

PellFermatCoursTdM15012009.pdf - Adobe Reader

Fichier Edition Affichage Document Outils Fenêtre Aide

68 / 179 155% Rechercher

Une infinité de solution

non triviale en entiers > 0

S'il y a une solution (x_1, y_1) il y en a une infinité, obtenues en écrivant

$$(x_1 + y_1\sqrt{d})^n = x_n + y_n\sqrt{d}$$

pour $n = 1, 2, \dots$

On ordonne les solutions selon $x + y\sqrt{d}$ (il revient au même de prendre l'ordre donné par x , ou celui donné par y). Il existe donc une solution > 1 minimale, on l'appelle la solution fondamentale de l'équation.

30 / 65

Groupes abéliens de type fini.

Groupe abélien = \mathbb{Z} -module.

$$\begin{array}{l} \text{"} \\ A \end{array} \quad \mathbb{Z} \times A \rightarrow A$$

$$(n, \alpha) \mapsto n\alpha$$

$$n\alpha = \begin{cases} \alpha + \dots + \alpha & n > 0 \\ 0 & n = 0 \\ -|\alpha| & n < 0 \end{cases}$$

Def.

\mathbb{Z} -module de type fini.

A

$$\exists \alpha_1, \dots, \alpha_m \in A$$

Eq $A = \mathbb{Z}$ -module engendré par $\alpha_1, \dots, \alpha_m$

$$= \left\{ k_1\alpha_1 + \dots + k_m\alpha_m; k_i \in \mathbb{Z} \right\}$$

$$= \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_m$$

Théorème de structure des \mathbb{Z} -modules de type fini

A un \mathbb{Z} -module de type fini

$$A \cong_{\text{is.}} T \times \mathbb{Z}^r \quad T \text{ groupe abélien fini}$$

$r = \text{rang de } A$

r entier ≥ 0

Sous-groupe de torsion $A_{\text{tors}} \cong T$

$$= \{ \text{éléments d'ordre fini} \}$$

$$x^2 - dy^2 = \pm 1 \quad (x, y) \in \mathbb{Z} \times \mathbb{Z}.$$

Groupe abélien G sous-ensemble de $\mathbb{Z} \times \mathbb{Z}$

$$\begin{array}{l} (x_1, y_1) \\ (x_2, y_2) \end{array} \quad \begin{array}{l} (x_1 + \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) = x_3 + \sqrt{d}y_3 \\ \rightarrow (x_3, y_3) \end{array}$$

groupe multiplicatif

élément neutre $(1, 0)$ "solution triviale"

$(-1, 0) \in G$ d'ordre 2

$$(-1 + 0\sqrt{d})(-1 + 0\sqrt{d}) = 1 + 0\sqrt{d}.$$

$(1, 0)$ et $(-1, 0)$ sont les seuls éléments de torsion dans G .

$$(x, y) \in G \Rightarrow \begin{array}{l} (-x, y) \\ (x, -y) \\ (-x, -y) \end{array} \in G$$

$$x^2 - dy^2 = \pm 1$$

$$x \neq 0$$

Si $x \neq 1$ et $x > 0$ alors $x \geq 2$; $\text{supp } y > 0$

$$(x + y\sqrt{d})^n \text{ suite croissante} \\ \neq (1, 0)$$

$$G_{\text{tors}} = \{(1, 0); (-1, 0)\} \simeq \mathbb{Z}/2\mathbb{Z}$$

Si (x_1, y_1) est la solution fondamentale de $x^2 - dy^2 = \pm 1$ (= la plus petite solution en entiers > 0 autre que $(1, 0)$) alors l'ensemble des solutions

* $(x, y) \in \mathbb{Z}_{>0}^2$ est donné par

$$(x_1 + y_1\sqrt{d})^m = x + y\sqrt{d}, \quad m \in \mathbb{Z}_{\geq 0}$$

* $(x, y) \in \mathbb{Z}^2$ est donné par

$$(x_1 + y_1\sqrt{d})^n = x + \sqrt{d}y, \quad n \in \mathbb{Z}.$$

$$\begin{array}{ccc} G & \longrightarrow & \mathbb{R}^2 \ni (t_1, t_2) \\ \downarrow & & \\ (x, y) & \longmapsto & (\log|x + \sqrt{d}y|, \log|x - \sqrt{d}y|) \end{array}$$

homomorphisme de groupes

$$(1, 0) \longmapsto (0, 0)$$

$$(-1, 0) \longmapsto (0, 0)$$

noyau:

G_{tors}

image sous-groupe de \mathbb{R}^2

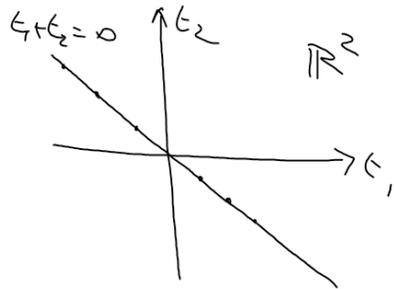
contenu dans la droite $t_1 + t_2 = 0$

groupe additif isomorphe à \mathbb{R} .

But : image G est

$$\mathbb{Z} (\log|x_1+y_1\sqrt{d}|, \log|x_1-y_1\sqrt{d}|)$$

où (x_1, y_1) est la solution fondamentale de l'équation de Pell. $x^2 - dy^2 = \pm 1$.



Si K est un compact de \mathbb{R}^2 , alors $K \cap G$ est fini
 G est discret.

Tout sous-groupe discret de \mathbb{R} est de la forme $\mathbb{Z}u$

$$u \geq 0$$

Dém. : Algorithme d'Euclide.