Leçon 126 : Exemples d'équations diophantiennes.

Développements :

Théorème des deux carrés de Fermat, Equations de Fermat pour $n = 2$ et $n = 4$.

Bibliographie :

Combes, Rombaldi, 1001 problèmes, Berhuy (Algèbre le grand combat), OA, Risler et Boyer, Duverney, Escofier.

Rapport du jury :

Dans cette leçon on doit présenter 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 de Fermat 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).

Remarque 1. *Voir Rombaldi p288.*

Définition 2 (Combes). *Equation diophantienne : $P(x_1, ..x_n) = 0$ où $P \in \mathbb{Z}[X]$.*

1 Equations diophantiennes linéaires

1.1 Résolution à une ou deux variables

Proposition 3. *L'équation $ax = b$ admet une unique solution entière si et seulement si a b. La solution est alors b/a.*

Proposition 4 (Combes p243). *Théorème de Bézout : Soient $a, b \in \mathbb{Z}$ et $d = pgcd(a, b)$. Alors il existe $(u, v) \in \mathbb{Z}$ tel que $au + bv = d$. Réciproquement, si $au_0 + bv_0 = c$, alors $d|c$.*
$pgcd(a, b) = 1$ si et seulement si il existe u, v tels que $au + bv = 1$.

Proposition 5. *Lemme de Gauss.*

Corollaire 6 (Combes p243). *L'équation $ax + by = c$ admet des solutions si et seulement si $pgcd(a, b)|c$. Dans ce cas, pour (u_0, v_0) une solution initiale, $a = a_0 pgcd(a, b)$ et $b = b_0 pcgd(a, b)$, les solutions sont de la forme $(u_0 + b_0k, v_0 - a_0k)$ pour $k \in \mathbb{Z}$.*

Remarque 7. *Ou utiliser directement 1001 p10.*

Remarque 8. *On peut trouver explicitement une solution initiale grâce à l'algorithme d'Euclide.*

Exemple 9 (1001 p101). *$42x + 66y = 10$ n'admet aucune solution. $112x + 70y = 14$ admet des solutions, par exemple $(2, -3)$. Les solutions de $3x + 7y = 11$ sont $\{(6 + 7k, -1 - 3k), k \in \mathbb{Z}\}$. L'équation $303x + 57y = a^2 + 1$ pour $a \in \mathbb{Z}$ n'a pas de solutions entières.*

1.2 Résolution à n variables

Résolution de $a_1x_1 + .. + a_nx_n = b$ où les a_i sont non nuls.

Théorème 10 (Beruy p248). *Posons $d = pgcd(a_1, .., a_n)$. Solutions si et seulement si d b. Elles sont données par ...*

Application 11. *$3x + 4y + 7z = b$.*

ou

Remarque 12. *Soient $A \in M_{m,n}(\mathbb{Z}), B \in \mathbb{Z}^m$. On veut résoudre $AX = B$ avec $X \in \mathbb{Z}^m$*

Proposition 13. *Si $A = Diag(d1, ..., dr, 0..0)$ avec $d_1, .., d_r \in Z^*$, alors $AX = B$ possède des solutions si et seulement si $\forall 1 \leq i \leq r$, $d_i|b_i$ et $\forall r + i \leq i \leq m$, $b_i = 0$. Les solutions sont alors de la forme $(b_1d_1, .., b_rd_r, x_{r+1}, .., x_n)$ pour $x_{r+1}, .., x_n \in \mathbb{Z}$.*

Théorème 14 (OA). *Théorème des facteurs invariants : Pour $A \in M_{m,n}(\mathbb{Z})$, il existe une unique famille finie d'entiers strictement positifs $d_1, .., d_r$ telle que $d_1|..|d_r$ et telle qu'il existe $U \in Sl_m(\mathbb{Z}), V \in Sl_n(Z)$ tel que $UAV = Diag(d1, ..., dr, 0..0)$.*

Proposition 15. *Pour D la matrice des facteurs invariants de A, on a $AX = B$ si et seulement si $D(VX) = U^{-1}B$. On est ramenés à la résolution de $DX_0 = B_0$ pour $X_0 = VX$ et $B_0 = U^{-1}B$.*

Remarque 16. *On peut calculer explicitement les facteurs invariants de la matrice A en utilisant la division euclidienne dans $\mathbb{Z}$.*

Exemple 17. $\begin{matrix} 2 & \\ 3 & \end{matrix}$ $\begin{matrix} 4 \\ 8 \end{matrix} = PDiag(1, 4)Q$.

Exemple 18 (FGN AL2 ex35). *Partition d'un entier en parts fixées. Ou dans le problème de la monnaie.*

1.3 Problème de la monnaie ?

Voir Risler et Boyer

1.4 Systèmes modulaires et théorème chinois

Théorème 19 (Combes p249).

Proposition 20 (Combes p249). *[Cours de calcul formel Saux Picart p69] Méthode de résolution : Méthode de Newton.*

Exemple 21 (Combes p249). *Exemple d'un système.*

Exemple 22. $2p + 3q = n$.

2 Exemples et méthodes

2.1 Réduction modulaire

Remarque 23. *Dans le cas où certains termes de P de petit degré total sont multiples d'un nombre premier p, on peut chercher à résoudre $P(x_1, .., x_n) = 0$ dans F_p. Si P n'a pas de zéros dans F_p, alors il n'a pas de zéros dans $\mathbb{Z}$. Si P a des zéros dans F_p, on cherche alors à voir si ces zéros peuvent être étendus en des zéros dans $\mathbb{Z}$.*

Exemple 24 (1001 ex855). *Pas de solutions à $x^2 + y^2 = 8z + 7$.*

Exemple 25 (1001 ex787). *Pas de solutions à $x^3 + 5 = 117y^3$.*

Exemple 26 (1001 ex847). *Pas de solutions à $x^3 + y^3 + z^3 = 4$ ou 5.*

Exemple 27 (Combes p223). *$x^2 + 1 = p$ avec p premier et p non congru à 1 mod 4 n'a pas de solutions entières. (Réduire mod p.)*

2.2 Descente infinie

Proposition 28. *Principe : On suppose que l'équation admet une solution $(x_1, .., x_n)$ vérifiant certaines propriétés (non-triviale par ex), et l'on dispose d'une fonction w qui à $(x_1, .., x_n)$ associe un entier strictement positif. Si l'on est capable de montrer que l'existence de cette solution implique l'existence d'une autre solution $(y_1, .., y_n)$ vérifiant les mêmes propriétés, et pour laquelle l'image par w est un entier strictement positif inférieur à $w(x_1, .., x_n)$, alors cela veut dire que l'équation n'admet aucune solution vérifiant lesdites propriétés, car une sous-partie majorée de $\mathbb{N}^*$ ne contient pas un nombre infini d'éléments distincts.*

Remarque 29. *Principe pour montrer qu'une équation n'a que des solutions triviales :*

1. *Raisonner par l'absurde et supposer qu'il existe une solution non triviale $(x_1, .., x_n)$ avec des conditions de minimalité.*
2. *Construire une autre solution non triviale plus petite que la solution minimale précédente.*
3. *On aboutit à une contradiction.*

Exemple 30 (Combes p275). *Pas de solutions non triviales à $x^4 + y^x = z^2$.*

Exemple 31 (Duv p52). *$x^4 + y^4 = z^4$ n'a pas d'autres solutions que la solution nulle. (Equation de Fermatpour $n = 4$.)*

Exemple 32 (1001 ex854). *$x^2 + 2y^3 = 4z^4$ n'a pas d'autres solutions entières que la solution nulle.*

Exemple 33 (1001 ex89).

2.3 Utilisation des corps quadratiques

Définition 34 (Duv p47). *Corps des nombres quadratiques. $Q(\sqrt{d})$ avec d sans facteurs carrés.*

Exemple 35. $Q(\sqrt{2})$, $Q(i)$.

Définition 36 (Duv p48). *Norme, conjugué.*

Définition 37 (Duv p48). *Entier quadratique.*

Définition 38 (Duv p48). *Anneau des entiers quadratiques.*

Exemple 39 (Duv p48). *Le nombre d'or.*

Exemple 40. *Entiers de $Q(i)$ est $\mathbb{Z}[i]$, de $Q(j)$ est $\mathbb{Z}[j]$.*

Entiers de Gauss

Proposition 41 (Duv p48). *L'anneau des entiers de Gauss ($d = -1$) est euclidien, description de ses inversibles.*

Application 42 (Duv p56). *Equation de Mordell : $y^2 = x^3 - 1$.*

Entiers $Z[j]$

Proposition 43 (Duv p48). *L'anneau $Z[j]$ ($d = 3$) est euclidien, description de ses inversibles.*

Application 44 (Duv p56). *Equation de Fermat pour $n = 3$.*

3 Carrés et sommes de carrés

3.1 Symbole de Legendre

Définition 45 (Romb p429). *[Gozard p155][Duv p64] Symbole de Legendre.*

Proposition 46 (Duv p65). *Le symbole de Legendre est une fonction multiplicative.*

Proposition 47 (Romb)**.** *Caractérisation des carrés.*
-1 *est un carré si et seulement si* $p = 1[4]$.

Application 48. $x^2 + 1 = p$ *admet des solutions si et seulement si* $p = 1[4]$.

Application 49. *Classification des formes quadratiques.*

Proposition 50. $(\frac{x}{p}) = x^{\frac{p-1}{2}}$.

Exemple 51 (Gozard p155)**.** $(\frac{-1}{p}), (\frac{2}{p})$

Théorème 52. *Loi de réciprocité quadratique.*

Exemple 53 (Gozard p156)**.** $(\frac{23}{59} = -1$.

Application 54. *L'équation* $x^2 + py = q$ *pour* p *premier impair et* q *non multiple a une solution si et seulement si* $(\frac{p}{q}) = 1$.

Corollaire 55. *L'équation* $x^2 + 59y = 23$ *n'a pas de solutions.*
L'équation $x^2 + 5y = -1$ *admet au moins une solution.*

Remarque 56. *La loi de réciprocité quadratique, les symboles pour* -1 *et* 2 *et la division euclidienne, permettent de calculer les symboles de Legendre.*

Application 57 (Combes p275)**.** *[Duv p204] Les équations de la forme* $ax^2 + bx + c = 0$ *pour a,b,c non divisibles par* p *ont des solutions dans* F_p *ssi* $(\frac{b^2-4ac}{p}) = 1$. *Si* $(\frac{b^2-4ac}{p}) = -1$ *pour un certain p premier, alors* $ax^2+bx+c = 0$ *n'a pas de solutions dans* $\mathbb{Z}$.

3.2 Somme de deux carrés

Remarque 58. *Perrin*

Proposition 59. *L'équation diophantienne* $x^2 + y^2 = n$ *admet des solutions si et seulement si pour tout* p *premier tel que* $p = 3mod(4)$, *on a* $vp(n)$ *pair.*

Exemple 60 (Perrin)**.** $260 = 8^2 + 14^2$.

Exemple 61 (Duv p62)**.** $585 = 24^2 + 3^2$.

3.3 Somme de quatre carrés

Lemme 62 (Duv p73)**.** *Soit* p *premier impair. Il existe une solution à* $1 + x^2 + y^2 = 0modp$.

Théorème 63 (Duv p73)**.** *Tout entier s'écrit comme somme de* 4 *carrés.*

Remarque 64 (Duv p73)**.** *Meilleur possible car* 7 *n'est pas somme de* 3 *carrés.*

Exemple 65. $15 = 3^2 + 2^2 + 1^2 + 1^2$.

4 Représentation par des formes quadratiques

Voir éventuellement Escofier p650.