

4. Applications

4.1. Equations diophantiennes

$$2x + 5y = 7 \quad (1,1) \text{ est solution}$$

$$x^2 + y^3 + 7z = 8$$

$$ax + by = c \quad \text{avec } a, b, c \in \mathbb{Z}.$$

Si $b = 0$, $ax = c$: l'équation admet une solution ssi $a \mid c$

$$\text{et } S = \left\{ \left(\frac{c}{a} \right) \right\}.$$

• $ax + by = c$ Vérifier que $d = \text{pgcd}(a, b) \mid c$.

Si $d \nmid c$ alors $S = \emptyset$.

Supposons que $d \mid c$. On a $a'dx + b'dy = c'd$

En divisant par $d \neq 0$, $a'x + b'y = c'$. avec $a'n + b'n = 1$.

$$\text{Donc } a'x + b'y = a'x_0 + b'y_0$$

$$\text{Donc } a'(\underbrace{x - x_0}_{\in \mathbb{Z}}) = b'y_0 - b'y = b'(\underbrace{y_0 - y}_{\in \mathbb{Z}})$$

$a' \nmid n$
alors $a' \mid n$

Donc $a' \mid b'(y_0 - y)$. Or a' et b' sont premiers entre eux

Donc d'après le thm de Gauss, $a' \mid y_0 - y$.

Donc il existe $k \in \mathbb{Z}$ tel que $y_0 - y = ka'$

Donc $y = y_0 - ka'$. Donc $a'(x - x_0) = b'ka'$

Donc $x = x_0 + kb'$.

Donc $(x, y) = (x_0 + kb', y_0 - ka')$.

Réciproquement, $a'(x_0 + kb') + b'(y_0 - ka') = a'x_0 + \cancel{a'kb'} + b'y_0 - \cancel{b'ka'} = c'$.

Donc l'ensemble des solutions de $a'x + b'y = c'$, donc de

$ax + by = c$ est $S = \{ (x_0 + kb', y_0 - ka'), k \in \mathbb{Z} \}$.

Ex 82 $36x + 21y = 9$.

$\text{pgcd}(36, 21) = 3$. On a bien $3 \mid 9$.

$$36 = 21 \times 1 + 15$$

$$21 = 15 \times 1 + 6$$

$$15 = 6 \times 2 + 3$$

$$6 = 3 \times 2 + 0$$

En divisant par 3, l'équation se ramène à

$$12x + 7y = 3.$$

Donc l'ensemble des solutions dans $\mathbb{Z}^2$ de $36x + 21y = 9$ est

égal à l'ensemble des solutions dans $\mathbb{Z}^2$ de $12x + 7y = 3$.

12 et 7 sont premiers entre eux

On cherche $u, v \in \mathbb{Z}^2$ tels que $12u + 7v = 1$.

$$12 = 12 \times 1 + 7 \times 0$$

$$7 = 12 \times 0 + 7 \times 1$$

$$\times (-1) \quad 5 = 12 \times 1 + 7 \times (-1)$$

$$\times (-2) \quad 2 = 12 \times (-1) + 7 \times 2$$

$$1 = 12 \times 3 + 7 \times (-5)$$

En multipliant par 3, $3 = 12 \times 9 + 7 \times (-15)$

Donc $(x_0, y_0) = (9, -15)$ est une solution particulière de

$$3 = 12x + 7y.$$

On vérifie que $(x_0 + 7k, y_0 - 12k)$ est solution pour tout $k \in \mathbb{Z}$:

$$\begin{aligned} 12(x_0 + 7k) + 7(y_0 - 12k) &= 12x_0 + 12 \times 7k + 7y_0 - 7 \times 12k \\ &= 12x_0 + 7y_0 = 3. \end{aligned}$$

Par exemple, pour $k = 3$, $9 + 7 \times 21 = 30$ et $-15 - 12 \times 3 = -51$

$(30, -51)$ est une solution.

• Ex 84. Supposons que $(x, y) \in \mathbb{Z}^2$ soit solution de $x^2 + y^2 = 8z + 7$.

En regardant modulo 8, $8z + 7 \equiv 0z - 1 \equiv -1 \pmod{8}$.

a	0	1	2	3	4	5	6	7	$\pmod{8}$
---	---	---	---	---	---	---	---	---	------------

a^2	0	1	4	1	0	1	4	1	$\pmod{8}$
-------	---	---	---	---	---	---	---	---	------------

$$5 \equiv -3 \pmod{8} \quad \text{Donc} \quad s^2 \equiv (-3)^2 \equiv 3^2 \pmod{8} \equiv 1 \pmod{8}$$

$$\text{Donc } x^2 + y^2 \equiv 0, 1, 4, 2, 5 \pmod{8}.$$

$$\begin{matrix} \uparrow & \uparrow \\ \in \{0, 1, 4\} & \in \{0, 1, 4\} \end{matrix}$$

Donc $x^2 + y^2 \not\equiv 8z + 7 \pmod{8}$. Donc pas de solutions.

4. Applications

4.2. Anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. $(\mathbb{Z}/n\mathbb{Z}, +)$ groupe cyclique

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

$$\mathbb{R} \quad \begin{aligned} x+0 &= 0+x=x \\ x \times 1 &= 1 \times x=x \end{aligned}$$

$$\bar{a} \times \bar{1} = \overline{a \times 1} = \overline{1 \times a} = \bar{a}$$

 $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si il existe $u \in \mathbb{Z}$ tel que

$$\bar{a} \times \bar{u} (= \bar{u} \times \bar{a}) = \bar{1}.$$

$$\mathbb{Z}/3\mathbb{Z}, \quad \bar{2} \times \bar{2} = \bar{4} = \bar{1}$$

Sur $\mathbb{R}$, si $x \times y = 0$ alors $x=0$ ou $y=0$.

$$\begin{array}{c} au + nv = 1 \\ \uparrow \\ au + nv \equiv 1 \pmod{n} \end{array}$$

$$\bar{a} \bar{u} = \bar{1} \text{ dans } \mathbb{Z}/n\mathbb{Z}.$$

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases} (*)$$

$$\begin{cases} x_1 \equiv 1 \pmod{m_1} \\ x_1 \equiv 0 \pmod{m_2} \end{cases}$$

$$\text{et } \begin{cases} x_2 \equiv 0 \pmod{m_1} \\ x_2 \equiv 1 \pmod{m_2} \end{cases}$$

Donc $ax_1 + bx_2$ est solution de $(*)$:

$$\begin{aligned} ax_1 + bx_2 &\equiv a \pmod{m_1} \\ &\equiv a \pmod{m_1} \equiv 0 \pmod{m_1} \end{aligned}$$

$$\begin{aligned} ax_1 + bx_2 &\equiv b \pmod{m_2} \\ &\equiv 0 \pmod{m_2} \equiv b \pmod{m_2} \end{aligned}$$

 $m_1, m_2 = 1$ donc d'après le thm de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$\begin{aligned} um_1 + vm_2 &= 1 \\ &\equiv vm_2 \pmod{m_1} \end{aligned}$$

Alors

$$\begin{cases} vm_2 \equiv 1 \pmod{m_1} \\ vm_2 \equiv 0 \pmod{m_2} \end{cases}$$

$$\text{et } \begin{cases} um_1 \equiv 0 \pmod{m_1} \\ um_1 \equiv 1 \pmod{m_2} \end{cases}$$

$$x_1 = vm_2, \quad x_2 = um_1.$$

$$\text{Donc } ax_1 + bx_2 = avm_2 + bum_1.$$

est solution de $(*)$.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases} (*)$$

$$\begin{cases} x_1 \equiv 1 \pmod{m_1} \\ x_1 \equiv 0 \pmod{m_2} \\ \vdots \\ x_1 \equiv 0 \pmod{m_r} \end{cases}$$

$$\begin{cases} x_2 \equiv 0 \pmod{m_1} \\ x_2 \equiv 1 \pmod{m_2} \\ \vdots \\ x_2 \equiv 0 \pmod{m_r} \end{cases}$$

$$\begin{cases} x_n \equiv 0 \pmod{m_1} \\ \vdots \\ x_n \equiv 0 \pmod{m_{r-1}} \\ x_n \equiv 1 \pmod{m_r} \end{cases}$$

Alors $a_1x_1 + a_2x_2 + \dots + a_r x_r$ est solution de $(*)$ • m_1 et $m_2 \times m_3 \times \dots \times m_r = \Pi_1$ sont premiers entre eux, donc d'après le thm deBézout, il existe $(u_1, v_1) \in \mathbb{Z}^2$ tel que $u_1 m_1 + v_1 \Pi_1 = 1$.

$$\text{Alors } \begin{cases} v_1 \Pi_1 \equiv 1 \pmod{m_1} \\ v_1 \Pi_1 = v_1 m_2 \times m_3 \times \dots \times m_r \equiv 0 \pmod{m_2} \\ \vdots \\ v_1 \Pi_1 \equiv 0 \pmod{m_r} \end{cases}$$

$$x_1 = v_1 \Pi_1$$

$$\bullet \quad m_2 \quad \text{et} \quad \Pi_2 = m_1 \times \cancel{m_2} \times m_3 \times \dots \times m_r, \quad m_2 \wedge \Pi_2 = 1$$

$$v_2 m_2 + v_2 \Pi_2 = 1$$

$$\begin{cases} v_2 \Pi_2 \equiv 0 \pmod{m_1} \\ v_2 \Pi_2 \equiv 1 \pmod{m_2} \\ v_2 \Pi_2 \equiv 0 \pmod{m_3} \\ \vdots \\ v_2 \Pi_2 \equiv 0 \pmod{m_r} \end{cases}$$

$$x_2 = v_2 \Pi_2$$

$$\bullet \quad m_r \quad \text{et} \quad \Pi_r = m_1 \times m_2 \times \dots \times m_{r-1} \quad m_r \wedge \Pi_r = 1$$

$$v_r m_r + v_r \Pi_r = 1$$

$$\begin{cases} v_r \Pi_r \equiv 0 \pmod{m_1} \\ \vdots \\ v_r \Pi_r \equiv 0 \pmod{m_{r-1}} \\ v_r \Pi_r \equiv 1 \pmod{m_r} \end{cases}$$

$$x_r = v_r \Pi_r$$

Ex 94.

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 0 \pmod{5} \\ x \equiv 0 \pmod{9} \end{cases}$$

$$\underbrace{4}_{m_1} \quad \text{et} \quad \underbrace{5 \times 9 = 45}_{\Pi_1} \quad \text{sont premiers entre eux.}$$

$$45 = 4 \times 11 + 1, \quad 1 = 45 - 4 \times 11$$

$$\begin{cases} 45 \equiv 1 \pmod{4} \\ 45 \equiv 0 \pmod{5} \\ 45 \equiv 0 \pmod{9} \end{cases}$$

$$\begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 1 \pmod{5} \\ x \equiv 0 \pmod{9} \end{cases}$$

$$m_2 = 5 \quad \text{et} \quad \Pi_2 = 36$$

$$36 = 5 \times 7 + 1, \quad 1 = 36 - 5 \times 7$$

$$\begin{cases} 36 \equiv 0 \pmod{4} \\ 36 \equiv 1 \pmod{5} \\ 36 \equiv 0 \pmod{9} \end{cases}$$