Leçon 126 Exemples d'équations en arithmétique

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de François Combes
2. Algèbre et géométrie de Jean-Etienne Rombaldi
3. Cours d'algèbre de Daniel Perrin
4. Théorie des nombres de Daniel Duverney
5. Oraux X-ENS Algèbre 1
6. Histoires hédonistes de groupes et de géométries de Caldero et Germoni

Développements.

1. Equations des deux carrés par les entiers de Gauss
2. Equation de Mordell pour $k = 2$ et anneau $\mathbb{Z}[i\sqrt{2}]$
3. Théorème de Sophie Germain
4. Loi de réciprocité quadratique

Table des matières

1 Equations diophantiennes linéaires

1.1 Définition et premiers exemples

(Chapitres 12.7 d'Algèbre et géométrie de François Combes et 10.4 d'Algèbre et géoémtrie de Jean-Etienne Rombaldi)

1. Définition : Une équation diophantienne est une équation polynomiale à coefficients eniters et d'inconnues entiers
2. Exemple : $ax + ny = b$ ie $ax \equiv b[n]$
3. Proposition : $ax \equiv 1[n]$ admet des solutions si et seulement si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ie $a \wedge n = 1$, dans ce cas l'algorithme d'Euclide permet de trouver une solution x_0
4. Corollaire : Les solutions de $ax \equiv 1[n]$ sont $x_0 + kn$ avec $k \in \mathbb{Z}$
5. Corollaire : Si $a \wedge n = 1$ et $b \in \mathbb{Z}$ alors les solutions de $ax \equiv b[n]$ sont $bx_0 + kn$ avec $k \in \mathbb{Z}$
6. Théorème : $ax \equiv b[n]$ admet des solutions si et seulement si $pgcd(a, n) \mid b$, dans ce cas les solutions sont $\frac{b}{pgcd(a,n)}x_0 + kn$ avec $k \in \mathbb{Z}$ et x_0 solution particulière de $\frac{a}{pgcd(a,n)}x \equiv 1[n]$

1.2 Système de congruence

(Chapitre 8.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
On considère A un anneau principal.

1. Lemme : Soit $a_1, ..., a_r$ éléments deux à deux premiers entre eux dans A principal et pour tout k dans $[\![1, r]\!]$, $b_k := \prod_{\substack{i=1 \\ i \neq k}}^{r} a_i$ alors les $b_1, ..., b_r$ sont premiers entre eux dans leur ensemble
2. Théorème des restes chinois : Avec les notations du lemme précédent, en notant de plus $a := \prod_{k=1}^{r} a_k$ et les surjections canoniques $\pi : A \longrightarrow A/(a)$ et $\pi_k : A \longrightarrow A/(a_k)$ pour $k \in [\![1, r]\!]$, l'application $\varphi : \begin{array}{ccc} A & \longrightarrow & A/(a_1) \times ... \times A/(a_r) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$ est un morphisme d'anneaux surjectif, en particulier φ induit un isomorphisme d'anneaux
$\overline{\varphi} : \begin{array}{ccc} A/(a) & \longrightarrow & A/(a_1) \times ... \times A/(a_r) \\ \pi(x) & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$ d'inverse
$\overline{\varphi}^{-1} : \begin{array}{ccc} A/(a_1) \times ...A/(a_r) & \longrightarrow & A/(a) \\ (\pi_1(x_1), ..., \pi_r(x_r)) & \longmapsto & \pi\left(\sum_{k=1}^{r} x_k u_k b_k\right) \end{array}$ avec $(u_1, ..., u_r) \in A^r$ tel que $1 = \sum_{k=1}^{r} u_k b_k$
3. Application : On considère le système de congruences $\left\{ \begin{array}{ccc} x & \equiv & a[n] \\ x & \equiv & b[n] \end{array} \right.$ d'inconnue $x \in \mathbb{Z}$ et de paramètres $(a, b, n, m) \in \mathbb{Z}^4$ avec n et m premiers entre eux, alors il existe une solution $x \in \mathbb{Z}$ (unique modulo nm) de ce système

4. Exemple : Le système $\begin{cases} x & \equiv & 2[4] \\ x & \equiv & 3[5] \\ x & \equiv & 1[9] \end{cases}$ a pour ensemble de solutions $\{838+180k, k \in \mathbb{Z}\}$ car on a la relation de Bézout entre 4,5 et 9 : $1 = 1 \times 5 \times 9 + 11 \times 4 \times 9 - 22 \times 4 \times 5$

2 Utilisation d'anneaux d'entiers quadratiques

2.1 Equation des deux carrés et anneau des entiers de Gauss

(Chapitre II.6 du Cours d'algèbre de Daniel Perrin)

1. Définition : L'anneau des entiers de Gauss est l'anneau A_{-1} des entiers de $\mathbb{Q}(i)$, comme $-1 \equiv 3[4]$, il s'agit de $\mathbb{Z}[i]$
2. Lemme : On a $\mathbb{Z}[i]^\times = \{-1, 1, i, -i\}$
3. Théorème : L'équation de Mordell (pour $k = 1$) $y^2 = x^3 - 1$ admet pour une unique solution $(x, y) = (1, 0)$
4. Définition : On définit $\Sigma = \{n \in \mathbb{N}, \exists (x, y) \in \mathbb{N}^2, n = x^2 + y^2\}$
5. Lemme : Soit $n \in \mathbb{N}$, alors $n \equiv 3[4] \Longrightarrow n \notin \Sigma$
6. Lemme : Soit $n \in \mathbb{N}$, alors $n \in \Sigma \Longleftrightarrow \exists z \in \mathbb{Z}[i], n = N(z)$
7. Proposition : L'ensemble Σ est stable par multiplication
8. Lemme : Soit $p \in \mathcal{P}$, alors $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$
9. Théorème : Soit $p \in \mathcal{P}$, alors $p \in \Sigma \Longleftrightarrow p = 2$ *ou* $p \equiv 1[4]$
10. Exemple : $41, 53$ et 61 sont congrus à 1 modulo 4, donc sont sommes de deux carrés, effectivement $41 = 5^2 + 4^2, 53 = 7^2 + 2^2, 61 = 6^2 + 5^2$
11. Théorème : Soit $n \in \mathbb{N}$, alors :
    — Si $n \in \{0, 1\}$ alors $n \in \Sigma$
    — Sinon on décompose n en facteurs irréductibles (car $\mathbb{Z}$ factoriel) $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ et ainsi $n \in \Sigma \Longleftrightarrow \forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}$

2.2 Une équation de Mordell et anneau $\mathbb{Z}[i\sqrt{2}]$

(Exercice 5.17 de Théorie des nombres de Daniel Duverney)

1. Définition : $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2}, a, b \in \mathbb{Z}\}$
2. Exemple : $1 + i\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$
3. Définition : Soit $z = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$, alors $N(z) = z\overline{z} = a^2 + 2b^2$
4. Proposition : $\mathbb{Z}[i\sqrt{2}]^\times = N^{-1}(1)$
5. Théorème : $\mathbb{Z}[i\sqrt{2}]$ est un anneau euclidien, donc principal, donc factoriel
6. Corollaire : L'équation de Mordell (pour $k = 2$) $y^2 = x^3 - 2$ d'inconnues $x, y \in \mathbb{Z}$ a pour uniques solutions $(3, 5)$ et $(3, -5)$

3 Autres équations diophantiennes non linéaires

3.1 Equations de Fermat

(Chapitre 12.7 d'Algèbre et géométrie de François Combes et Exercice 4.39 de Oraux X-ENS Algèbre 1)

1. Proposition : Soit $x, y, z \in \mathbb{N}^3$, alors $x^2 + y^2 = z^2$ si et seulement s'il existe $d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$ premiers entre eux tels que $(x, y, z) = (d(u^2 - v^2), 2duv, d(u^2 + v^2))$ ou $(y, x, z) = (d(u^2 - v^2), 2duv, d(u^2 + v^2))$
2. Proposition : Les équations $x^4 + y^4 = z^2$ et $x^4 + y^4 = z^4$ n'ont pas de solutions non triviales
3. Remarque (admis) : Soit $n \geq 3$, alors l'équation $x^n + y^n = z^n$ n'admet pas de solutions non triviales
4. Théorème de Sophie Germain : Soit $p \in \mathcal{P}$ impair tel que $q = 2p + 1 \in \mathcal{P}$, alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que p ne divise pas xyz et $x^p + y^p + z^p = 0$

3.2 Représentation d'entiers par des formes quadratiques entières

(Chapitre 6.5 de Théorie des nombres de Daniel Duverney)

1. Définition : Un forme quadratique binaire à coefficients entiers est $\varphi(x, y) = ax^2 + bxy + cy^2$ avec $a, b, c \in \mathbb{Z}^3$, de plus $\Delta := b^2 - 4ac$ est le discriminant de φ
2. Remarque : $\Delta \equiv b^2[4]$ donc Δ est un multiple de 4 si b pair et $\Delta \equiv 1$ si b impair
3. Définition : On dit que φ est définie positive sir $\Delta < 0$ et $a > 0$, dans ce cas $c > 0$ et $\varphi(x, y) > 0$ si $(x, y) \neq (0, 0)$
4. Exemple : $\varphi(x, y) = x^2 + y^2$ est définie positive
5. Définition : Soit $n \in \mathbb{Z}$, alors on dit que n est représenté par φ s'il existe $x, y \in \mathbb{Z}$ tels que $n = \varphi(x) = ax^2 + bxy + cy^2$
6. Exemple : Les entiers représentés par $\varphi(x, y) = x^2 + y^2$ ont été vus précédemment
7. Définition : Deux formes quadratiques φ_1, φ_2 sont dites équivalentes s'il existe $f(x, y) = (px + qy, rx + sy) \in \mathbb{Z}^2$ tel que $ps - qr = 1$ et $\varphi_1 = \varphi_2 \circ f$
8. Exemple : $f(x, y) = (y, -x), f(x, y) = (x + y, y), f(x, y) = x - y, y)$ sont de telles applications appelées transformations unimodulaires
9. Exemple : $(a, b, c) \sim (c, -b, a), (a, b, c) \sim (a, b+2a, a+b+c), (a, b, c) \sim (a, b-2a, a-b+c)$
10. Proposition : Deux formes équivalentes représentenant les même entiers
11. Théorème : Si φ définie positive alors $\varphi \sim (a, b, c)$ avec $-a < b \leq a < c$ ou $0 \leq b \leq a = c$, on dit que (a, b, c) est une forme réduite
12. Exemple : $(10, 34, 29) \sim (1, 0, 1)$
13. Théorème : Soit $n \in \mathbb{Z}$, alors n est proprement représenté par φ, ie $n = \varphi(x, y)$ avec x, y premiers entre eux, si et seulement si $\Delta \equiv k^2[4n]$

4 Carrés dans un corps fini

4.1 Symbole de Legendre

(Chapitres 13.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.d du Cours d'algèbre de Daniel Perrin)

On considère p, q des nombres premiers.

1. Théorème : Il existe $\frac{q-1}{2}$ carrés et $\frac{q-1}{2}$ non carrés dans $\mathbb{F}_q^*$
2. Théorème de caractérisation des carrés : Si $p > 2$ premier, soit $x \in \mathbb{F}_q$, alors x est un carré dans $\mathbb{F}_q^*$ si et seulement si $x^{\frac{q-1}{2}} = 1$
3. Corollaire : -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1[4]$
4. Application : Il existe une infinité de nombre premiers $p \equiv 1[4]$
5. Définition : On dit que a non multple de p est un résidu quadratique modulo p si $\overline{a}$ est un carré dans $\mathbb{F}_p^*$ et on note $\left(\frac{a}{p}\right) = 1$ si a est résidu quadratique et $\left(\frac{a}{p}\right) = -1$ sinon, appelé symbole de Legendre
6. Exemple : $4^2 \equiv 1[5]$, donc 4 est un résidu quadratique modulo 5
7. Proposition : Soit $a \in \mathbb{F}_p^*$, alors $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)[p]$ et $a \in \mathbb{F}_p^* \longmapsto \left(\frac{a}{p}\right) \in \{-1, 1\}$ est l'unique morphisme de groupes non trivial
8. Exemple : $2^{\frac{5-1}{2}} = 2^2 = 4 \equiv -1[5]$, donc 2 n'est pas un résidu quadratique modulo 5
9. Corollaire : Si $n = \pm\prod_{i=1}^{r} p_i^{\alpha_i}$ alors $\left(\frac{n}{p}\right) = (\pm 1)^{\frac{p-1}{2}} \prod_{i=1}^{r} \left(\frac{p_i}{p}\right)^{\alpha_i}$
10. Proposition : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

4.2 Loi de réciprocité quadratique

(Chapitres 13.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.d du Cours d'algèbre de Daniel Perrin et V.C de H2G2 de Caldero et Germoni)

1. Lemme : Soit $a \in \mathbb{F}_p^*$, alors $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$
2. Proposition : Soit p et q deux nombres premiers distincts et $X := \left\{(x_1, ..., x_p) \in \mathbb{F}_q^p, \sum_{i=1}^{p} x_i^2 = 1\right\}$, alors $|X| \equiv \left(\frac{p}{q}\right) + 1[p]$
3. Proposition : On a également $|X| = \left(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) q^d$ avec $d = \frac{p-1}{2}$
4. Corollaire : Loi de réciprocité quadratique : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
5. Exemple : $\left(\frac{219}{383}\right) = 1$ donc 219 est un résidu quadratique modulo 383