Leçon d'agrégation
Équations diophantiennes du premier degré $ax + by = c$. Exemples d'équations de degré supérieur.

Nicolas Lim

1 Définition

On appelle équation diophantienne une équation du type $f(x_1, ..., x_n) = 0$ où $(x_1, ..., x_n) \in \mathbf{Z}^n$. On se contentera ici de traiter le cas où f est un polynôme de $\mathbf{Z}$[X].

Exemples : $x + y$, $x^2 + y^2$...

2 Cas des équation du premier degré

Théorème : L'équation diophantienne $ax + by = c$ admet une solution si et seulement si $d = a \wedge b$ divise c. De plus si (x_0, y_0) est une solution, l'ensemble de solution est $\{(x_0 + t\frac{b}{d}, y_0 - t\frac{a}{d}), t \in \mathbb{Z}\}$.

Théorème : L'équation diophantienne $a_1x_1 + ... + a_nx_n = c$ admet une solution si et seulement si $d = a_1 \wedge ...x_n$ divise c. Il éxiste alors une matrice A telle que l'ensemble des solotuitions soit l'image par A des n-uplet de la forme $(1, t_1, ..., t_{n-1}) \in \mathbb{Z}^n$.

On peut se poser la question de savoir si plusieurs équations diophantiennes on une solution commune dans un domaine fixé de $\mathbf{Z}^n$. C'est ce qu'on fait dans le cas de l'éxercice suivant :

On se donne $2^n - 1$ points (A_i)dans $\mathbf{Z}^n$ montrer que l'on peut trouver un autre point A de $\mathbf{Z}^n$ tel que aucun segment $[A_i, A]$ ne rencontre $\mathbf{Z}^n$ en aucun autre point que ses extrémités.

3 Exemples d'équations de degré supérieur

3.1 L'équation de Fermat

Fermat prétendait avoir montrer qu'il n'éxistait pas de solution non triviale à l'équation diophantienne $x^n + y^n = z^n$ si $n \geq 3$. On peut le démontrer dans le cas où n est de la forme 4^m (pour $m \geq 1$).

Lemme : Toute solution de $x^2 + y^2 = z^2$ est de la forme $(t(a^2 - b^2), 2tab, t(a^2 + b^2))$ ou $(2tab, t(a^2 - b^2), t(a^2 + b^2))$ où a et b n'ont pas la même parité.

Théorème: L'équation diophantienne $x^n + y^n = z^n$ où n est de la forme 4^m n'a pas d'autre solution que $x = z$ et $y = z$.

3.2 Equations quadratiques

3.2.1 Definitions

Soit $q(x,y) = ax^2 + bxy + cy^2$ une forme quadratique à coefficients entiers, on dit que n est représentable par q s'il est dans son image. On dit qu'il est premièrement représentable si $n = q(x,y)$ avec $x \wedge y = 1$.

On appelle discriminant de q l'entier $d = b^2 - 4ac$.

On dit que q et q' sont équivalentes s'il éxiste $f \in \mathrm{SL}(2, \mathbf{Z})$ telle que $q = q'of$.

On dit que $[a,b,c]$ est réduite si :

$$-|a| < b \geq |a| < |c|$$

$$\text{ou si } |a| = |c| : 0 \leq |b| \leq |a| = |c|$$

3.2.2 Théorèmes

Toute classe d'équivalence contient une forme réduite.

Un entier n est premièrement représentable par $[a,b,c]$ ssi il éxiste une forme $[n,b',c']$ équivalente à $[a,b,c]$.

Si n est non nul est premièrement représentable par une forme de discriminant d ssi d est un carré dans $\mathbf{Z}/4|n|\mathbf{Z}$.

3.2.3 Exemple

Un entier est somme de deux carrés ssi tous ses facteurs premiers congrus à 3 modulo 4 ont une valuation paire.

3.3 Somme de 4 carrés

Tout entiers positif est somme de 4 carrés.

Lemme: Construction du corps des quaternions sur $\mathbf{Q}$.

Definition: On appelle entier du corps des quaternions tout élement de la forme $(a,b,c,d) \in \mathbf{Z}^4$ ou de la forme $(a,b,c,d) \in (\frac{1}{2} + \mathbf{Z})^4$. On note cet ensemnble $\mathbb{H}$.

Definition: On appelle norme réduite de (a,b,c,d) le nombre $a^2 + b^2 + c^2 + d^2$.

Lemme: Tout idéal de $\mathbf{H}$ est principal.

On travail dans $\mathbf{H}$ pour prouver le théorème des 4 carrés.

Références

Hunter, Number theory
Samuel, Théorie des nombres