Equations Diophantiennes.

$f(x_1, -, x_n) = 0$

donné $f \in \mathbb{Z}[X_1, -, X_n]$

inconnues : $(x_1, -, x_n)$ dans $\mathbb{Z}^n$

ou dans $\mathbb{Q}^n$ (points entiers)
(points rationnels)

Hilbert 1900

? algorithme. nombre fini ou infini de solutions $\in \mathbb{Z}^n$.

1970. Matijacewicz.

(J. Robinson, Davis, ...)

Il n'y a pas de tel algorithme.

Hilbert. $\mathbb{Z}^n$.

Question ouverte : $\mathbb{Q}^n$?

$f\left(\frac{a_1}{b_1}, -, \frac{a_n}{b_n}\right) = 0$ $\qquad$ $F(X_1, -, X_n) =$

$b_1^{d_1} \cdots b_n^{d_n}$ $\qquad$ $X_1^{d_1} \cdots X_n^{d_n} f(X_1, -, X_n)$

$f \in \mathbb{Q}[X_1, -, X_n]$.

d degré

$X_0^d f\left(\frac{X_1}{X_0}, -, \frac{X_n}{X_0}\right) = F(X_0, X_1, -, X_n)$

$f(x_1, -, x_n) = 0 \qquad (x_1, -, x_n) \in \mathbb{Q}^n$.

points rationnels

$F(x_0, x_1, -, x_n) = 0 \qquad (x_0, x_1, -, x_n) \in \mathbb{Z}^n$.

points entiers.

$f(x, y) = 0 \qquad f \in \mathbb{Z}[X, Y]$.

① degré 1. Equation linéaire.

$f(X, Y) = aX + bY + c$. $\qquad (a, b, c) \in \mathbb{Z}^3$

$(a, b) \neq (0, 0)$

. solutions rationnelles.

si $a \neq 0$. $\qquad x = -\frac{by + c}{a} \qquad y \in \mathbb{Q}$.

. solutions entières.

$2x + 4y - 5 = 0$ pas de solution.

$d | a$ et $d | b \Rightarrow d | c$.

pgcd $(a, b) | c$

$ax+by=c$ $\quad a,b,c$ donnés $\in \mathbb{Z}$.

$(a,b)\neq(0,0)$.

$d=\text{pgcd}(a,b)$

supp. $d \mid c$.

$\longrightarrow$ nouvelle équation $\quad a'=\frac{a}{d}$, $b'=\frac{b}{d}$, $c'=\frac{c}{d}$

$a'x+b'y=c'$ $\quad \text{pgcd}(a',b')=1$.

si $a'x_0+b'y_0=1$ alors $x=c'x_0$, $y=c'y_0$ est une solution de $a'x+b'y=c'$.

Si on a une solution $(x_1,y_1)\in\mathbb{Z}\times\mathbb{Z}$ à $a'x_1+b'y_1=c'$

$(x_2,y_2)\in\mathbb{Z}\times\mathbb{Z}$ $\quad a'x_2+b'y_2=c'$

alors (x_2-x_1, y_2-y_1) est solution de l'équation homogène

$\star$ $ax+by=0$ $\quad \text{pgcd}(a,b)=1$

$\star$ $ax+by=1$ $\quad \text{pgcd}(a,b)=1$.

Homogène $\quad ax+by=0$. $\quad b\neq 0$.

$-\frac{a}{b}=\frac{y}{x}$.

$y=ka$, $x=-kb$ $\quad k\in\mathbb{Z}$.

Non homogène. Bézout. Etant donné $(a,b)\in\mathbb{Z}\times\mathbb{Z}$ $\quad \text{pgcd}(a,b)=1$, il existe $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ t.q. $ax+by=1$.

Algorithme: Euclide.

$ax+by=1$.

a,b donnés

$\{ax+by\,;\,(x,y)\in\mathbb{Z}\times\mathbb{Z}\}\subset\mathbb{Z}$.

sous groupes de $\mathbb{Z}$?

tous de la forme $k\mathbb{Z}$ $\quad k\in\mathbb{Z}_{\geq 0}$

$\{kn,\ n\in\mathbb{Z}\}$

(division euclidienne).

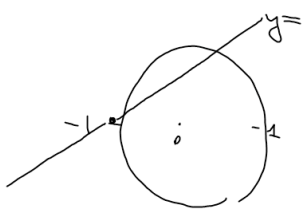
$\{ax+by,(x,y)\in\mathbb{Z}\times\mathbb{Z}\}=d\mathbb{Z}$.

$d=\text{pgcd}(a,b)$

Equations quadratiques. (degré 2).

Exemple 1. $x^2+y^2-1=0$ cercle.

points rationnels ?



$(-1,0)$.

$t\in\mathbb{Q} \Leftrightarrow (x,y)\in\mathbb{Q}\times\mathbb{Q}$.

$x^2-1+t^2(x+1)^2=0$

$(x+1)\left(x-1+t^2(x+1)\right)=0$

$x=\frac{1-t^2}{1+t^2}$. $\quad y=\frac{2t}{t^2+1}$.

Equation homogène associée

$x = \frac{X}{Z}$ $\quad y = \frac{Y}{Z}$ $\qquad x^2+y^2=1$

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

$(X,Y,Z) \in \mathbb{Z}^3$

points entiers.

Eq. de Pythagore.

$x = \frac{1-t^2}{1+t^2}$ $\quad y = \frac{2t}{1+t^2}$.

$t \in \mathbb{Q}$. $\qquad t = \frac{a}{b}$ $\quad (a,b) \in \mathbb{Z}\times\mathbb{Z}$ $\quad \text{pgcd}(a,b)=1$.

$x = \frac{b^2-a^2}{b^2+a^2}$ $\quad y = \frac{2ab}{b^2+a^2}$.

L'application

$(a,b) \longmapsto (X = b^2-a^2,\ Y = 2ab,\ Z = b^2+a^2)$

est une bijection entre

l'ensemble des couples (a,b) d'entiers >0 premiers entre eux

et

l'ensemble des triplets $(X,Y,Z) \in \mathbb{Z}^3$ d'entiers >0 $\text{pgcd}(X,Y,Z)=1$, solutions de

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

2e exemple d'équation quadratique en 2 variables

$x^2-dy^2=\pm 1$. Pell-Fermat.

Brouncker.

d entier $\in \mathbb{Z}$

inconnues $(x,y) \in \mathbb{Z}^2$.

Si $d \leq -2$ alors $y=0$ $\quad x=\pm 1$.

Si $d=-1$ $\quad x^2+y^2=\pm 1$

$x^2+y^2=1$. $\quad (\pm 1, 0)$ et $(0, \pm 1)$

Si $d=0$ $\quad x^2=\pm 1$. $\quad (\pm 1, y)$

$x^2-dy^2=\pm 1$ $\qquad d>0$

Si $d=e^2$ $\qquad e \in \mathbb{Z}$.

$x^2-e^2y^2=\pm 1$.

$(x-ey)(x+ey)=\pm 1$.

$\Rightarrow$ $x-ey$ et $x+ey$ sont ± 1

seules solutions triviales

$x=\pm 1$ $\quad y=0$

$d=+1$

$x^2-y^2=\pm 1$.

$\begin{cases} x=0 \\ y=\pm 1 \end{cases}$

Cas intéressant : d entier ≥ 2
qui n'est pas un carré.

Il y a une infinité de solutions
à l'équation $x^2 - dy^2 = \pm 1$.

$(x, y) \in \mathbb{Z}^2_{>0}$ ordre naturel

ie y en a une avec $x > 1$ minimal.

(x_0, y_0) solution fondamentale.

$(x_0 - \sqrt{d}\, y_0)(x_0 + \sqrt{d}\, y_0) = \pm 1$. n entier ≥ 1.

$(x_0 + \sqrt{d}\, y_0)^n = x_n + \sqrt{d}\, y_n$. $(x_n, y_n) \in \mathbb{Z}^2_{>0}$

$(x_0 - \sqrt{d}\, y_0)^n = x_n - \sqrt{d}\, y_n$. $x_n > x_{n-1}$

$\mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$. automorphisme du corps $\mathbb{Q}$-e-v.
$u + v\sqrt{d} \longmapsto u - v\sqrt{d}$

$\Rightarrow (x_n, y_n)$ est aussi une solution.
$x_n^2 - d y_n^2 = \pm 1$.

A partir de la solution fondamentale
$(x_0, y_0) \in \mathbb{Z}^2_{>0}$ de l'équation
$x^2 - dy^2 = \pm 1$ $(x_0 > 1)$.
on trouve tous les solutions $\in \mathbb{Z}^2_{>0}$
en considérant $(x_0 + y_0\sqrt{d})^n = x_n + \sqrt{d}\, y_n$.
$n \geq 0$
$(x_n, y_n) \in \mathbb{Z}^2_{>0}$
on trouve toutes les solutions dans $\mathbb{Z}^2$
en prenant $(x_0 \pm \sqrt{d}\, y_0)^n$, $n \in \mathbb{Z}$

Si la solution fondamentale (x_0, y_0)
vérifie $x_0^2 - d y_0^2 = -1$ $(\mathbb{Z}_{>0} \times \mathbb{Z}_{>0})$
alors les solutions de $x^2 - dy^2 = +1$
sont les (x_n, y_n) avec n pair $(n \geq 0)$
et les solutions dans $\mathbb{Z}^2_{>0}$ de $x^2 - dy^2 = -1$
sont les (x_n, y_n) avec $n \geq 1$ impair.

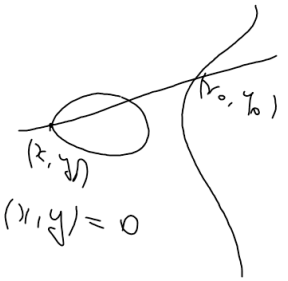
Si la solution fondamentale (x_0, y_0)
de $x_0^2 - d y_0^2 = 1$
alors il n'y a pas de solution à
l'équation $x^2 - d y^2 = -1$

Cubiques (degré 3).

$f(x,y) = 0$ $\quad f \in \mathbb{Z}[X,Y]$ degré 3.

points rationnels $(x,y) \in \mathbb{Q} \times \mathbb{Q}$

Si on a deux solutions rationnelles
(x_0, y_0) et (x_1, y_1)
la droite passant
par ces 2 points coupe
"généralement" la courbe $f(x,y) = 0$
en un troisième point



$f(x,y) = 0$ $\quad (x_0, y_0)$
(x_1, y_1).

$$y - y_0 = \frac{y_1 - y_0}{x_1 - x_0}(x - x_0). \qquad (x_1 \neq x_0)$$

$f \in \mathbb{Z}[X,Y]$ degré 3

$$F(X) = f\left(X,\ y_0 + \frac{y_1 - y_0}{x_1 - x_0}(X - x_0)\right) \in \mathbb{Q}[X]$$

en général $\deg F = 3$
racines $x_0, x_1 \in \mathbb{Q}$.
$\rightarrow$ 3e racine $\in \mathbb{Q}$. $\quad (x_2, y_2)$

Si (x_0, y_0) est un point rationnel sur
la courbe, la tangente à la courbe
en ce point coupe la courbe en un 3e pt
rationnel.

Méthode de la courbe et de la tangente.

Courbes elliptiques.

$f(x,y) = 0$ degré 3

Mordell $\exists$ nombre fini de points
rationnels à partir desquels on les trouve tous.

Conjectures diophantiennes.

Pillai. Catalan 1844.

puissances parfaites

1, 4, 8, 9, 16, 25, 27, 32, 36, ...

consécutifs.

Thm (Mihailescu). $x^n - y^m = 1$ seule solution $3^2 - 2^3 = 1$

x, y entiers ≥ 2

n, m

Conjecture de Pillai.

Soit k entier ≥ 1

L'équation $x^n - y^m = k$

n'a qu'un nombre fini de solutions

(x, y, n, m) en entiers ≥ 2.

$k = 1$ OK.

Exercice Cj $\Leftrightarrow$ la différence entre

2 termes consécutifs de la suite des

puissances parfaites tend vers l'infini