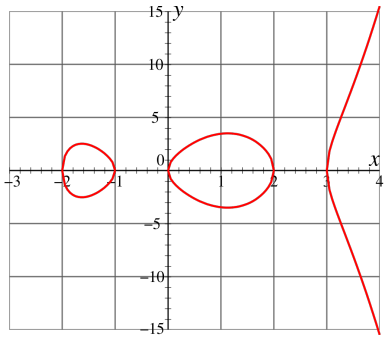
et soit X le nombre de points rationnels de C.

- Si C est de genre 0, $X = 0$ ou $X = \infty$.
- Si C est de genre 1, $X = 0$ ou $X = \infty$ mais C peut être muni d'une structure de groupe abélien de type fini. (Mordell, 1922)
- Si C est de genre ≥ 2, $X < \infty$. (Faltings)

Faltings (1953–)







Et maintenant ? Expliciter.

- Question contemporaine : expliciter le théorème de Faltings
- Divers nouveaux outils
- Équation aux S-unités : beaucoup de résultats explicites
  Stratégie toujours puissante, sujet actif, ...
  On a étudié une preuve issue de la géométrie des nombres, conçue par Beukers et Schlickewei en 1996.

L'équation aux S-unités

Corps de nombres

L'objet de base sur lequel nous travaillons est celui des *corps de nombres*.

Définition : corps de nombres

Un corps de nombres K est une extension finie de $\mathbb{Q}$.

Corps de nombres

L'objet de base sur lequel nous travaillons est celui des *corps de nombres*.

Définition : corps de nombres

Un corps de nombres K est une extension finie de $\mathbb{Q}$.

Exemple

Pour résoudre l'équation de Pell-Fermat $a^2 - db^2 = 1$ d'inconnue $(a, b) \in \mathbb{Z}^2$, il est utile de se placer dans $\mathbb{Q}[\sqrt{d}]$.

Corps de nombres

L'objet de base sur lequel nous travaillons est celui des *corps de nombres*.

Définition : corps de nombres

Un corps de nombres K est une extension finie de $\mathbb{Q}$.

Exemple

Pour résoudre l'équation de Pell-Fermat $a^2 - db^2 = 1$ d'inconnue $(a, b) \in \mathbb{Z}^2$, il est utile de se placer dans $\mathbb{Q}[\sqrt{d}]$.

Un corps de nombres K ressemble à $\mathbb{Q}$, quel serait l'analogue des éléments entiers ?

Anneau des entiers

Définition : anneau des entiers

Soient K un corps de nombres et $x \in K$. On dit que x est un *entier algébrique* si le polynôme minimal de x sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$.
On note $\mathcal{O}_K$ l'ensemble des entiers algébriques de K.

Anneau des entiers

Définition : anneau des entiers

Soient K un corps de nombres et $x \in K$. On dit que x est un *entier algébrique* si le polynôme minimal de x sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$.
On note $\mathcal{O}_K$ l'ensemble des entiers algébriques de K.

Proposition

Soit K un corps de nombres.

- $\mathcal{O}_K$ est un anneau.
- Le corps des fractions de $\mathcal{O}_K$ est K.

Anneau des entiers

Propositions et exemples

K corps de nombres	$\mathcal{O}_K$ son anneau des entiers
$\mathbb{Q}$	$\mathbb{Z}$
$\mathbb{Q}[i]$	$\mathbb{Z}[i]$
$\mathbb{Q}[i\sqrt{5}]$	$\mathbb{Z}[i\sqrt{5}]$
$\mathbb{Q}[\sqrt{5}]$	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$

Arithmétique sur $\mathbb{Z}$

Sur $\mathbb{Z}$, on dispose du théorème fondamental suivant :

Théorème fondamental de l'arithmétique

Tout nombre entier strictement positif admet une unique factorisation comme produit de nombres premiers à l'ordre des facteurs près.

On généralise cela aux rationnels en écrivant $x = \frac{a}{b}$.

Arithmétique sur $\mathbb{Z}$

Sur $\mathbb{Z}$, on dispose du théorème fondamental suivant :

Théorème fondamental de l'arithmétique

Tout nombre entier strictement positif admet une unique factorisation comme produit de nombres premiers à l'ordre des facteurs près.

On généralise cela aux rationnels en écrivant $x = \frac{a}{b}$.
Qu'en est-il sur $\mathcal{O}_K$?

Arithmétique sur $\mathbb{Z}$

Sur $\mathbb{Z}$, on dispose du théorème fondamental suivant :

Théorème fondamental de l'arithmétique

Tout nombre entier strictement positif admet une unique factorisation comme produit de nombres premiers à l'ordre des facteurs près.

On généralise cela aux rationnels en écrivant $x = \frac{a}{b}$.
Qu'en est-il sur $\mathcal{O}_K$?

Exemple

Pour $K = \mathbb{Q}[i\sqrt{5}]$, on a $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$, et :

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

Arithmétique sur $\mathbb{Z}$

Sur $\mathbb{Z}$, on dispose du théorème fondamental suivant :

Théorème fondamental de l'arithmétique

Tout nombre entier strictement positif admet une unique factorisation comme produit de nombres premiers à l'ordre des facteurs près.

On généralise cela aux rationnels en écrivant $x = \frac{a}{b}$.
Qu'en est-il sur $\mathcal{O}_K$?

Exemple

Pour $K = \mathbb{Q}[i\sqrt{5}]$, on a $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$, et :

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

Le théorème fondamental n'est pas valable sur $\mathcal{O}_K$!

Arithmétique sur $\mathcal{O}_K$: les idéaux

Définition : idéal

Soit A un anneau. On appelle idéal de A tout sous-groupe additif qui est de plus stable par multiplication par les éléments de l'anneau.

Arithmétique sur $\mathcal{O}_K$: les idéaux

Définition : idéal

Soit A un anneau. On appelle idéal de A tout sous-groupe additif qui est de plus stable par multiplication par les éléments de l'anneau.

Les idéaux généralisent la notion de diviseur.

Exemple

Sur $\mathbb{Z}$, les idéaux sont exactement les $n\mathbb{Z}$ où $n \in \mathbb{Z}$.

Arithmétique sur $\mathcal{O}_K$: les idéaux

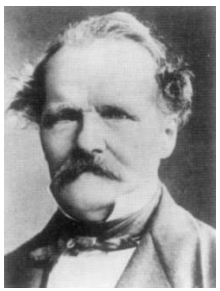
Définition : idéal

Soit A un anneau. On appelle idéal de A tout sous-groupe additif qui est de plus stable par multiplication par les éléments de l'anneau.

Les idéaux généralisent la notion de diviseur.

Exemple

Sur $\mathbb{Z}$, les idéaux sont exactement les $n\mathbb{Z}$ où $n \in \mathbb{Z}$.



Ernst Kummer (1810-1893)

Richard Dedekind (1831-1916)

Arithmétique sur $\mathcal{O}_K$

Théorème de Dedekind

Tout idéal non nul de $\mathcal{O}_K$ admet une unique décomposition comme produit d'idéaux premiers, à l'ordre des facteurs près.

Arithmétique sur $\mathcal{O}_K$

Théorème de Dedekind

Tout idéal non nul de $\mathcal{O}_K$ admet une unique décomposition comme produit d'idéaux premiers, à l'ordre des facteurs près.

La preuve est géométrique, et repose sur la théorie des réseaux.

Conséquences

- Cela permet de parler de la décompositions des éléments de $\mathcal{O}_K$ en regardant les idéaux principaux.

Conséquences

- Cela permet de parler de la décompositions des éléments de $\mathcal{O}_K$ en regardant les idéaux principaux.

Exemple

Dans $\mathbb{Z}[i\sqrt{5}]$:

$$(2) = (1 + i\sqrt{5}, 1 - i\sqrt{5}) \times (1 + i\sqrt{5}, 1 - i\sqrt{5})$$
$$(3) = (1 + i\sqrt{5}, 3) \times (1 - i\sqrt{5}, 3)$$

Conséquences

- Cela permet de parler de la décompositions des éléments de $\mathcal{O}_K$ en regardant les idéaux principaux.

Exemple

Dans $\mathbb{Z}[i\sqrt{5}]$:

$$(2) = (1 + i\sqrt{5}, 1 - i\sqrt{5}) \times (1 + i\sqrt{5}, 1 - i\sqrt{5})$$
$$(3) = (1 + i\sqrt{5}, 3) \times (1 - i\sqrt{5}, 3)$$

- On peut étendre la notion de décomposition aux éléments de $x \in K$ via $x = \frac{a}{b}$ où $a, b \in \mathcal{O}_K$.

Conséquences

- Cela permet de parler de la décompositions des éléments de $\mathcal{O}_K$ en regardant les idéaux principaux.

Exemple

Dans $\mathbb{Z}[i\sqrt{5}]$:

$$(2) = (1 + i\sqrt{5}, 1 - i\sqrt{5}) \times (1 + i\sqrt{5}, 1 - i\sqrt{5})$$
$$(3) = (1 + i\sqrt{5}, 3) \times (1 - i\sqrt{5}, 3)$$

- On peut étendre la notion de décomposition aux éléments de $x \in K$ via $x = \frac{a}{b}$ où $a, b \in \mathcal{O}_K$.
- On dispose de fonctions de valuations $\mathfrak{p}$-adiques $v_{\mathfrak{p}}$ sur K.

Conséquences

- Cela permet de parler de la décompositions des éléments de $\mathcal{O}_K$ en regardant les idéaux principaux.

Exemple

Dans $\mathbb{Z}[i\sqrt{5}]$:

$$(2) = (1 + i\sqrt{5}, 1 - i\sqrt{5}) \times (1 + i\sqrt{5}, 1 - i\sqrt{5})$$
$$(3) = (1 + i\sqrt{5}, 3) \times (1 - i\sqrt{5}, 3)$$

- On peut étendre la notion de décomposition aux éléments de $x \in K$ via $x = \frac{a}{b}$ où $a, b \in \mathcal{O}_K$.
- On dispose de fonctions de valuations $\mathfrak{p}$-adiques $v_\mathfrak{p}$ sur K.
- Attention ! Les idéaux effacent les unités.

Les S-unités

Nous sommes armés pour définir les S-unités :

Définition : ensemble des S-unités $\mathcal{O}_{K,S}^{\times}$

Soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. On dit que $x \in K$ est une S-unité si la décomposition x ne fait intervenir que des idéaux de S. Ainsi :

$$\mathcal{O}_{K,S}^{\times} = \left\{ x \in K \,\middle|\, \forall \mathfrak{p} \notin S \; v_{\mathfrak{p}}(x) = 0 \right\}.$$

Les S-unités

Nous sommes armés pour définir les S-unités :

Définition : ensemble des S-unités $\mathcal{O}_{K,S}^{\times}$

Soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. On dit que $x \in K$ est une S-unité si la décomposition x ne fait intervenir que des idéaux de S. Ainsi :

$$\mathcal{O}_{K,S}^{\times} = \left\{ x \in K \,\middle|\, \forall \mathfrak{p} \notin S \; v_{\mathfrak{p}}(x) = 0 \right\}.$$

Les S-unités sont les éléments de K qui ne s'expriment qu'avec S.

Les S-unités

Nous sommes armés pour définir les S-unités :

Définition : ensemble des S-unités $\mathcal{O}_{K,S}^{\times}$

Soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. On dit que $x \in K$ est une S-unité si la décomposition x ne fait intervenir que des idéaux de S. Ainsi :

$$\mathcal{O}_{K,S}^{\times} = \left\{ x \in K \,\middle|\, \forall \mathfrak{p} \notin S \; v_{\mathfrak{p}}(x) = 0 \right\}.$$

Les S-unités sont les éléments de K qui ne s'expriment qu'avec S.

Exemple

Dans $\mathbb{Q}$ avec $S = \{2, 3\}$:

$$\mathcal{O}_{\mathbb{Q},S}^{\times} = \left\{ \pm 2^n 3^m \,\middle|\, n, m \in \mathbb{Z} \right\}.$$

Structure des S-unités

Intuitivement, un élément de $\mathcal{O}_{K,S}^{\times}$ est défini :

- Par les exposants apparaissant dans sa décomposition en idéaux premiers.
- A un facteur unitaire près.

Structure des S-unités

Intuitivement, un élément de $\mathcal{O}_{K,S}^{\times}$ est défini :

- Par les exposants apparaissant dans sa décomposition en idéaux premiers.
- A un facteur unitaire près.

Cette intuition se vérifie :

Proposition

$$\mathcal{O}_{K,S}^{\times} \cong \mathcal{O}_K^{\times} \times \mathbb{Z}^{|S|}.$$

Reste à élucider la structure de $\mathcal{O}_K^{\times}$.

Le théorème des unités de Dirichlet

Théorème des unités de Dirichlet

Le groupe $\mathcal{O}_K^\times$ des unités de $\mathcal{O}_K$ est isomorphe à $\mu(K) \times \mathbb{Z}^r$, où

- $\mu(K)$ est le groupe cyclique des racines de l'unité de $\mathcal{O}_K$, qui est fini.
- r est une valeur qui dépend de K.

La preuve fait intervenir des résultats de la théorie des réseaux, dont le théorème de Minkoswki.

Le théorème des unités de Dirichlet

Théorème des unités de Dirichlet

Le groupe $\mathcal{O}_K^\times$ des unités de $\mathcal{O}_K$ est isomorphe à $\mu(K) \times \mathbb{Z}^r$, où

- $\mu(K)$ est le groupe cyclique des racines de l'unité de $\mathcal{O}_K$, qui est fini.
- r est une valeur qui dépend de K.

La preuve fait intervenir des résultats de la théorie des réseaux, dont le théorème de Minkoswki.

Corollaire

$$\mathcal{O}_{K,S}^\times \cong \mu(K) \times \mathbb{Z}^{r+|S|}.$$

L'équation aux S-unités

Equation aux S-unités

Soit K un corps de nombres. Soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. On appelle *équation aux S-unités* l'équation d'inconnues $x, y \in \mathcal{O}_{K,S}^{\times}$:

$$x + y = 1$$

Cette équation a-t-elle un nombre fini de solutions ?

L'équation aux S-unités

Un cas élémentaire

Dans $\mathbb{Q}$ avec $S = \{2, 3\}$ comme précédemment, résoudre l'équation aux S-unités revient à trouver les solutions de

$$\pm 2^{n_1} 3^{m_1} \pm 2^{n_2} 3^{m_2} = 1$$

d'inconnues $n_1, m_1, n_2, m_2 \in \mathbb{Z}$.

L'équation aux S-unités

Un cas élémentaire

Dans $\mathbb{Q}$ avec $S = \{2, 3\}$ comme précédemment, résoudre l'équation aux S-unités revient à trouver les solutions de

$$\pm 2^{n_1} 3^{m_1} \pm 2^{n_2} 3^{m_2} = 1$$

d'inconnues $n_1, m_1, n_2, m_2 \in \mathbb{Z}$.

On peut montrer avec des outils d'arithmétique élémentaires la finitude de l'ensemble des solutions en l'explicitant.
Bien qu'élémentaire, la preuve *ad hoc* est fastidieuse et fait sentir le besoin d'outils plus complexes et plus puissants pour un résultat général.

Le résultat de finitude sur $\mathbb{Q}$

Théorème : Mahler 1933

Soit $S = \{p_1, ..., p_s\}$ un ensemble de nombres premiers. L'équation d'inconnues $x, y \in \mathcal{O}_{\mathbb{Q},S}^{\times}$

$$x + y = 1$$

admet un nombre fini de solutions.

Kurt Mahler (1903-1988)

Un théorème général et quantitatif

Théorème : Beukers, Schlickewei

Soit H un sous-groupe de $(\mathbb{C}^*)^2$ de type fini de rang sans torsion r. Alors l'équation d'inconnue $(x, y) \in H^2$:

$$x + y = 1$$

admet au plus 2^{16r+8} solutions.

L'énoncé est en fait plus fort, les inconnues peuvent se trouver dans la $\mathbb{Q}$-clôture de H.

L'équation aux S-unités sur K

Rappel : $\mathcal{O}_{K,S}^{\times} \cong \mu(K) \times \mathbb{Z}^{r+|S|}$.

Corollaire

Sur $\mathcal{O}_K$, l'équation aux S-unités admet au plus $2^{16(r+|S|)+8}$ solutions.

Frits Beukers (1953-)

Hans Peter Schlickewei (1947-)

Idée de la preuve

Démarche générale de la preuve

La preuve du théorème de Beukers et Schlickewei repose sur une *géométrisation du problème*.

Démarche générale de la preuve

La preuve du théorème de Beukers et Schlickewei repose sur une *géométrisation du problème*.

1. Le groupe de départ H est transformé en un $\mathbb{Q}$-espace vectoriel de dimension finie.

Démarche générale de la preuve

La preuve du théorème de Beukers et Schlickewei repose sur une *géométrisation du problème*.

1. Le groupe de départ H est transformé en un $\mathbb{Q}$-espace vectoriel de dimension finie.
2. Ce $\mathbb{Q}$-espace vectoriel est muni d'une norme qui mesure la complexité des éléments. Elle est construite à l'aide de la *hauteur*.

Démarche générale de la preuve

La preuve du théorème de Beukers et Schlickewei repose sur une *géométrisation du problème*.

1. Le groupe de départ H est transformé en un $\mathbb{Q}$-espace vectoriel de dimension finie.
2. Ce $\mathbb{Q}$-espace vectoriel est muni d'une norme qui mesure la complexité des éléments. Elle est construite à l'aide de la *hauteur*.
3. Les solutions de l'équation vérifient des propriétés géométriques relativement à cette norme : elles sont éloignées les unes des autres en un certain sens.

Démarche générale de la preuve

La preuve du théorème de Beukers et Schlickewei repose sur une *géométrisation du problème*.

1. Le groupe de départ H est transformé en un $\mathbb{Q}$-espace vectoriel de dimension finie.
2. Ce $\mathbb{Q}$-espace vectoriel est muni d'une norme qui mesure la complexité des éléments. Elle est construite à l'aide de la *hauteur*.
3. Les solutions de l'équation vérifient des propriétés géométriques relativement à cette norme : elles sont éloignées les unes des autres en un certain sens.
4. On étend cette structure à celle d'un $\mathbb{R}$-espace vectoriel de dimension finie, tout en préservant la norme.

Démarche générale de la preuve

La preuve du théorème de Beukers et Schlickewei repose sur une *géométrisation du problème*.

1. Le groupe de départ H est transformé en un $\mathbb{Q}$-espace vectoriel de dimension finie.
2. Ce $\mathbb{Q}$-espace vectoriel est muni d'une norme qui mesure la complexité des éléments. Elle est construite à l'aide de la *hauteur*.
3. Les solutions de l'équation vérifient des propriétés géométriques relativement à cette norme : elles sont éloignées les unes des autres en un certain sens.
4. On étend cette structure à celle d'un $\mathbb{R}$-espace vectoriel de dimension finie, tout en préservant la norme.
5. Le problème devient alors purement géométrique : il s'agit de borner le cardinal d'un ensemble dont les éléments sont éloignés les uns des autres.

Démarche générale de la preuve

La preuve du théorème de Beukers et Schlickewei repose sur une *géométrisation du problème*.

1. Le groupe de départ H est transformé en un $\mathbb{Q}$-espace vectoriel de dimension finie.
2. Ce $\mathbb{Q}$-espace vectoriel est muni d'une norme qui mesure la complexité des éléments. Elle est construite à l'aide de la *hauteur*.
3. Les solutions de l'équation vérifient des propriétés géométriques relativement à cette norme : elles sont éloignées les unes des autres en un certain sens.
4. On étend cette structure à celle d'un $\mathbb{R}$-espace vectoriel de dimension finie, tout en préservant la norme.
5. Le problème devient alors purement géométrique : il s'agit de borner le cardinal d'un ensemble dont les éléments sont éloignés les uns des autres.

Construction de la norme : la hauteur

- **Objectif** : Trouver une norme adaptée au problème. Elle doit mesurer la *complexité arithmétique des nombres*.

Construction de la norme : la hauteur

- **Objectif** : Trouver une norme adaptée au problème. Elle doit mesurer la *complexité arithmétique des nombres*.
- Les solutions de l'équation aux S-unités vérifient des propriétés arithmétiques : on en déduira des résultats géométriques dans notre espace vectoriel normé.

Construction de la norme : la hauteur

- **Objectif** : Trouver une norme adaptée au problème. Elle doit mesurer la *complexité arithmétique des nombres*.
- Les solutions de l'équation aux S-unités vérifient des propriétés arithmétiques : on en déduira des résultats géométriques dans notre espace vectoriel normé.
- La *hauteur* d'un nombre est une réponse possible à cette question. Les nombres de faible hauteur (et donc de faible complexité) sont en nombre fini.

Construction de la norme : la hauteur

- **Objectif** : Trouver une norme adaptée au problème. Elle doit mesurer la *complexité arithmétique des nombres*.
- Les solutions de l'équation aux S-unités vérifient des propriétés arithmétiques : on en déduira des résultats géométriques dans notre espace vectoriel normé.
- La *hauteur* d'un nombre est une réponse possible à cette question. Les nombres de faible hauteur (et donc de faible complexité) sont en nombre fini.

André Weil (1906-1998)

La hauteur sur $\mathbb{Q}$

Sur $\mathbb{Q}$, la hauteur a une expression très simple.

Définition : hauteur

Soit $\frac{a}{b} \in \mathbb{Q}$ écrit sous forme de fraction irréductible. On appelle *hauteur* de $\frac{a}{b}$ le nombre :

$$H(\frac{a}{b}) = \max(|a|, |b|).$$

La hauteur sur $\mathbb{Q}$

Sur $\mathbb{Q}$, la hauteur a une expression très simple.

Définition : hauteur

Soit $\frac{a}{b} \in \mathbb{Q}$ écrit sous forme de fraction irréductible. On appelle *hauteur* de $\frac{a}{b}$ le nombre :

$$H(\frac{a}{b}) = \max(|a|, |b|).$$

Exemple

$\frac{121}{60} \simeq 2$, mais $H(\frac{121}{60}) = 121$ alors que $H(2) = 2$.

Quelques propriétés de la hauteur sur $\mathbb{Q}$

Proposition

- $H(x^n) = H(x)^n$.
- $H(xy) \leq H(x)H(y)$
- $H(x) = 1 \Leftrightarrow x = \pm 1$

Quelques propriétés de la hauteur sur $\mathbb{Q}$

Proposition

- $H(x^n) = H(x)^n$.
- $H(xy) \leq H(x)H(y)$
- $H(x) = 1 \Leftrightarrow x = \pm 1$

La définition permet aussi d'obtenir un résultat de finitude.

Théorème de Northcott sur $\mathbb{Q}$

Soit $M \in \mathbb{N}$.

$$\text{L'ensemble } \left\{ x \in \mathbb{Q} \,\middle|\, H(x) \leq M \right\} \text{ est fini.}$$

Quelques propriétés de la hauteur sur $\mathbb{Q}$

Proposition

- $H(x^n) = H(x)^n$.
- $H(xy) \leq H(x)H(y)$
- $H(x) = 1 \Leftrightarrow x = \pm 1$

La définition permet aussi d'obtenir un résultat de finitude.

Théorème de Northcott sur $\mathbb{Q}$

Soit $M \in \mathbb{N}$.

$$\text{L'ensemble } \left\{ x \in \mathbb{Q} \,\middle|\, H(x) \leq M \right\} \text{ est fini.}$$

Les nombres rationnels de faible complexité sont en nombre fini.

La hauteur sur des corps de nombres

- La hauteur sur $\mathbb{Q}$ a une définition simple, mais peut aussi être construite comme une combinaison de toutes les *valeurs absolues* disponibles sur $\mathbb{Q}$.

La hauteur sur des corps de nombres

- La hauteur sur $\mathbb{Q}$ a une définition simple, mais peut aussi être construite comme une combinaison de toutes les *valeurs absolues* disponibles sur $\mathbb{Q}$.
- Cette construction peut s'étendre à tout corps de nombres. Les propriétés que l'on avait sur $\mathbb{Q}$ sont conservées.

La hauteur sur des corps de nombres

- La hauteur sur $\mathbb{Q}$ a une définition simple, mais peut aussi être construite comme une combinaison de toutes les *valeurs absolues* disponibles sur $\mathbb{Q}$.
- Cette construction peut s'étendre à tout corps de nombres. Les propriétés que l'on avait sur $\mathbb{Q}$ sont conservées.
- La norme de notre problème est alors obtenue en prenant le logarithme de la hauteur.

La hauteur sur des corps de nombres

- La hauteur sur $\mathbb{Q}$ a une définition simple, mais peut aussi être construite comme une combinaison de toutes les *valeurs absolues* disponibles sur $\mathbb{Q}$.
- Cette construction peut s'étendre à tout corps de nombres. Les propriétés que l'on avait sur $\mathbb{Q}$ sont conservées.
- La norme de notre problème est alors obtenue en prenant le logarithme de la hauteur.
- Les solutions sont bien éloignées des unes des autres grâce aux propriétés de finitude.

La hauteur sur des corps de nombres

- La hauteur sur $\mathbb{Q}$ a une définition simple, mais peut aussi être construite comme une combinaison de toutes les *valeurs absolues* disponibles sur $\mathbb{Q}$.
- Cette construction peut s'étendre à tout corps de nombres. Les propriétés que l'on avait sur $\mathbb{Q}$ sont conservées.
- La norme de notre problème est alors obtenue en prenant le logarithme de la hauteur.
- Les solutions sont bien éloignées des unes des autres grâce aux propriétés de finitude.

La hauteur permet bien de construire une norme adaptée au problème.

Raisonnements géométriques

On se place donc maintenant dans un $\mathbb{R}$-espace vectoriel de dimension finie muni de notre norme. Les solutions vérifient des propriétés géométriques.

Raisonnements géométriques

On se place donc maintenant dans un $\mathbb{R}$-espace vectoriel de dimension finie muni de notre norme. Les solutions vérifient des propriétés géométriques.

- On montre d'abord qu'il existe un R tel que les solutions de norme $||x|| \geq R$ sont en nombre fini.
- On montre ensuite que dans toute boule centrée en l'origine il ne peut y avoir qu'un nombre fini de solutions.
- On dispose de bornes explicites dans les deux cas.

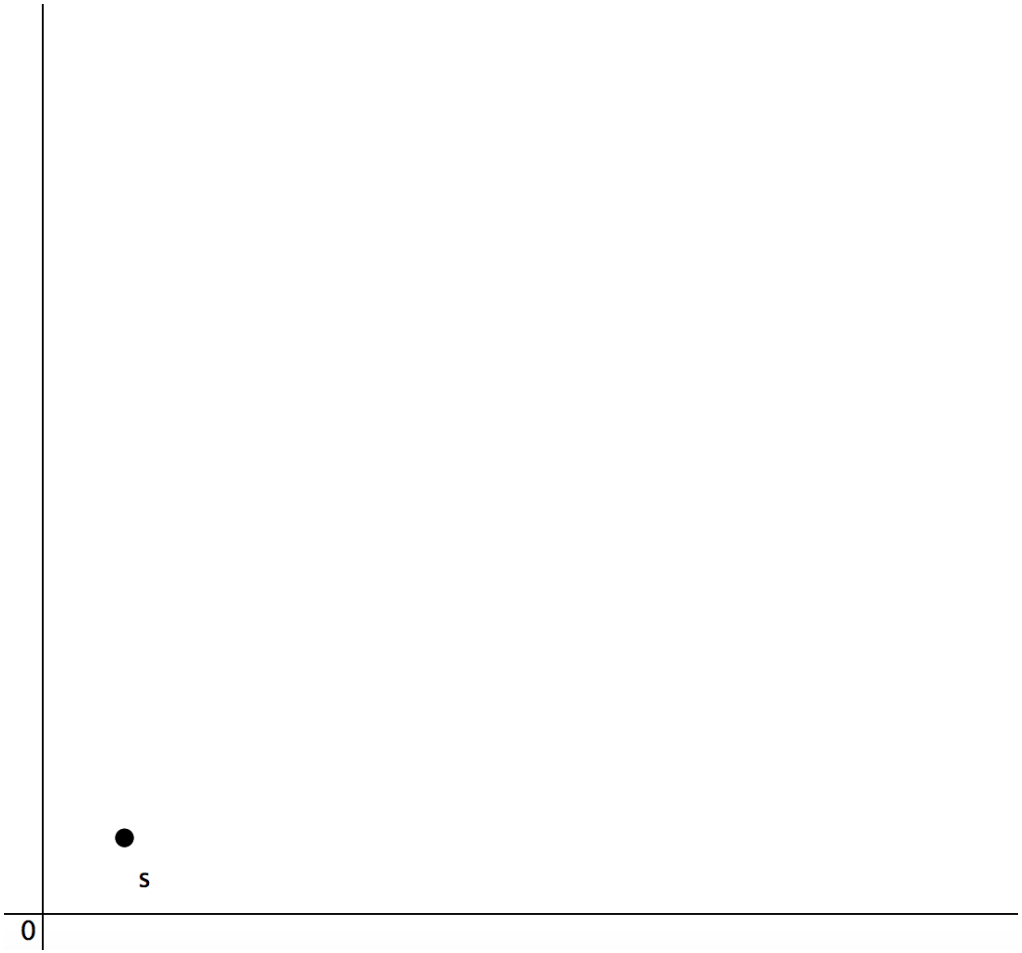
Raisonnements géométriques

On se place donc maintenant dans un $\mathbb{R}$-espace vectoriel de dimension finie muni de notre norme. Les solutions vérifient des propriétés géométriques.

- On montre d'abord qu'il existe un R tel que les solutions de norme $||x|| \geq R$ sont en nombre fini.
- On montre ensuite que dans toute boule centrée en l'origine il ne peut y avoir qu'un nombre fini de solutions.
- On dispose de bornes explicites dans les deux cas.

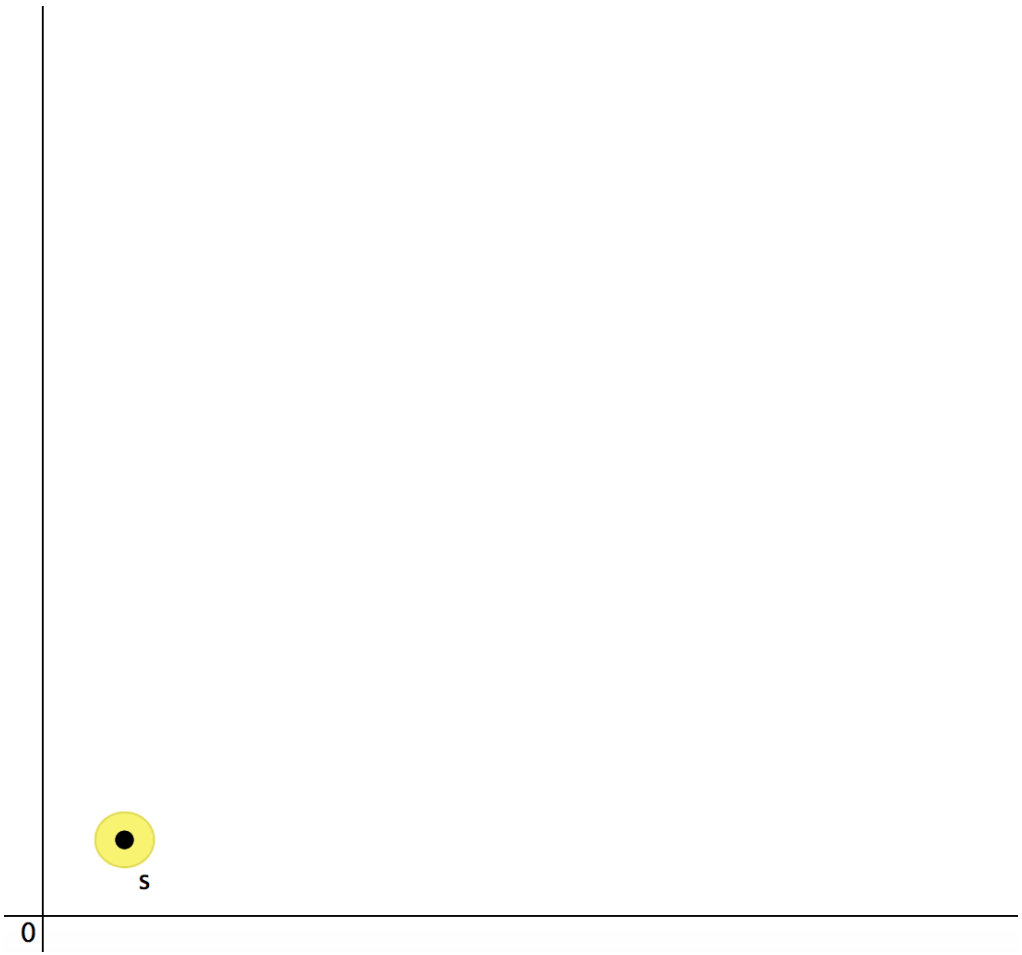
Les raisonnement utilisés sont valables dans n'importe quel espace vectoriel normé de dimension finie.

Quelques constructions typiques : loin de l'origine



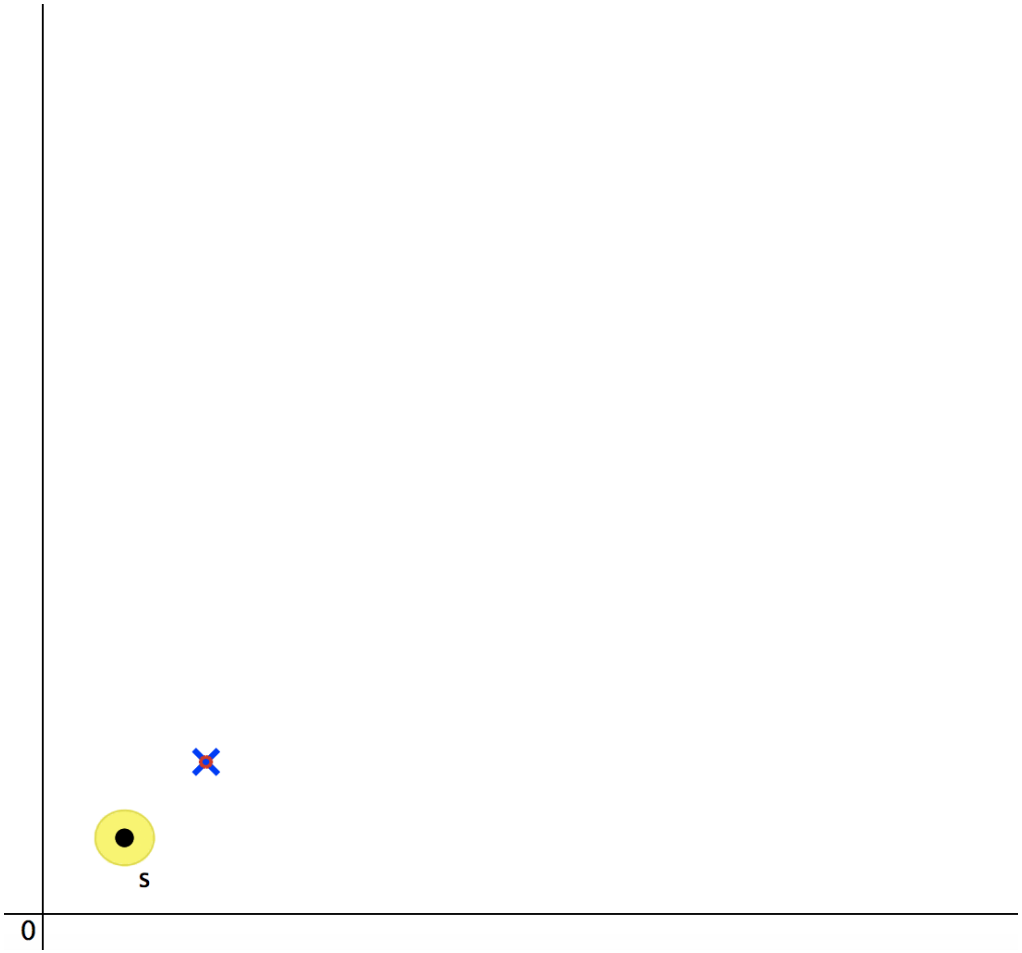
- On se donne une solution s loin de l'origine.

Quelques constructions typiques : loin de l'origine



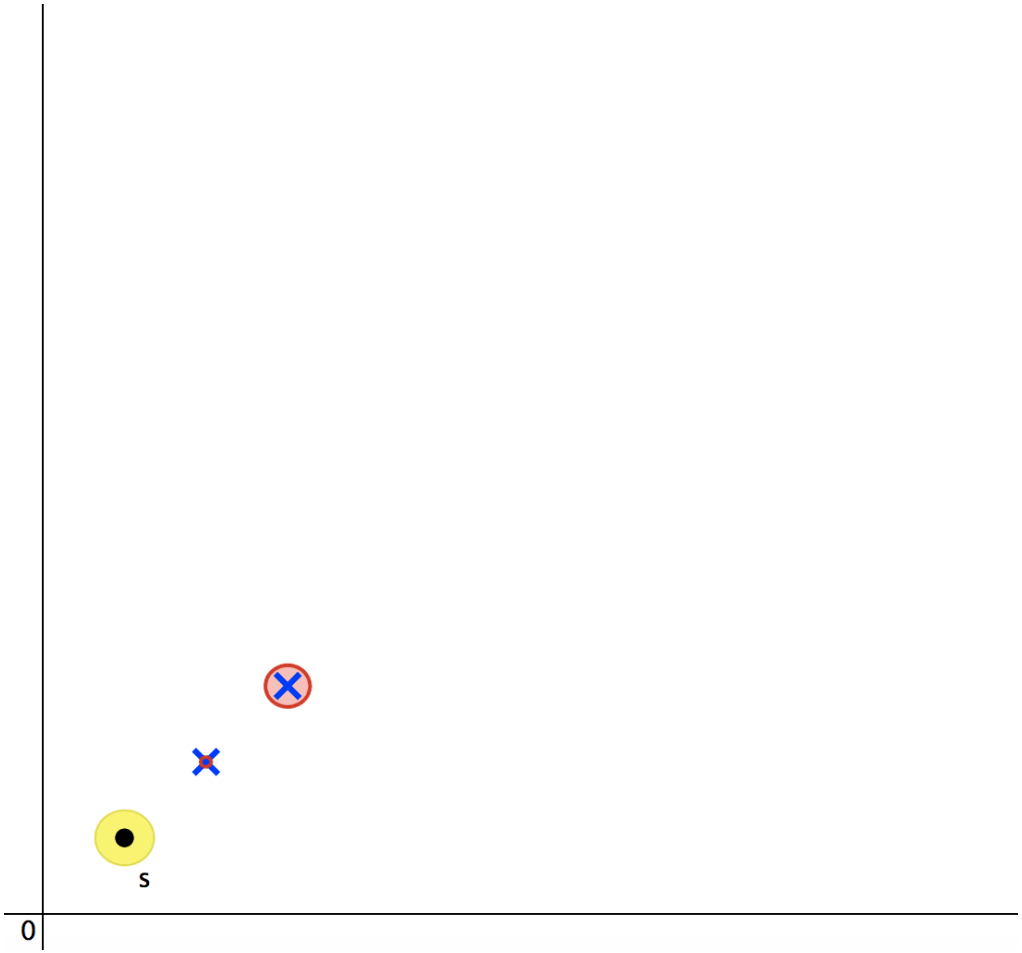
- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.

Quelques constructions typiques : loin de l'origine



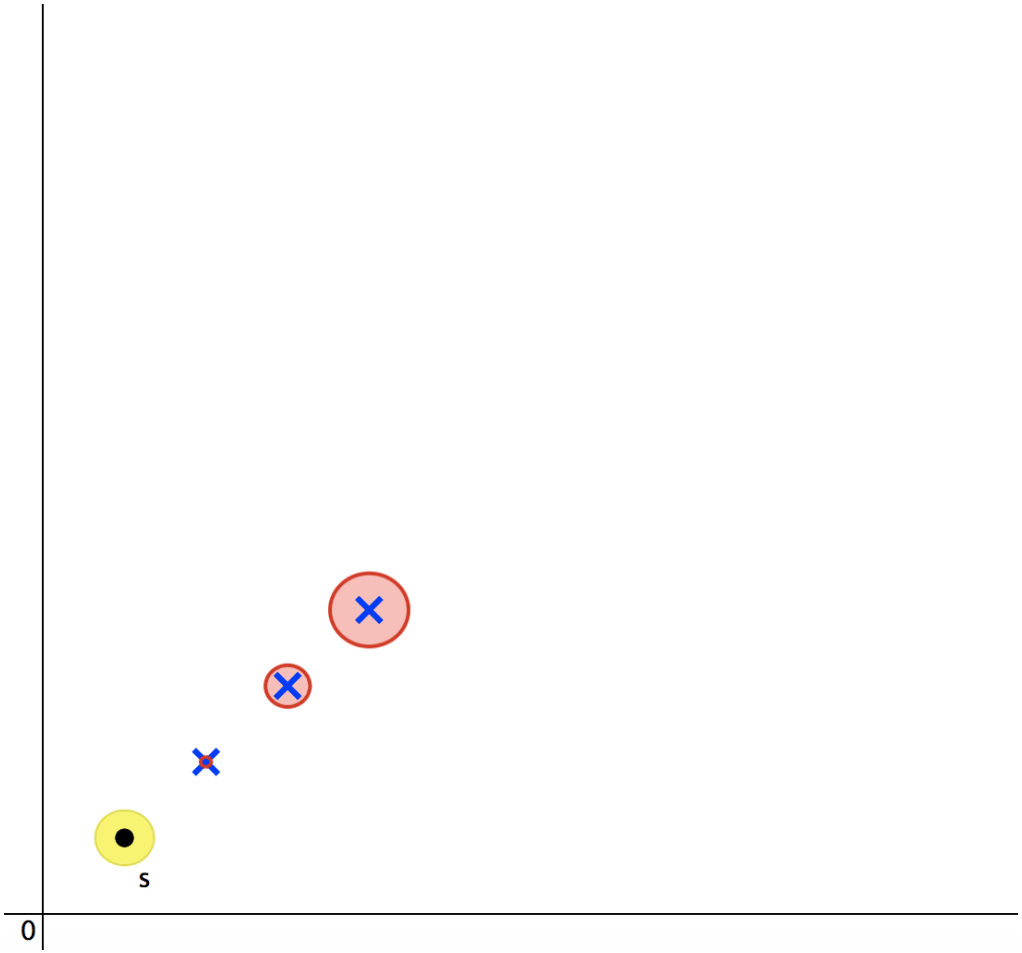
- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.
- Pas d'autres solutions dans les cercles rouges.

Quelques constructions typiques : loin de l'origine



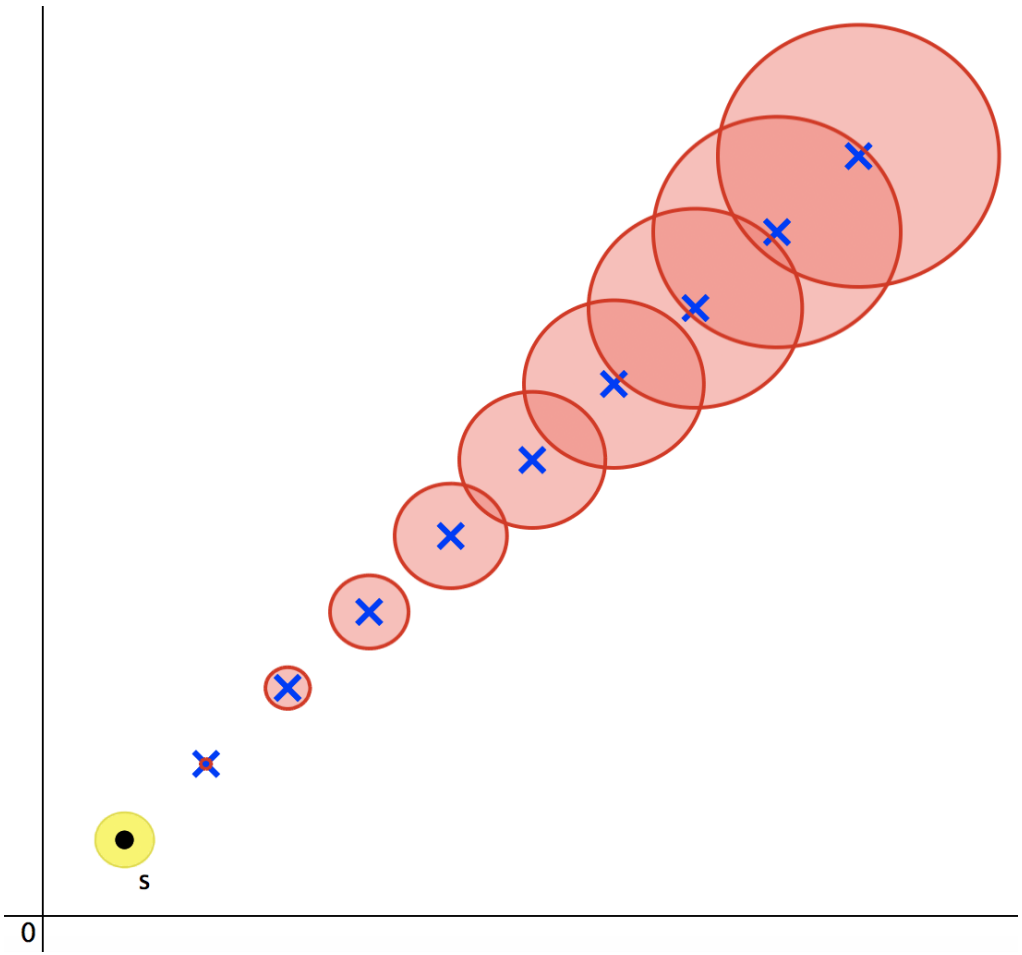
- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.
- Pas d'autres solutions dans les cercles rouges.

Quelques constructions typiques : loin de l'origine



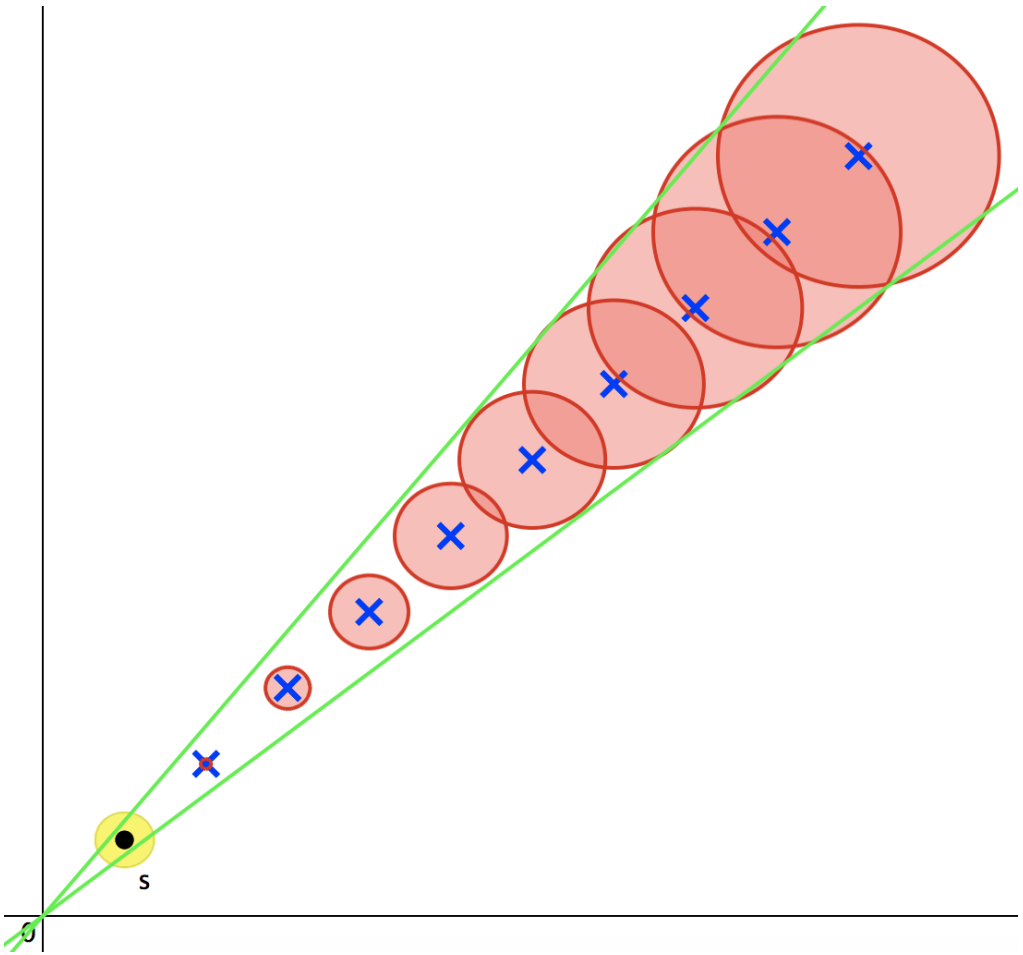
- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.
- Pas d'autres solutions dans les cercles rouges.

Quelques constructions typiques : loin de l'origine



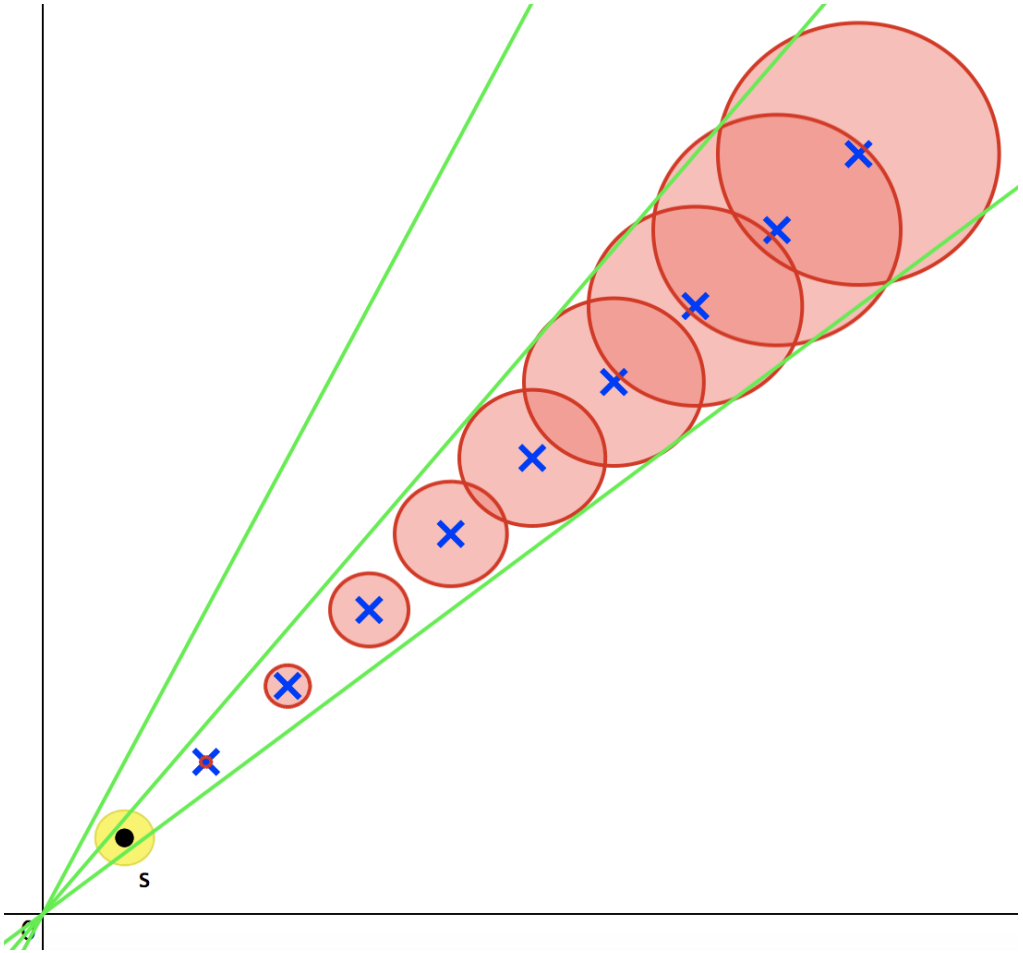
- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.
- Pas d'autres solutions dans les cercles rouges.

Quelques constructions typiques : loin de l'origine



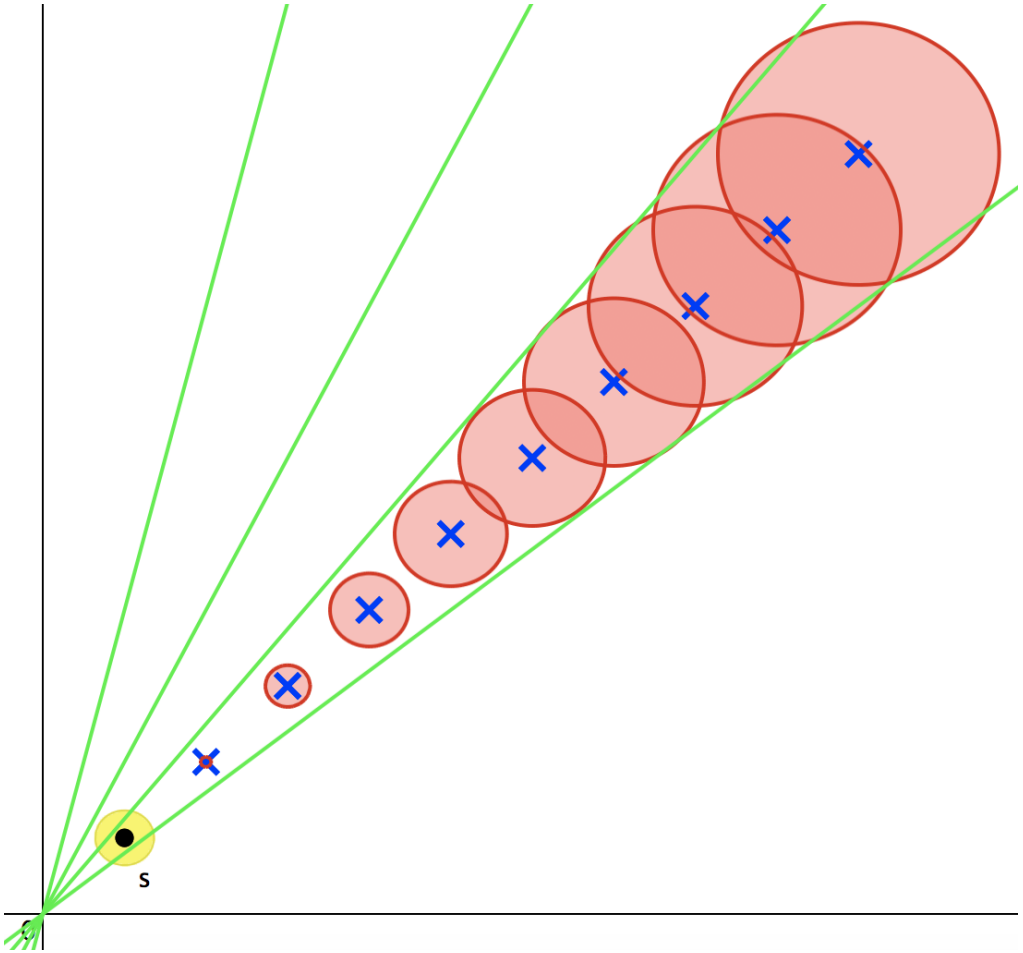
- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.
- Pas d'autres solutions dans les cercles rouges.
- On contrôle le nombre de solutions dans le cône.

Quelques constructions typiques : loin de l'origine



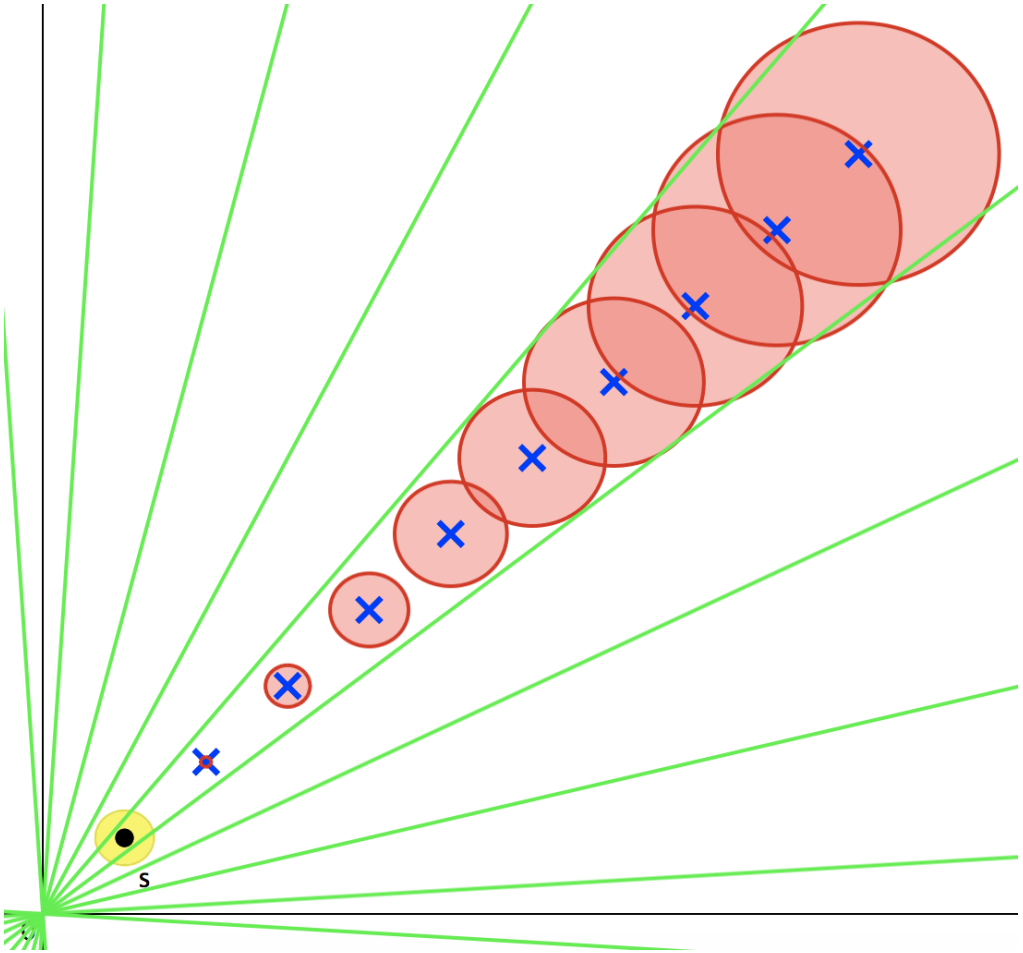
- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.
- Pas d'autres solutions dans les cercles rouges.
- On contrôle le nombre de solutions dans le cône.
- On pave l'espace avec un nombre fini de cônes.

Quelques constructions typiques : loin de l'origine



- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.
- Pas d'autres solutions dans les cercles rouges.
- On contrôle le nombre de solutions dans le cône.
- On pave l'espace avec un nombre fini de cônes.

Quelques constructions typiques : loin de l'origine



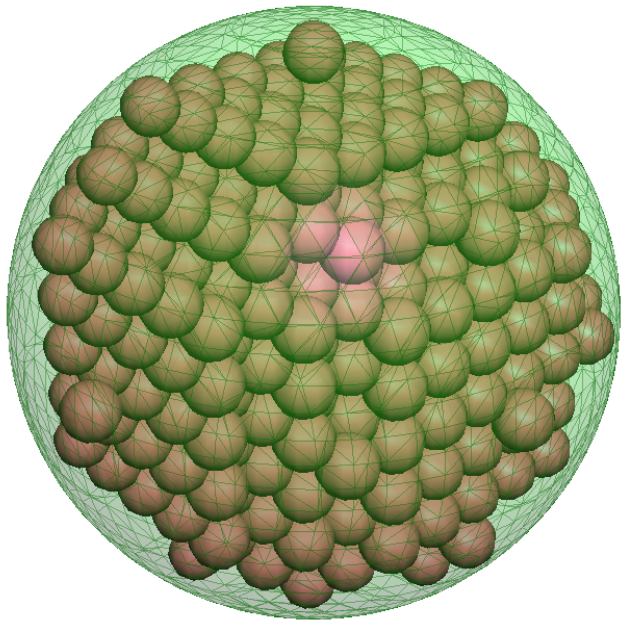
- On se donne une solution s loin de l'origine.
- Pas d'autres solutions dans le cercle jaune.
- Pas d'autres solutions dans les cercles rouges.
- On contrôle le nombre de solutions dans le cône.
- On pave l'espace avec un nombre fini de cônes.

Quelques constructions typiques : proche de l'origine

On montre qu'il existe une constante C telle que trois solutions ne peuvent se trouver dans une même boule de rayon C.

Quelques constructions typiques : proche de l'origine

On montre qu'il existe une constante C telle que trois solutions ne peuvent se trouver dans une même boule de rayon C.
Cela permet d'obtenir une majoration explicite du nombre de solutions dans notre boule de rayon R.



Une preuve géométrique

- Les bornes obtenues sont explicites.

Une preuve géométrique

- Les bornes obtenues sont explicites.
- En contrôlant le rayon R de la boule, on optimise leur somme en 2^{16r+8}.

Une preuve géométrique

- Les bornes obtenues sont explicites.
- En contrôlant le rayon R de la boule, on optimise leur somme en 2^{16r+8}.

Le problème était arithmétique, mais la preuve utilise des raisonnements géométriques.

Exemples & Applications

Un théorème de Siegel

Le théorème suivant peut-être obtenu à l'aide des résultats de finitude sur les S-unités. Il s'agit d'un cas particulier du théorème de Siegel (1929).

Théorème de Siegel

Soit K un corps de nombres, soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. Soit $f(X) \in K[X]$ ayant au moins trois racines simples. Alors l'équation d'inconnues $x, y \in \mathcal{O}_{K,S}$

$$y^2 = f(x)$$

a un nombre fini de solutions.

Un théorème de Siegel

Le théorème suivant peut-être obtenu à l'aide des résultats de finitude sur les S-unités. Il s'agit d'un cas particulier du théorème de Siegel (1929).

Théorème de Siegel

Soit K un corps de nombres, soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. Soit $f(X) \in K[X]$ ayant au moins trois racines simples. Alors l'équation d'inconnues $x, y \in \mathcal{O}_{K,S}$

$$y^2 = f(x)$$

a un nombre fini de solutions.

Ce théorème est une forme plus faible que le théorème de Faltings, dans le cas des courbes hyperelliptiques. Il permet de parcourir tous les genres $g \geq 1$.

Un corollaire

Pour $K = \mathbb{Q}$, $S = \emptyset$, on a le résultat suivant :

Corollaire

Soit $f(X) \in \mathbb{Q}[X]$ avec au moins trois racines simples. Alors l'équation

$$y^2 = f(x)$$

a un nombre fini de solutions entières.

Carl Siegel (1896-1981)

Conclusion

Conclusion

- L'équation aux S-unités est un sujet central en arithmétique, lié à des théorèmes importants.

Conclusion

- L'équation aux S-unités est un sujet central en arithmétique, lié à des théorèmes importants.
- L'étude de ce problème fait intervenir des notions d'algèbre, de géométrie des nombres ou encore d'analyse complexe.

Conclusion

- L'équation aux S-unités est un sujet central en arithmétique, lié à des théorèmes importants.
- L'étude de ce problème fait intervenir des notions d'algèbre, de géométrie des nombres ou encore d'analyse complexe.
- La preuve de Beukers et Schlickewei est de nature géométrique : elle repose sur la construction d'un $\mathbb{R}$-espace vectoriel muni d'une norme adaptée.

Conclusion

- L'équation aux S-unités est un sujet central en arithmétique, lié à des théorèmes importants.
- L'étude de ce problème fait intervenir des notions d'algèbre, de géométrie des nombres ou encore d'analyse complexe.
- La preuve de Beukers et Schlickewei est de nature géométrique : elle repose sur la construction d'un $\mathbb{R}$-espace vectoriel muni d'une norme adaptée.

Merci de votre attention !