Concours Agrégation, Mathématiques générales

Leçon 26- Exemples d'équations diophantiennes.

Commentaires du jury 2015 : Il s'agit d'une leçon nouvelle ou plus exactement d'une renaissance. On attend là les notions de bases servant à aborder les équations de type $ax + by = d$ (identité de Bezout, lemme de Gauss), les systèmes de congruences, avec le lemme des noyaux. A ce sujet, il est important que le candidat connaisse l'image du morphisme du lemme des noyaux lorsque les nombres ne sont pas premiers entre eux. On attend 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).
Commentaires du jury 2016 : 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).

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2'] Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)
et
[Sa.] Samuel P. *Théorie algébrique des nombres* (Hermann 1997)

Une proposition de plan.

Définition. Une équation diophantienne est la donnée de un ou plusieurs polynômes à $n \geq 1$ indéterminées à coefficients dans $\mathbb{Z}$. L'objectif est d'en trouver les zéros communs dans $\mathbb{Q}^n$ ou $\mathbb{Z}^n$, [Fr. F] p. 63.

(1) Le cas des polynômes de degré 1.
   (a) $a_1x_1 + a_2x_2 + ... + a_nx_n = b$ a une solution dans $\mathbb{Z}^n$ ssi $\text{pgcd}(a_1, a_2, ..., a_n)|b$, [Fr. F] ex. 1.9.41 p. 62.
   (b) Le système $A\ {}^t(x_1, x_2, ..., x_p) = {}^t(b_1, b_2, ..., b_n)$ avec $A \in M_{n,p}(\mathbb{Z})$ et $b_i \in \mathbb{Z}$, [Fr. F] ex. 1.9.42 p.63.

(2) Le cas des polynômes de degré 2.
   (a) Si une conique admet un point rationnel alors on peut paramétrer toutes les solutions dans $\mathbb{Q}^2$, [Fr. MMG] p. 328.
   (b) Le cas où il n'y a pas de point rationnel. Par exemple pour l'équation $(x, y) \in \mathbb{Q}^2,\ x^2+y^2+ap = 0$ avec $a \in \mathbb{Z} - p\mathbb{Z}$ et p un nombre premier $p = 3 \mod 4$ on teste l'existence d'une solution en regardant $\mod p$ une solution éventuelle $(x, y, z) \in \mathbb{Z}^3$ avec $z \neq 0$, $\text{pgcd}(xz) = \text{pgcd}(y, z) = 1$ de l'équation $x^2+y^2+apz^2 = 0$. On déduit que $p|x,\ p|y$ et donc que $p|z$; ce qui est une contradiction.
   (c) L'équation de Fermat d'exposant 2, $x^2 + y^2 = z^2$.
      (i) Les solutions dans $\mathbb{Q}$ avec la paramétrisation rationnelle du cercle par la tangente t de l'arc moitié ; $X^2 + Y^2 = 1$, $X = \frac{1-t^2}{1+t^2}$, $Y = t(X - 1) = \frac{2t}{1+t^2}$. Ainsi les solutions dans $\mathbb{Q}$ sont $(z\frac{1-t^2}{1+t^2}, z\frac{2t}{1+t^2}, z)$ avec $z \in \mathbb{Q}$ et $t \in \mathbb{Q} \cup \infty$ (ce n'est pas une paramétrisation injective).
      (ii) Les solutions $(x, y, z) \in \mathbb{Z}^3$ et $xy \neq 0$, se déduisent par symétrie des solutions $(x, y, z) \in (\mathbb{N}^\star)^3$. Si $\delta = \text{pgcd}(x, y)$ alors $\delta|z$ ainsi on peut supposer que $\text{pgcd}(x, y) = 1$. Facilement x ou y est alors pair et par symétrie on peut supposer que y est pair alors une paramétrisation injective

de ces solutions est donnée par $(x,y,z) = (a^2-b^2, 2ab, a^2+b^2)$ avec $(a,b) \in \mathbb{N}^2$, $b > a > 0$, $\text{pgcd}(a,b) = 1$ et $a + b = 1 \mod 2$.

Preuve. On a $(x,y,z) = (z\frac{1-t^2}{1+t^2}, z\frac{2t}{1+t^2}, z)$ *avec* $t = \frac{b}{a}$, $a,b \in \mathbb{N}^\star$ *et* $\text{pgcd}(a,b) = 1$. *On note alors que* $\text{pgcd}(a^2+b^2, a^2-b^2) = 1$ *ou* 2.

Si $\text{pgcd}(a^2+b^2, a^2-b^2) = 2$ *i.e.* $a = 1 \mod 2$, $b = 1 \mod 2$ *et donc* $z = \frac{a^2+b^2}{2}$ *et* $(x,y,z) = (\frac{a^2-b^2}{2}, ab, \frac{a^2+b^2}{2}$ *et donc* $y = ab = 1 \mod 2$ *ce qui est une contradiction.*

Ainsi $\text{pgcd}(a^2+b^2, a^2-b^2) = 1$ *i.e.* $\text{pgcd}(a,b) = 1$ *et* $a + b = 1 \mod 2$, *alors* $z = a^2+b^2$ *et* $(x,y,z) = (a^2-b^2, 2ab, a^2+b^2)$. *Réciproquement on vérifie que ces triplets sont solutions. ///*

Pour une preuve directe qui utilise seulement les congruences, [F. M. 2] p. 211 ou [Sa.] p. 20.

Une approche différente due à N. Elkies est proposée en exercice.

(d) Le théorème de Legendre, l'équation $ax^2 + by^2 = cz^2$, [F. M. 1] $n°100$ p. 273.

(3) La technique de descente infinie.

(a) L'équation de Fermat d'exposant 4, $x^4 + y^4 = z^4$, [F. M.2] p. 212.

(b) Un théorème d'Euler. Les solutions dans $\mathbb{Q}^2$ de l'équation $y^2 = x^3 + 1$ sont $\{(-1,0), (0,1), (0,-1), (2,3), (2,-3)\}$, [F. M. 2] p. 214.

(4) Les cubiques planes.

(a) La cubique plane avec un point double.
Les solutions dans $\mathbb{Z}^2$ de l'équation $y^2 = x^2(x-1)$ sont $(0,0) \cup \{1+a^2, a(1+a^2)\}$ avec $a \in \mathbb{Z}$ (on cherche les solutions avec $y = ax, a \in \mathbb{Q}$).

(b) La cubique plane avec un point de rebroussement.
Les solutions dans $\mathbb{Z}^2$ de l'équation $y^2 = x^3$ sont $\{(a^2, a^3)\}$ avec $a \in \mathbb{Z}$ (on cherche les solutions avec $y = ax, a \in \mathbb{Q}$).

(5) Les méthodes de la théorie des nombres ; i.e. l'utilisation des anneaux d'entiers.

(a) L'équation $y^2 = x^3 - 2$, [F. M. 1] $n°98$ p.269. On utilise l'anneau $Z[i\sqrt{2}]$.

(b) Les solutions de $n = x^2 + y^2$, [F. M. 1] $n°94$ p.260. On utilise l'anneau $Z[i]$.

(c) L'anneau $Z[\sqrt{2}]$ et l'équation $n = x^2 - 2y^2$, [F. M. 2] p. 203.

(d) L'équation de Pell-Fermat $x^2 - dy^2 = \pm 1$ et les inversibles de l'anneau $Z[\sqrt{d}]$ avec $d \in \mathbb{N}^\star$, [F. M. 1] $n°98$ p.269.

(6) Une remarque sur le test par congruence.
Une équation peut avoir des solutions modulo $m\mathbb{Z}$ pour tout $m > 0$ et ne pas avoir de solution en entiers, , [F. M. 1] $n°101$ p.276.

Développements conseillés :

(1) L'anneau $Z[i\sqrt{2}]$ et l'équation de Mordell, [F. M. 1] $n°98$ p. 269.

(2) Equation de Fermat sur $\mathbb{Z}$, application aux équations $x^4+y^4 = z^2$, $x^4+y^4 = z^4$ et la descente infinie, [F. M. 2] p. 211.

(3) Un théorème d'Euler. Les solutions dans $\mathbb{Q}^2$ de l'équation $y^2 = x^3 + 1$ sont $\{(-1,0), (0,1), (0,-1), (2,3), (2,-3)\}$, [F. M. 2] p. 214.

(4) L'équation de Pell-Fermat $x^2 - dy^2 = \pm 1$ et les inversibles de l'anneau $Z[\sqrt{d}]$ avec $d \in \mathbb{N}^\star$, [F. M. 1] $n°98$ p.269.

Exercice 1 Le test de congruence. La seule solution de l'équation diophantienne $(x,y,z) \in \mathbb{Z}^3$, $x^2 + y^2 = 7z^2$ est $x = y = z = 0$.

Preuve. On suppose que $xyz \neq 0$. *On note* δ *le PGCD de* x, y, z *et on pose* $(x', y', z') := (\frac{x}{\delta}, \frac{y}{\delta}, \frac{y}{\delta})$ *il suit que* $x'^2 + y'^2 = 0$ *mod* 7. *Puisque* $(-1)^{\frac{7-1}{2}} = -1$ *il suit que* -1 *n'est pas un carré modulo* 7 *et ainsi* 7 *divise* x' *et* y' *et donc* 7^2 *divise* $7z^2$ *d'où* 7 *divise* z' *ce qui est une contradiction. Si* $z = 0$ *il suit de la positivité de* $x^2 + y^2$ *que* $x = y = 0$. *Et si* $z \neq 0$ *et* $xy = 0$ *on peut supposer par symétrie que* $y = 0$ *et ainsi* $x^2 = 7z^2$, *ainsi* $2v_7(x) = 1 + 2v_7(z)$, *ce qui est une contradiction. ///*

Voir [Sa.] exercices p. 115 pour une généralisation.

Complément. On peut souhaiter résoudre l'équation diophantienne $(x, y, z) \in \mathbb{Z}^3,\ x^2 + y^2 = pz^2$ *avec* p *premier.*

Si $p = 3$ *mod* 4 *comme dans le cas de* $p = 7$ *on trouve seulement la solution triviale* $(0, 0, 0)$. *Par contre si si* $p = 2$ *ou* $p = 1$ *mod* 4 *il y a une infinité de solutions. Traitons le cas* $p = 5$, *le cas général se traite de façon similaire. Soit donc* $(x, y, z) \in \mathbb{Z}^3,\ x^2 + y^2 = 5z^2$. *On remarque que* $(1, 2, 1)$ *est une solution non triviale. On peut écrire* $|x + iy|^2 = |1 + 2i|^2 z^2$ *ainsi* $|(x + 2y) + i(y - 2x)|^2 = (5z)^2$ *ce qui en posant* $5X = x + 2y$ *et* $5Y = -2x + y$ *et* $Z = z$, *donne* $X^2 + Y^2 = Z^2$. *De plus* $x^2 + y^2 = (x + 2y)(x - 2y)$ *mod* 5, *ainsi quitte à changer* y *en* $-y$ *on peut supposer que* $5|(x + 2y)$ *et donc* $5|(-2x + y) = -2(x + 2y)$ *mod* 5 *et alors* $(X, Y, Z) \in \mathbb{Z}^3$ *et donc à permutation près de* X, Y *([Sa.] p. 20)* $X = \epsilon_1 d(u^2 - v^2)$, $Y = \epsilon_2 2duv$ *et* $Z = \epsilon_3 d(u^2 + v^2)$ *avec* $u, v \in \mathbb{Z}$, $(u, v) = 1$ *et* $\epsilon_i \in \{1, -1\}$. *Puisque* $x = X - 2Y$ *et* $y = 2X + Y$, *on en déduit que* $x = \epsilon_1 d(u^2 - v^2) - 2\epsilon_2(2duv)$, $y = 2\epsilon_1 d(u^2 - v^2) + \epsilon_2 2duv$, $z = \epsilon_3 d(u^2 + v^2)$ *ou* (y, x, z). *Réciproquement on vérifie que ces formules donnent des solutions.*

Une autre solution est de remarquer que $X^2 + Y^2 - 5$ *définit une conique sur* Q *et que* $(1, 2)$ *est une solution. Si* $(X, Y) \in Q^2$ *est solution soit* $X = 1$, *auquel cas* $Y = 2$ *ou* $Y = -2$ *soit* $X - 1 \neq 0$ *auquel cas on pose* $T := \frac{Y-2}{X-1}$ *et alors* $Y = 2 + T(X - 1)$ *d'où* $X^2 + Y^2 - 5 = (X - 1)[(T^2 + 1)X - (1 + 4T - T^2)]$ *et donc* $X = \frac{T^2-4T+1}{T^2+1}$ *et* $Y = \frac{-2T^2-2T+2}{T^2+1}$. *Ainsi les solutions de* $X^2 + Y^2 = 5$ *avec* $(X, Y) \in Q$ *sont* $(1, 2)$, $(1, -2)$ *et* $(X = \frac{T^2-4T+1}{T^2+1}, Y = \frac{-2T^2-2T+2}{T^2+1})$ *avec* $T \in Q$.

Les solutions de $(x, y, z) \in \mathbb{Z}^3,\ x^2 + y^2 = 5z^2$. *sont pour* $z = 0$ *le triplet* $(0, 0, 0)$ *et pour* $z \neq 0$ *vérifient les conditions au-dessus en posant* $X := \frac{x}{z}$ *et* $Y = \frac{y}{z}$. *Posant* $T = \frac{u}{v}$ *avec* $u, v \in \mathbb{Z}$, $(u, v) = 1$ *et* $v \neq 0$ *on retrouve les solutions entières précédentes. ///*

Exercice 2 Test de congruence. Résoudre l'équation diophantienne $x^2 - 14y^2 - 17z^2 = 0$ (calculer le symbole de Legendre $(\frac{14}{17})$)

Exercice 3 Equations diophantiennes et Hilbert 90 dans les extensions quadratiques d'après N. Elkies.

Lemme. Hilbert 90 dans les extensions quadratiques. Soit $\delta \in \mathbb{Z}$ non carré, $K := \mathbb{Q}(\sqrt{\delta}) \subset \mathbb{C}$. Si $w := a + \sqrt{\delta}b \in K$ on note $\sigma(w) = a - \sqrt{\delta}b$ et $U(K) := \{w \in K \mid w\sigma(w) = 1\}$. Alors $U(K) = \{\frac{x}{\sigma x},\ x \in K^\times\}$.

Preuve. On remarque que K est stable par σ. Alors $-1 = \frac{x}{\sigma x}$ pour $x := \sqrt{\delta}$. Soit maintenant $-1 \neq w \in U(K)$ et $x := w + 1 \neq 0$, alors $w = \frac{x}{\sigma x}$ d'où l'égalité $U(K) = \{\frac{x}{\sigma x},\ x \in K^\times\}$.

Corollaire 1. Le triplet $(x, y, z) \in \mathbb{Z}^3$ est solution de l'équation diophantienne $x^2 + y^2 = z^2$ ssi il existe $(m, n) \in \mathbb{Z}^2$ et $c \in \mathbb{Q}$ avec $(x, y, z) = c(m^2 - n^2, 2mn, m^2 + n^2)$.

Preuve. Supposons que $(x, y, z) \in \mathbb{Z}^3$ satisfait l'équation diophantienne $x^2 + y^2 = z^2$. Si $z = 0$ alors $(m, n) = (0, 0)$. Supposons donc que $z \neq 0$ et soit $w := \frac{x+iy}{z}$, alors $w \in U(\mathbb{Q}(i))$ et ainsi (c'est le lemme et dans ce cas σ est la conjugaison complexe) il existe $a \in \mathbb{Q}(i) - \{0\}$ avec $w = \frac{a}{\bar{a}}$ et quitte à changer a en ra avec $r \in \mathbb{Z}$ on peut supposer que $a = m + in \in \mathbb{Z}[i] - \{0\}$. Alors $w = \frac{(m^2-n^2)+i(2mn)}{m^2+n^2}$, ce qui montre bien que (x, y, z) est proportionnel à $(m^2 - n^2, 2mn, m^2 + n^2)$. Réciproquement on vérifie que la condition est suffisante.

Remarque. Si $xyz \neq 0$, quitte à diviser (x, y, z) par leur pgcd, on peut supposer que $PGCD(x, y, z) = 1$. On peut dans le corollaire supposer que $PGCD(m, n) = 1$. Si $m \in 1 + 2\mathbb{Z},\ n \in 2\mathbb{Z}$ alors $PGCD(m^2 - n^2, 2mn, m^2 + n^2) = 1$ et alors $c \in \{-1, 1\}$ (on écrit $c = \frac{u}{v}$ avec $PGCD(u, v) = 1$ et alors $v\mathbb{Z} =$

$PGCD(vx, vy, vz)\mathbb{Z} = PGCDu(m^2 - n^2, 2mn, m^2 + n^2)\mathbb{Z} = u\mathbb{Z})$. Si $m \in 1 + 2\mathbb{Z},\ n \in 1 + 2\mathbb{Z}$ alors $PGCD(m^2 - n^2, 2mn, m^2 + n^2) = 2$ et $c \in \{-1/2, 1/2\}$.

Corollaire 2. Soient $A, B \in \mathbb{Z}$ avec $A^2 - 4B = \delta$ non carré dans $\mathbb{Z}$. Soit $K := \mathbb{Q}(\sqrt{\delta}) \subset \mathbb{C}$ et $\theta \in K$ une racine de $P = X^2 + AX + B$. Le triplet $(x, y, z) \in \mathbb{Z}^3$ est solution de l'équation diophantienne $x^2 + Axy + By^2 = z^2$ ssi il existe $(m, n) \in \mathbb{Z}^2$ et $c \in \mathbb{Q}$ avec $(x, y, z) = c(m^2 - Bn^2, 2mn + An^2, m^2 + Amn + Bn^2)$

Preuve. Même chose que précédement avec $\sigma(a + \theta b) = a + (A - \theta)b$. Soit $w := \frac{x+\theta y}{z} \in K$, alors $w \in U(K)$ ssi $x^2 + Axy + By^2 = z^2$ et $z \neq 0$ et on applique le lemme à K.

Remarque. Plus généralement considérons l'équation diophantienne $x^2 + Axy + By^2 = Cz^2$ avec $A^2 - 4B = \delta$ non carré dans $\mathbb{Z}$ et $C \in \mathbb{Z} - \{0\}$. Il n'y a pas toujours une solution $(x, y, z) \in \mathbb{Z}^3 - \{(0, 0, 0)\}$. Cependant si $(x_0, y_0, z_0) \in \mathbb{Z}^3 - \{(0, 0, 0)\}$ est une solution alors $w_0 := \frac{x_0+\theta y_0}{z_0} \in K$ et $w_0\sigma(w_0) = C$. Il suit que $(x, y, z) \in \mathbb{Z}^3 - \{(0, 0, 0)\}$ est une solution ssi $\frac{w}{w_0} \in U(K)$ où $w := \frac{x+\theta y}{z}$. On applique le lemme à K.

Exercice 4 A propos du commentaire du jury : "A ce sujet, il est important que le candidat connaisse l'image du morphisme du lemme des noyaux lorsque les nombres ne sont pas premiers entre eux " il est probable qu'ils font allusion au théorème des restes chinois. Il s'agit donc de décrire l'image de l'homomorphisme diagonal $f : \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ défini par $f(x) = (x \mod a, x \mod b)$. Notez que Ker $f = \frac{ab}{\delta}\mathbb{Z}$ et ainsi $\Im f$ est un sous-groupe d'indice δ de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. D'où l'énoncer suivant :

Soient $a, b \in N^*$ et $\delta := (a, b)$ leur pgcd. Soient $(z_1, z_2) \in \mathbb{Z}^2$, montrer qu'il existe $x \in \mathbb{Z}$ avec $x = z_1$ modulo a et $x = z_2$ modulo b si et seulement si $z_1 = z_2$ modulo δ. Enfin si cette condition est satisfaite trouver toutes les solutions.

Preuve. La condition est manifestement nécessaire, voyons qu'elle est suffisante. Considérons une relation de Bézout $\delta = ua + vb$ alors si $x := z_1 v\frac{b}{\delta} + z_2 u\frac{a}{\delta}$ on peut écrire $x = (z_1 - z_2)v\frac{b}{\delta} + z_2(u\frac{a}{\delta} + v\frac{b}{\delta}) = \frac{z_1-z_2}{\delta}vb + z_2$ d'une part et $x = z_1(u\frac{a}{\delta} + v\frac{b}{\delta}) + \frac{z_2-z_1}{\delta}ua$ d'autre part. Ainsi $x = z_1$ modulo a et $x = z_2$ modulo b. Puisque Ker $f = \frac{ab}{\delta}\mathbb{Z}$, l'ensemble des solutions est $z_1 v\frac{b}{\delta} + z_2 u\frac{a}{\delta} + \frac{ab}{\delta}\mathbb{Z}$.

Remarque.

Cet exemple trouve sa place dans cette leçon en application de la résolution des systèmes diophantiens linéaires en effet on cherche les entiers x tels qu'il existe $y, z \in \mathbb{Z}$ avec $x = z_1 + ay$ et $x = z_2 + bz$. Ce système se ramène au système $x - ay - 0z = z_1$ et $0x - ay + bz = z_1 - z_2$ (la condition $z_1 = z_2$ modulo δ apparaît alors clairement). On résout la seconde équation et on a alors $x = ay + z_1$.

Exercice 5

Un système linéaire diophantien équivalent à la généralisation du théorème des restes chinois, [F. M. 2] p. 189.

On suppose donnés n entiers $a_i \neq 0,\ 1 \leq i \leq n$ et n entiers $c_i,\ 1 \leq i \leq n$. On se propose de résoudre le système de congruences en l'inconnue $x \in \mathbb{Z}$, $x = c_i$ modulo a_i pour $1 \leq i \leq n$. Ce système est équivalent à la recherche des solutions entières du système linéaire suivant :

$A\ {}^t(x, x_1, x_2, ..., x_n) = {}^t(c_1, c_2, ..., c_n)$ avec

$A := Matrix([[1, -a_1, 0, 0, .., 0], [1, 0, -a_2, 0, 0, .., 0], ..., [1, 0, 0, .., 0, -a_n]]) \in M_{n,n+1}(\mathbb{Z})$, et

$(x, x_1, x_2, ..., x_n) \in \mathbb{Z}^{n+1}$.

Alors qu'il y a une solution générale élémentaire avec les congruences ; les méthodes de résolution algorithmique (forme normale d'Hermite ou forme de Smith) ne semblent appropriées que pour résoudre des systèmes numériques.

(1) Résolution par les congruences.

   (a) Montrer qu'une condition nécessaire pour l'existence d'une solution au système de congruences est que (a_i, a_j) divise $c_i - c_j$ pour tout $1 \leq i < j \leq n$

   (b) Réciproquement on va montrer que cette condition est suffisante. Supposons donc que les c_i sont des entiers tels que (a_i, a_j) divise $c_i - c_j$ pour tout $1 \leq i < j \leq n$.

On note μ le PPCM des $a_i,\ 1 \leq i \leq n$ et $d_i := \frac{\mu}{a_i}$.

(i) Montrer que $(d_i,\ 1 \leq i \leq n) = 1$ (on pourra raisonner avec les valuations p-adiques).

(ii) Soient $u_i \in \mathbb{Z}$ avec $\sum_{1 \leq i \leq n} u_i d_i = 1$. Montrer que a_j divise $d_j(a_i, a_j)$ pour $j \neq i$ (remarquer que $(a_i, a_j)(a_i, a_j) = a_i a_j$ et que (a_i, a_j) divise μ) et en déduire que $x_0 = \sum_{1 \leq i \leq n} c_i u_i d_i$ est solution du système.

(iii) Montrer que $x_0 + \mathbb{Z}\mu$ est l'ensemble des solutions du système de congruences.

(2) Résolution avec la forme normale d'Hermite, [Fr. A] exercice 1.4.38 p. 103 et inspiré de [Co.].

La matrice A est de rang n puisque les a_i sont supposés non nuls, alors $AU = H$ avec $U_i n\, \mathrm{GL}_n(\mathbb{Z})$ et $H = (h_{i,j}) \in M_{n,n+1}(\mathbb{Z})$ est triangulaire supérieure avec $h_{i,j} = 0$ pour $i \geq j$, $0 \leq h_{i,j} < h_{i,i+1} > 0$ pour $1 \leq i < j \leq n+1$. La résolution du système diophantien $A\ {}^t(x, x_1, x_2, ..., x_n) = {}^t(c_1, c_2, ..., c_n)$ est alors équivalente à celle du système $H\ {}^t(y_0, y_1, y_2, ..., y_n) = {}^t(c_1, c_2, ..., c_n)$ avec ${}^t(x, x_1, x_2, ..., x_n) = U\ {}^t(y_0, y_1, y_2, ..., y_n)$. On dit que H est la forme normale d'Hermite de la matrice A et elle est unique. En d'autres termes les matrices H décrivent un système de représentants des orbites des matrices $A \in M_{n,n+1}(\mathbb{Z})$ de rang n.

Exemple numérique avec $a_1 = 15, a_2 = 21, a_3 = 35$. On suppose donc que

$A := Matrix([[1, -15, 0, 0], [1, 0, -21, 0], [1, 0, 0, -35]])$.

Alors $H = Matrix([[0, 15, 10, 1], [1, 0, 7, 1], [0, 0, 0, 1]])$ et

$U = Matrix([[105, 0, -35, 1], [7, -1, -3, 0], [5, 0, -2, 0], [3, 0, -1, 0]])$ (attention Maple anglais pratiquant les actions à gauche il faut chercher la forme normale d'Hermite de la transposée de A et on obtient en transposant une matrice triangulaire inférieure ; la discussion fonctionne sur le même mode que ce qui suit). On doit alors résoudre le système diophantien $0y_0 + 15y_1 + 10y_2 + y_3 = c_1,\ 7y_2 + y_3 = c_2,\ y_3 = c_3$ en les inconnues $y_0, ..., y_3$. Ainsi $y_0 \in \mathbb{Z},\ y_3 = c_3,\ 7y_2 = c_2 - c_3,\ 15y_1 = (c_1 - c_3) - 10y_2$ d'où il suit les conditions nécéssaires pour l'existence d'une solution $7 \mid (c_2 - c_3)$ et $5 \mid (c_1 - c_3)$. Si ces dernières conditions sont satisfaites on a donc $y_2 = \frac{c_2 - c_3}{7}$ et donc $15y_1 = (c_1 - c_3) - 10\frac{c_2 - c_3}{7} = (c_1 - c_2) - 3\frac{c_2 - c_3}{7}$ d'où une autre condition nécessaire $3 \mid (c_2 - c_1)$. On a donc retrouvé les conditions nécessaires vues dans le théorème des chinois généralisé. Supposons donc ces conditions réalisées alors $3y_1 = \frac{c_1 - c_3}{5} - 2\frac{c_2 - c_3}{7}$ et $5y_1 = \frac{c_1 - c_2}{3} - \frac{c_2 - c_3}{7}$ d'où $y_1 = 2 * 3y_1 - 5y_1 = 2\frac{c_1 - c_3}{5} - 3\frac{c_2 - c_3}{7} - \frac{c_1 - c_2}{3}$, ainsi ${}^t(x, x_1, x_2, x_3) = U\ {}^t(y_0, y_1, y_2, y_3)$ d'où $x = 105y_0 - 5c_2 + 6c_3$ avec $y_0 \in \mathbb{Z}$.

Remarque. Même si la condition nécessaire et suffisante pour l'existence d'une solution i.e. $(a_i, a_j) \mid (c_i - c_j)$ est facile à vérifier cela n'est pas satisfaisant pour caractériser les n uplets $(c_1, ..., c_n)$ pour lesquels l'ensemble des solutions n'est pas vide. Dans l'exemple il s'agit de résoudre le système d'équations diophantiennes $c_2 - c_1 = 3a,\ c_3 - c_1 = 5b,\ c_3 - c_2 = 7c$ i.e. $c_2 = c_1 + 3a,\ c_3 = c_1 + 5b$ et $3a - 5b + 7c = 0$. Pour résoudre cette dernière équation on projette les solutions sur la première coordonnée a et puisque $(a, b, c) := (1, 9, 6)$ est solution il suit que si (a, b, c) est solution alors $(a, b, c) - a(1, 9, 6) = (0, -9a + b, -6a + c)$ est encore solution d'où l'ensmble des solutions $(a, 9a + 7d, 6a + 5d)$ avec $(a, d) \in \mathbb{Z}^2$. D'où la paramétrisation des triplets (c_1, c_2, c_3) pour lesquels le théorème des restes chinois avec $(a_1, a_2, a_3) = (15, 21, 35)$ a un ensemble non vide de solutions $(c_1, c_2, c_3) = (e, e + 3a, e + 45a + 35d)$ avec $(a, d, e) \in \mathbb{Z}^3$. C'est un sous-groupe S de $\mathbb{Z}^3$ dont les facteurs invariants sont $1, 1, 105$, ainsi $\frac{\mathbb{Z}^3}{S} \simeq \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{7\mathbb{Z}}$.

(3) Résolution sur un exemple avec la réduction à la forme de Smith. Cas $a_1 = 15, a_2 = 21, a_3 = 35$.

Par ce qui précède la CNS est $(\frac{c_1 - c_2}{3}, \frac{c_1 - c_3}{5}, \frac{c_2 - c_3}{7}) \in \mathbb{Z}^3$.

On résout le système $A\ {}^t(x, y, z, w) = (c_1, c_2, c_3)$ où

$A := Matrix([[1, -15, 0, 0], [1, 0, -21, 0], [1, 0, 0, -35]])$; Maple donne

$S = Matrix([[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 105, 0]])$ (c'était prévisible avec le pgcd des mineurs de taille donnée) et

$U = Matrix([[0, 0, 1], [-3, 1, 2], [14, -5, -9]])$ avec $det\ U = 1$ et

$V = Matrix([[1, -35, -735, 105], [0, -2, -42, 7], [0, -1, -20, 3], [0, -1, -21, 5]])$ avec $det\ V = 1$ et

$UAV = S$. Cela revient à résoudre $S\,{}^t(X,Y,Z,W) = U\,{}^t(c_1,c_2,c_3)^t$ avec ${}^t(x,y,z,w) = V\,{}^t(X,Y,Z,W)$. Ainsi on obtient la CNS $105Z = 14c_1 - 5c_2 - 9c_3$. On vérifie que la condition $(\frac{c_1-c_2}{3}, \frac{c_1-c_3}{5}, \frac{c_2-c_3}{7}) \in \mathbb{Z}^3$ implique bien la divisibilité par $3*5*7 = 105$ de $14c_1 - 5c_2 - 9c_3$ (remarquer que $14c_1 - 5c_2 - 9c_3 = 14(c_1 - c_2) + 9(c_2 - c_3) = 14(c_1 - c_3) + 5(c_3 - c_2)$)...