ÉQUATIONS DIOPHANTIENNES

Marc HINDRY (*)

INTRODUCTION

Si on se donne une équation polynomiale à deux variables $P(x,y) = 0$, on peut considérer cette équation comme celle d'une courbe $(\mathcal{C})$ dans le plan affine $\mathbb{A}^2$. La recherche des solutions en nombres rationnels se traduit par la recherche des points à coordonnées rationnelles de $(\mathcal{C})$. C'est un exemple fondamental d'équation diophantienne.

Il est préférable, d'un point de vue géométrique, de se placer dans le plan projectif $\mathbb{P}^2$ (que l'on peut définir comme l'ensemble des droites de $\mathbb{A}^3$ passant par l'origine). Pour cela, si le polynôme P s'écrit $\Sigma_{i,j} a_{i,j} x^i y^j$ et si d est son degré total, on construit le polynôme homogène associé : $\bar{P}(X,Y,Z) = \Sigma_{i,j} a_{i,j} X^i Y^j Z^{d-i-j}$.

L'équation $\bar{P}(X,Y,Z) = 0$ définit alors une courbe dans le plan projectif qui contient d'ailleurs la courbe affine de départ mais à laquelle on a rajouté des "points à l'infini" (les points de $\mathbb{P}^2$ avec $Z = 0$).

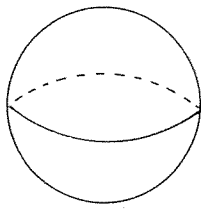
L'étude diophantienne de ces courbes mélange arithmétique et géométrie. En particulier, les travaux sont guidés par l'analogie entre corps de nombres et corps de fonctions. Par exemple on construit $\mathbb{Q}$ à partir de $\mathbb{Z}$ et de même on construit $\mathbb{C}(T)$, l'ensemble des fractions rationnelles à coefficients dans $\mathbb{C}$ à partir de $\mathbb{C}[T]$ l'anneau des polynômes. Cette analogie féconde n'est d'ailleurs pas entièrement comprise bien que largement exploitée.

I.– GENRE D'UNE COURBE ALGÉBRIQUE

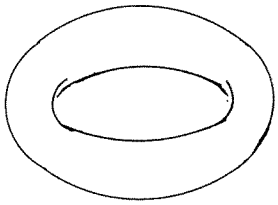
Les points complexes du plan projectif $\mathbb{P}^2(\mathbb{C}) = \{(X,Y,Z) \in \mathbb{C}^3 - \{(0,0,0)\}/ \{(X,Y,Z) = (\lambda X, \lambda Y, \lambda Z)\}$ forment un espace compact et la courbe $\bar{P}(X,Y,Z) = 0$ est également compacte. On est obligé de constater le conflit de deux vocabulaires : pour le géomètre algébriste il s'agit d'une courbe alors que pour le géomètre différentiel c'est une surface de Riemann! Comme telle, c'est une sphère à g trous.

On distingue trois cas selon que $g = 0$, $g = 1$ ou $g \geq 2$.

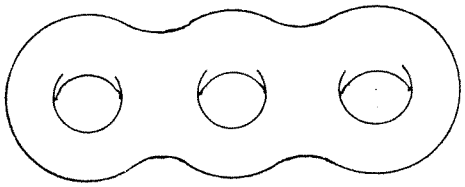
(*) Conférence IREM de Strasbourg - Régionale APMEP d'Alsace donnée le 17 mars 1993



$g = 0$
droite ou conique
dans $\mathbb{P}^2$



$g = 1$
cubique
dans $\mathbb{P}^2$



$g = 3$
quartique
dans $\mathbb{P}^2$

1) $g = 0$. Voici deux exemples :

$$X^2 + Y^2 - Z^2 = 0 \ (C_1)$$
$$X^2 + Y^3 - 3Z^2 = 0 \ (C_2).$$

D'un point de vue diophantien, l'étude de ces courbes est bien comprise; on dispose du théorème suivant :

> **Théorème :** *Si $(\mathcal{C})$ est une courbe de genre 0 alors ou bien $(\mathcal{C})$ ne possède aucun point rationnel ou bien $(\mathcal{C})$ admet une infinité de points rationnels que l'on peut paramétrer explicitement.*

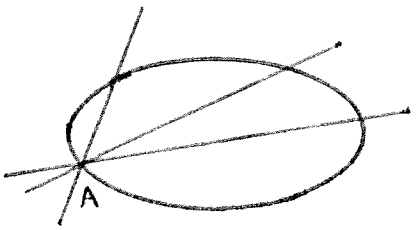
On peut voir aisément par une étude modulo 4 que la courbe $\mathcal{C}_2$ ne possède pas de points rationnels (le point $(0,0,0)$ est interdit!). Quant à la courbe $\mathcal{C}_1$ on peut la traiter de manière arithmétique : on écrit $Y^2 = Z^2 - X^2 = (Z+X)(Z-X)$, on peut supposer que $pgcd(X,Y,Z) = 1$ et on voit facilement que Z est impair et X, Y de parités opposées. Quitte à échanger X et Y on peut supposer X pair et Y impair. Ensuite si $d = pgcd(X+Z, Z-X)$ alors $d = 1$. En effet d divise $X+Z$ et $Z-X$ dont $2X$ et $2Z$ et donc 2. Mais $d = 2$ est impossible car $X+Z$ est impair.

Ainsi $Z+X$ et $Z-X$ doivent être des carrés et on obtient :

$$\begin{cases} Z+X = U^2 \\ Z-X = V^2 \end{cases} \qquad \text{ou encore} \qquad \begin{cases} X = 1/2(U^2 - V^2) \\ Y = UV \\ Z = 1/2(U^2 + V^2) \end{cases}$$

avec U et V entiers impairs premiers entre eux.

De manière plus géométrique, si la conique $\mathcal{C}_1$ possède un point rationnel A, le faisceau de droites passant par A et de pente rationnelle recoupe la courbe en un point rationnel et tous les points rationnels s'obtiennent ainsi :



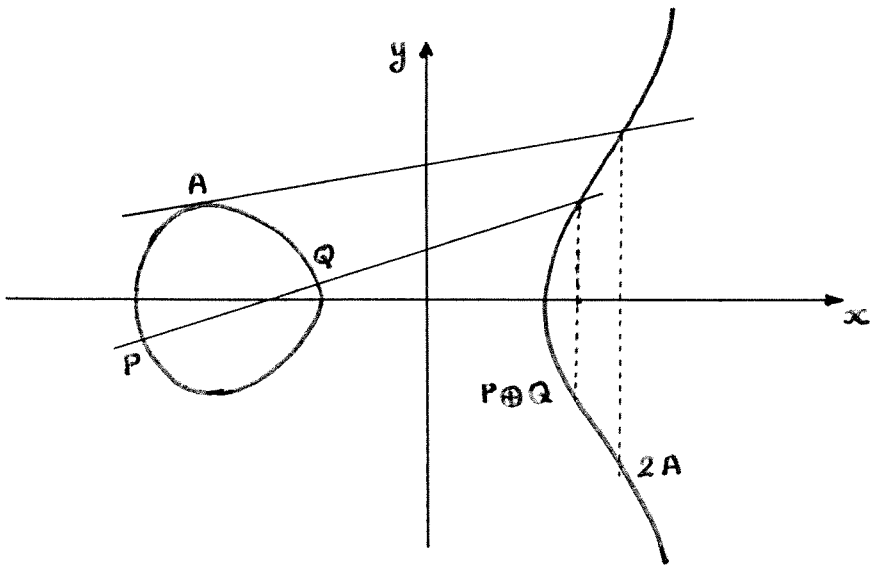
En prenant $A = (1, 0, 1)$ et en coupant par la famille de droites $D_{U,V}$: $U(X - Z) + VY = 0$ on retrouve les mêmes solutions.

2) $g = 1$. Ici encore on distingue deux cas : ou bien la courbe n'a pas de points rationnels ou bien elle en a un (au moins). Dans le deuxième cas il existe une loi de groupe naturelle sur l'ensemble des points rationnels que l'on peut mettre en évidence ainsi :

On démontre que l'on peut transformer la courbe pour obtenir une équation dite de Weierstrass :

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

avec $4a^3 + 27b^2 \neq 0$. L'élément neutre est le point à l'infini $e = (0, 1, 0)$. On construit le point $P \bigoplus Q$ ainsi : on trace la droite passant par P et Q (si $P = Q$ on choisit la tangente en P à la courbe) ; elle coupe la courbe en un troisième point R. Le point $P \bigoplus Q$ est le symétrique de R par rapport à l'axe des X. On peut tracer la courbe affine (où le point e est à l'infini) :



(la loi de groupe sur la courbe $y^2 = x^3 + ax + b$)

Il est facile de voir que les coordonnées de $P \bigoplus Q$ s'expriment rationnellement en fonction des coordonnées de P et de Q.

Théorème (Mordell 1922) *Le groupe des points rationnels est de type fini; c'est-à-dire que toutes les solutions s'obtiennent à partir d'un nombre fini de points par le procédé des cordes et tangentes.*

Malheureusement on ne sait pas, à l'heure actuelle, trouver a priori les générateurs.

3) $g \geq 2$. Dans l'article de 1922, Mordell avait conjecturé le théorème suivant :

Théorème (Faltings 1983). *Soit C une courbe de genre ≥ 2, alors elle possède seulement un ensemble fini (éventuellement vide) de points rationnels.*

Exemple : pour $n \geq 4$ l'équation de Fermat $X^n + Y^n = Z^n$ ne possède qu'un nombre fini de solution. Malheureusement, on ne sait pas déterminer effectivement les solutions dont le théorème garantit la finitude. Une curieuse application est la remarque suivante dûe à Heath-Brown : Soit $\mathcal{F}$ l'ensemble des entiers pour lesquels le "grand" théorème de Fermat est vrai alors si p est un nombre premier, il existe m_0 (dépendant de p) tel que pour $m \geq m_0$ on ait $mp \in \mathcal{F}$. Moyennant quelques calculs on s'aperçoit que :

$$\lim_{X \to \infty} X^{-1} \text{ cardinal } \{n \leq X \text{ tel que } n \in \mathcal{F}\} = 1.$$

C'est-à-dire : "le grand théorème de Fermat est vrai avec probabilité un".

II.– ANALOGIES ENTRE $\mathbb{Z}$ et $\mathbb{C}[T]$.

Tout nombre entier non nul peut s'écrire (dans $\mathbb{Z}$)

$$n = \varepsilon p_1^{m_1} \dots p_r^{m_r}$$

où les p_i sont des nombres premiers, les m_i sont dans $\mathbb{N}^*$ et ε vaut $+1$ ou -1.

De la même façon tout polynôme non nul de $\mathbb{C}[T]$ s'écrit : $P = \varepsilon p_1^{m_1} \dots p_r^{m_r}$ où les p_i sont des polynômes unitaires du premier degré $p_i = T - \alpha_i$, les m_i sont dans $\mathbb{N}^*$ et ε est une constante non nulle.

Sur $\mathbb{Z}$ on dispose de la valeur absolue usuelle que nous notons $|n|_\infty$. On peut aussi définir pour chaque p un ordre de divisibilité

$$\text{ord}_p(n) = \max\{m / p^m \text{ divise } n\}.$$

Sur $\mathbb{C}[T]$ on dispose du degré noté *deg* et pour chaque $\alpha \in \mathbb{C}$ de l'ordre de divisibilité

$$\text{ord}_\alpha(P) = \max\{m | (T-\alpha)^m \text{ divise } P\}.$$

Pour un entier nous avons la formule du produit :

$$\log |n|_\infty - \sum_p \text{ord}_p(n) \log p = 0.$$

Analogue de celle valable pour les polynômes :

$$\deg(P) - \sum_{\alpha} \mathrm{ord}_{\alpha}(P) = 0.$$

Si l'on pose $|n|_p = p^{-\mathrm{ord}_p(n)}$, la formule du produit s'écrit

$$\sum_{v} \log |n|_v = 0$$

où v est soit le symbole ∞ soit un nombre premier. Dans $\mathbb{Z}$, sauf pour $v = \infty$ on a

$$|a + b|_v \leq \max\left(|a|_v, |b|_v\right)$$

ce qui montre que $|.|_p$ est une norme ultramétrique. Par contre dans $\mathbb{C}[T]$, la relation d'ultramétricité est vraie même pour le degré. En fait on peut interpréter le degré comme l'ordre en un certain point en se plaçant sur la droite projective $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$. Alors $\deg(P) = \mathrm{ord}_{\infty}(P)$.

On trouve ainsi certaines limites aux analogies. En fait on peut dire que travailler sur $\mathbb{Z}$ est plus difficile que sur $\mathbb{C}[T]$.

La théorie de schémas de Grothendieck permet de considérer $\mathcal{P} = \{p \text{ premier}\}$ comme les points d'une courbe appelée le spectre de $\mathbb{Z}$, mais les recherches dues notamment à Arakelov permettant de travailler sur l'objet $\mathcal{P} \cup \{\infty\}$ sont encore bien incomplètes!

III.– THÉORÈME DE FERMAT POUR LES POLYNÔMES

Nous choisissons d'illustrer la puissance que donne d'une part l'ultramétrisation et d'autre part l'existence d'une dérivation dans $\mathbb{C}[T]$ en donnant la preuve du théorème suivant, où $r(P)$ désigne le nombre de racines distinctes d'un polynôme P.

> **Théorème** (Mason) *Si $P + Q + R = 0$ où P, Q, R sont des polynômes non constants premiers entre eux de $\mathbb{C}[T]$ alors :*
>
> $$\max(\deg P, \deg Q, \deg R) \leq r(PQR) - 1.$$

Voyons d'abord comment ce théorème entraîne "Fermat pour les polynômes". Supposons que A, B, C soient des polynômes non constants premiers entre eux tels que :

$$A^n + B^n + C^n = 0$$

alors comme $\deg A^n = n \deg A$ et $r(A^n) = r(A)$ on a :

$$n \max(\deg A, \deg B, \deg C) \leq r(ABC) - 1 \leq \deg A + \deg B + \deg C - 1$$

ce qui est clairement impossible dès que $n \geq 3$ puisque par hypothèse $\deg A \geq 1, \deg B \geq 1, \deg C \geq 1$.

Venons-en à la preuve du théorème, écrivons :

$$\begin{array}{lll} P(T) = \alpha_0 \Pi_{i=1}^{p} (T-\alpha_i)^{l_i} & \text{avec donc} & p = r(P) \\ Q(T) = \beta_0 \Pi_{i=1}^{q} (T-\beta_i)^{m_i} & & q = r(Q) \\ R(T) = \gamma_0 \Pi_{i=1}^{s} (T-\gamma_i)^{n_i} & & s = r(R). \end{array}$$

Considérons alors le déterminant $\Delta = \left|\begin{smallmatrix} P & P' \\ Q & Q' \end{smallmatrix}\right|$. Il est clair que $\deg \Delta \leq \deg P + \deg Q - 1$ et il est facile de voir que Δ est non nul. D'autre part $\Pi_{i=1}^{p}(T-\alpha_i)^{l_i-1}$ divise P et P' et donc Δ. De même $\Pi_{i=1}^{q}(T-\beta_i)^{m_i-1}$ divise Q et Q' et donc Δ et de même $\Pi_{i=1}^{q}(T-\beta_i)^{m_i-1}$ divise R et R' et donc Δ.

Pour ce dernier pas, observer que $P = -Q-R$ donc $\Delta = \left|\begin{smallmatrix} -Q-R-Q'-R' \\ Q \qquad\quad Q' \end{smallmatrix}\right| = -\left|\begin{smallmatrix} R & R' \\ Q & Q' \end{smallmatrix}\right|$.

Par suite, comme les trois produits sont premiers entre eux, on obtient que Δ est divisible par

$$\Pi_{i=1}^{p}(T-\alpha)^{l_i-1} \Pi_{i=1}^{q}(T-\beta_i)^{m_i-1} \Pi_{i=1}^{s}(T-\gamma_i)^{n_i-1}$$

d'où une inégalité de degré

$$(\deg P - p) + (\deg Q - q) + (\deg R - s) \leq \deg P + \deg Q - 1$$

d'où $\deg R \leq p + q + s - 1 = r(PQR) - 1$.
En procédant de même avec P et Q on obtient l'énoncé du théorème.

L'analogue immédiat sur $\mathbb{Z}$ serait de penser que si $a+b+c = 0$ avec $\operatorname{pgcd}(a,b,c) = 1$ alors $\max(|a|,|b|,|c|) \leq$ constante $\times r(abc)$ avec

$$r(abc) = \prod_{\substack{p \text{ premier} \\ p \text{ divise } abc.}} p$$

Ceci est faux (voir l'exposé Oesterlé à Bourbaki) mais on peut conjecturer avec Oesterlé et Masser.

Conjecture a - b - c (Oesterlé-Masser).
Il existe deux constantes γ et δ telles que si $a + b + c = 0$ avec $\operatorname{pgcd}(a,b,c) = 1$ alors

$$\max(|a|,|b|,|c|) \leq \gamma r(abc)^{\delta} \ ?$$

Une preuve de cette conjecture serait un grand progrès; par exemple il est facile d'en déduire le théorème de Fermat asymptotique (id est pour n assez grand).

NB : Après cet exposé, Wiles a annoncé le preuve de la conjecture de Tariyama-Weil qui entraîne Fermat. Cela donne de l'espoir de démontrer la conjecture $a-b-c$ (affirmation optimiste bien sûr).

BIBLIOGRAPHIE (succinte)

Des articles originaux :

Mordell L.J.- "*On the rational solutions of the indetermidate equation of the third and the fourth degrees*", Proc. Cambridge Philos. Soc., 21 (1922), pp. 179-182.

Faltings G.- "*Endlichkeitssätze für Abelsche Varietäten über Zahlkörpen*", Inv. Math. 73 (1983), pp. 349-366.

Des "surveys" ou articles de "vulgarisation" :

Oesterlé J.- *Nouvelles approches du théorème de Fermat*, exposé Bourbaki n° 694 (1988).

Hindry M.- *Géométrie arithmétique* Cahier du Séminaire d'Histoire des Mathématiques, vol. 3 (1993) Univ. P. et M. Curie.

Mason.- *Diophantine equations over function fields*, Lecture notes, n° 96, London, Math. Soc. (1984).

Boutot et Moret-Bailly.- *Equations diophantiennes : la conjecture de Mordell*, Courrier du CNRS, Images des mathématiques (1985).

AUTO-RÉFÉRENCE!

Le contraire du vrai peut être vrai comme le montrent les deux phrases suivantes :

Cette phrase comporte exactement dix lettres "e".
Cette phrase ne comporte pas exactement dix lettres "e".

De même le contraire du faux peut être faux comme le montrent les deux phrases suivantes :

Cette phrase comporte exactement treize lettres "e".
Cette phrase ne comporte pas exactement treize lettres "e".

Deux expressions contradictoires peuvent être vraies simultanément :

Cette phrase comporte exactement dix lettres "e".
Cette phrase comporte exactement onze lettres "e".

Ou bien encore fausses simultanément :

Cette phrase comporte exactement douze lettres "e".
Cette phrase comporte exactement treize lettres "e".