Exemples d'équation diophantienne

Florian Bertuol, Maximilien Dreveton

February 10, 2016

Rapport du jury 2015 : Il s'agit d'une leçon nouvelle, ou plus exactement d'une renaissance. On y attend les notions de bases servant à aborder les équations de type ax+by = d (identité de Bezout, lemme de Gauss), les systèmes de congruences, mais aussi bien entendu la méthode de descente et l'utilisation de la réduction modulo un nombre premier p. La leçon peut aussi dériver vers la notion de factorialité, illustrée par des équations de type Mordell, Pell-Fermat, et même Fermat (pour n = 2, ou pour les nombres premiers de Sophie Germain).

Notes historiques : Nommées en l'honneur de Diophante, mathématicien grec.

Définition 1. *Une équation Diophantienne est une équation polynômiale*

$$p(x_1, \dots, x_n) = 0$$

à coefficients entiers dont on cherche les solutions entières, ie dans $\mathbb{Z}^n$ ou dans $\mathbb{Q}^n$.

Motivations irrationalité de 2; Équation de Fermat

$\frac{26}{65} = \frac{2}{5}$: clairement, on a simplifié par 6. Chercher les fractions où ce genre de simplification grotesque est vérifié revient à résoudre une eq diophantienne. En effet, on veut : $\frac{10x+y}{10y+z} = \frac{x}{z}$ ce qui donne (10 x+y)z = x(10y +z). (rq : on veut en plus x,y,z positifs inférieurs à 10).

Problème de ces équations On peut résoudre les plus simple à la main en étant astucieux, mais (contrairement à des équations sur R ou C) si on change un paramètre et la méthode ne marche plus. On voudrait donc pouvoir classifier les équations en fonction de leur nombre de solutions.

Théorème 0.1. *Théorème de Matiyasevich (1970, admis)*

Il n'y a pas d'algorithme général permettant de déterminer si une équation en nombre entiers $p(x_1, \dots, x_n) = 0$ a ou non une infinité de solutions dans $\mathbb{Z}^n$.

Remarque : cela résout le 10ème problème de Hilbert. Par contre, si l'on restreint la famille d'équation, la réponse peut devenir positive (ex : équations de Thue (dur), formes quadratiques, ou équation du premier degré sont résolvables algorithmiquement).

Preuve 0.2. *Idée de la preuve : en gros introduire les nombres diophantiens. Montrer que c'est récursivement énumérable.*

1 Equation du premier ordre

1.1 Equation ax+b=c

Proposition 1.1. *Soient a,b $\in \mathbb{Z}$, pas tous les deux nuls, et $d = pgcd(a,b)$ leur pgcd. Pour $c \in \mathbb{Z}$, l'équation ax+by = c a une solution si et seulement si d divise c. Si (x_0, y_0) est une solution particulière, les autres solutions sont tous les couples de la forme $(x_0 - kb_0, y_0 + ka_0)$, où k décrit $\mathbb{Z}$, $a = da_0$ et $b = db_0$.*

Proof. Découle de Bézout + linéarité de l'équation □

Algorithme d'Euclide et complexité cf Demazure

Proposition 1.2. *pgcd(u,v)=pgcd(u,qv) où q est le quotient dans la division euclidienne de u par v.*

Algorithme :

Proposition 1.3. *Si l'ago d'Euclide partant de (u,v) (avec $u > v > 0$) s'arrête au bout de n pas, alors on a :*

$$u \geq dF_{n+2} \quad v \geq dF_{n+1}$$

où F_n désigne la suite de Fibonacci (qui part de (0,1)).

Preuve 1.4. *Par récurrence.*

Sachant que $F_n = (\phi - \bar{\phi})/\sqrt{5}$, on a dans le pire des cas :

$$n + 1 \leq \frac{\ln(y\sqrt{5} + 1)}{\ln \phi}$$

Le pire peut être atteint si l'on part de deux nombres de Fibonnacci successifs.
Conclusion : algorithme efficace (ln(y) linéaire en le nombre de chiffres de y).

Interprétation matricielle de l'algorithme d'Euclide Sorte de pivot de Gauss, voir plus loin (paragraphe sur équations linéaires)

1.2 Equations $a_1x_1 + \ldots + a_nx_n = c$

Même topo, avec Bezout on a CNS d'existence des solutions. Par linéarité on casse le problème en solution particulière + solution homogène.

Pour vraiment résoudre, il faut se ramener au pb précédent avec deux inconnues seulement. On pose :

$$x_{n-1} = \alpha u + \beta v \quad x_n = \gamma u + \delta v$$

avec $\alpha\delta - \beta\gamma = 1$. On prend

$$\beta = \frac{a_n}{pgcd(a_n, a_{n-1})} \quad \delta \frac{-\alpha_{n-1}}{pgcd(a_n, a_{n-1})}$$

pour bien avoir pgcd$(\delta, \beta) = 1$

L'équation devient

$$a_1x_1 + \dots a_{n-2}x_{n-2} + (\alpha_{n-1}\alpha + \alpha_k\gamma) = c$$

On a en plus :

$$a_{k-1}\alpha + a_k\gamma = -(pgcd(a_{k-1}, a_k)\alpha\delta) + pgcd(a_{n-1}a_n)\beta\gamma = -pgcd(a_{n-1}, a_n)$$

$$pgcd(a_1, a_2, \dots a_{n-2}, pgcd(a_{n-1}, a_n)) = pgcd(a_1, \dots, a_n)$$

On continue le procédé jusqu'à obtenir une équation de degré 2 qu'on sait résoudre, puis on remonte. C'est dégeulasse à faire à la main (et à écrire en latex), mais possible.

La conclusion est que la solution générale d'une équation à n inconnues s'exprime en fonction de n-1 paramètres.

Proposition 1.5. *Dénombrement des solutions*

Soient $a_1, \dots, a_n \in \mathbb{N}^*$ premiers entre eux dans leur ensemble, S_N le nombre de solutions positives ou nulles de l'équation $\sum_{i=1}^{N} a_i x_i = N$. Alors :

(i) S_N est le coefficient de t^N dans la série entière $\frac{1}{\prod_{i=1}^{n}(1-t^{a_i})}$

(ii) lorsque $N - - > \infty$ on a $S_N \equiv \frac{1}{a_1 \dots a_p} \frac{N^{p-1}}{(p-1)!}$

1.3 Système d'équations diophantiennes linéaire

On pose $A \in M_{m,n}(\mathbb{Z})$ et $B \in \mathbb{Z}^m$ et on étudie AX=B où $X \in mathbbZ^n$.

Idée : on se plonge dans $\mathbb{Q}$: les solutions sont soit l'ensemble vide, soit un sous espace affine de $\mathbb{Q}^n$ de dimension n-rg(A). Mais ça merde pour repasser dans $\mathbb{Z}$ (pas trop compris pourquoi en fait....).

Bêtement, on peut résoudre les équations une par une, ou bien on substitue la première dans la deuxième, etc... Mais ça va être pénible. On propose dans la suite une méthode plus générale.

Solution du système homogène AX=0

Les solutions sont un sous groupe de $\mathbb{Z}^n$, noyau d'un morphisme de Z-module. Via le théorème de la base adaptée, c'est faisable (à parement).

Lemme 1.6. *L'ensemble des $X \in \mathbb{Z}^n$ tels que AX=0 est un sous groupe de $\mathbb{Z}^n$, libre de rang n-rg(A) où le rang de A est calculé dans $M_{m,n}(\mathbb{Q})$.*

Solution particulière

Théorème 1.7. *Soit $M \in M_{n,m}\mathbb{Z}$. Alors il existe deux matrices inversibles $P \in GL_m(\mathbb{Z})$ et $Q \in GL_n(\mathbb{Z})$ et une matrice (quasi)-diagonale $DP \in M_{n,m}(\mathbb{Z})$ telle que :*

(i) M=PDQ

(ii) D=diag$(d_1, \dots d_r, 0, \dots, 0)$ avec $d_1|d_2, \dots, d_i|d_{i+1}, \dots$.

De plus, si $M' = P'D'Q'$ est une autre décomposition avec ces deux propriétés, les scalaires d_j et d'_j sont associés. Donc à un inversible près, les d_i sont uniques.

Définition 2. *Les scalaires $d_1, \ldots, d_r$ sont appelés les facteurs invariants de M.*

Proof. Voir Denis Serre, Matrices p.101

Unicité : faisable

Existence : Par récurrence.

Idée : Le but est de construire M' equivalente à M telle que $m'_{1,1}$ soit divisible par tous les coefficients de M, par exemple égal au pgcd des coeffs de M.

Méthode : Construire une suite de matrices équivalentes $M^{(p)}$ tel que $m_{11}^{(p)}$ divise $m_{11}^{(p-1)}$ et divise un élément de plus de $M^{(p-1)}$. Raisonner pour 4 cas possibles distincts.

Ceci étant fait, on peut réduire M en M' matrice avec que des zéros sur la première ligne et première colonne, sauf en (1,1) (où on a le pgcd des coeff de M). On applique l'HR et c'est plié.

□

On peut voir ça comme une variante de Gauss pour réduire A en matrice diagonale avec des facteurs invariants $Q^{-1}AP = D$ avec D=diag$(d_1 \ldots d_r, 0, \ldots, 0)$.

On peut avoir D via opérations élémentaires sur lignes colonnes, et P et Q gardent la trace de ces opérations (cf pivot de Gauss).

Ensuite il suffit de poser $X' = P^{-1}X$ et $B' = Q^{-1}B$ et on a :

$$AX = B \iff DX' = B'$$

1.4 Equations modulaires

Résolvables via lemme chinois, voir Demazure.

2 Equations de degré supérieures : méthodes de résolution

2.1 Descente infinie

Définition 3. *Descente infinie : principe de la méthode, inventée par Fermat.*

On considère l'ensemble de $\mathbb{N}$ (supposé non vide, donc avec un plus petit élément) formé des éléments solutions de l'équation Diophantienne. On choisit le plus petit, puis on en exhibe un autre strictement plus petit, aboutissant à une contradiction.

Théorème 2.1. *Soit $d \in \mathbb{N}$; on suppose d n'est pas un carré parfait. Alors $\sqrt{d}$ est irrationnel.*

Preuve 2.2. *Supposons $\sqrt{d} = \frac{a}{b}$ avec a, b entiers premiers entre eux. Donc $b^2d = a^2$. Comme d n'est pas carré, il existe un nombre premier p et un entier k tel que $d = p^{2k+1}\delta$, avec $p \not| \delta$. Alors $p^{2k+1}|a^2$ donc $p^{k+1}|a$ et on écrit $a = p^{k+1}\alpha$ Donc $b^2\delta = p\alpha^2$. Donc p divise $b^2\delta$ mais ne divise pas δ. Donc $p|b^2$, et par suite $p|b$. Ainsi, $p|a$ et $p|b$, ce qui est en contradiction avec l'hypothèse a et b premier entre eux.*

Remarque : dans la preuve, on suppose un argument de minimalité (pgcd(a,b)=1) pour avoir une contradiction. Si on veut réellement être dans le cas de la descente infinie, on enlève cette hypothèse, et on voit qu'en partant de a, on construit une suite d'entiers positifs strictement décroissante, ce qui est impossible, et on est bien dans le cas de la descente. La preuve avec la minimalité est plus simple, mais l'autre est juste à savoir au cas où le jury pète les couilles.

Corollaire 2.3. *Si $d \in \mathbb{N}$ n'est pas un carré parfait, les nombres 1 et $\sqrt{d}$ sont linéairement indépendants sur $\mathbb{Q}$; cad si p,q$\in \mathbb{Q}$ et $p + q\sqrt{d} = 0$, alors p=q=0.*

Exemple : triplet pythagoriciens
Prop : L'aire d'un triangle pythagoricien ne peut pas être un carré.
Application : Équation de Fermat pour n=4.
Exemple : $x^3 + 2y^3 = 4z^3$ n'a pas de solutions non triviales.

Proposition 2.4. *Sophie Germain*
Si p nombre premier tel que 2p+1 est premier, alors $\nexists (x, y, z) \in \mathbb{Z}^3$ tels que $xyz \neq 0[p]$ and $x^p + y^p + z^p = 0$

Exemple : $n \in \mathbb{N}, \alpha \in \mathbb{N}, \alpha > n \geq 2 \quad x_1^2 \dots x_n^2 = \alpha x_1 \dots x_n$ n'admet pas de solutions non triviales. (à enlever? en tout cas de mémoire j'ai pas de référence.... Si on enlève le second membre, c'est le problème de Warning il me semble, et c'est chaud.)

2.2 Changement d'anneau et réduction modulaire

Réduction modulaire Principe : On suppose il existe une solution, et on passe dans $\mathbb{Z}/p\mathbb{Z}$ pour trouver une contradiction. Permet en général de montrer l'inexistence de solutions.
Ex : $x^3 + 5 = 117y^3$ n'a pas de solutions entières (réduction modulo 9)
$x^3 + y^3 + z^3 = 4ou5$ n'ont pas de solutions entières (modulo 9)
Si $p \equiv 3[4]$, p premier, alors $x^2+y^2 = pc^2$ n'a pas de solutions non triviales (réduction modulo p + descente infinie). Par contre, si $p \equiv 1ou2[4]$, il y en a une infinité !
$2^n - 1$ n'est jamais le carré d'un nombre pour $n \geq 3$

Changement d'anneau On se ramène au problème de trouver les unités dans un anneau du type $\mathbb{Q}[d]$

Théorème 2.5. *Théorème des deux carrés*

Preuve 2.6. *voir Perrin + Gourdon*

2.3 Méthodes géométriques

Solutions rationnelles On peut chercher à résoudre sur Q pour revenir sur Z. Dans le cas particulier où l'application qui a une solution sur Q associe une solution sur Z est surjective, c'est plié, mais c'est quand même un cas particulier...

Paramétrisation rationnelle

Définition 4. *On considère une équation p(X,Y,Z)=0, om $p \in \mathbb{Z}[X,Y,Z]$ est un polynôme homogène tel que la courbe d'équation p(x,y,1)=0 possède une paramétrage rationnel. On trouve les racines rationnelles de p(x,y,z) à partir de ce paramétrage.*

Exemple : cercle $x^2+y^2=1$ paramétré par $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ permet d'obtenir l'ensemble des triplets pythagoriciens : ce sont les (x,y,z) = $(d(u^2-v^2), 2duv, d(u^2+v^2))$ où $d \in \mathbb{N}$ et pgcd(u,v)=1.

Paramétrisation rationnelle On considère f(x,y)=0 d'une conique, et (x_0, y_0) une solution particulière. Alors on trace la droite de pente $t \in \mathbb{Q}$ passant par (x_0, y_0). Le point d'intersection entre cette droite et la conique est alors une autre solution rationnelle.

Proposition 2.7. *Toutes les solutions rationnelles sont ainsi obtenues.*

En dimension supérieure, le problème virent du fait qu'il n'y a pas forcément un seul point d'intersection.

Exemple : $x^2+y^2=1$: solution particulière (-1,0) et on considère la droite y=t(x+1); le point d'intersection s'obtient en résolvant $x^2+t^2(x+1)^2-1=0$, avec $x \neq -1$, donc $x-1+t^2(x+1)=0$ cad :

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

En écrivant t=a/b, on obtient les solutions de l'équation $x^2+y^2=z^2$ déjà étudié précédemment.

Proposition 2.8. *Points entier appartenant à une hyperbole.*

Preuve 2.9.

Critique/Limitations de cette méthode :

A partir de points rationnels, pas forcément direct de trouver les points entiers, et tâtonnement garanti.

En degré supérieur : un point rationnel ne suffit pas pour construire d'autres points (une droite coupe la courbe en strictement plus d'un point en général). Y'a des livres entiers sur les courbes elliptiques

3 Autres types d'équations diophantiennes