AG1
Gr 1

TD du vendredi 27 novembre 2020

Exercice 6.11 1. Déterminer le pgcd d de $a := 2873$ et $b := 1001$ ainsi que deux entiers relatifs u et v tels que $au + bv = d$.
2. Peut-on trouver deux entiers u et v tels que $au + bv = 15$?

Rem méthodes pour calculer le pgcd de deux nombres entiers relatifs :

1) algo d'Euclide
2) on décompose a et b en nb. premiers
3) on teste la divisibilité de a et b par tous les nb premiers. ($\simeq$ 2)

1. A.E. (meth.1)

$2873 = 1001 \times 2 + 871$

$1001 = 871 \times 1 + 130$

$871 = 130 \times 6 + 91$

$130 = 91 \times 1 + 39$

221×13

$91 = 39 \times 2 + 13$

$39 = 13 \times 3$ pgcd = 13

(meth.2)

$2873 = 13 \times 221 = 13^{2} \times 17$

$1001 = 13 \times 77 = 7 \times 11 \times 13^{1}$

donc pgcd $= 13$

ppcm $= 7 \times 11 \times 13^2 \times 17$

Trouver u et v :

$13 = 91 - 39 \times 2 = \dots$ long !

$= \underbrace{-66}_{v} \times 1001 + \underbrace{23}_{u} \times 2873$

2. Existe-t-il u et v tels que $au + bv = 15$?

Non car a et b divisibles par 13

donc $au + bv \equiv 15 \equiv 2$ impossible !

$\not\equiv$ mod 13

Un thème de réflexion pour le week-end

4 et 7 premiers entre eux

$\Rightarrow$ il existe $u_0, v_0 \in \mathbb{Z}$ t.q. $4u_0 + 7v_0 = 1$

$\rightarrow \forall n \in \mathbb{Z}_{\geq 1}$, il existe $u, v \in \mathbb{Z}$ tels que $4u + 7v = n$.

Sur la planète Mars, les habitants utilisent deux types de pièces : a et b M$\not\in$ ("marsos") premiers entre eux.

Quels prix peut-on payer exactement, sans rendu de monnaie ?

Exercice 6.12

1. Montrer que tout entier pair a vérifie $a^2 \equiv 0 \mod 4$.
2. Montrer que tout entier impair a vérifie $a^2 \equiv 1 \mod 8$.
3. Soient a, b, c trois entiers *impairs*.
   (a) Quel est le reste de la division de $a^2 + b^2 + c^2$ par 8 ? En déduire que ce n'est pas un carré d'un entier.
   (b) En développant $(a+b+c)^2$, montrer que $ab + bc + ac \equiv 3 \mod 4$. En déduire que ce n'est pas non plus le carré d'un entier.

1. Si a est pair, il existe $n \in \mathbb{Z}$ tel que $a = 2n$. Alors $a^2 = 4n^2 \equiv 0 \mod 4$.

2. Si a est impair, il existe $n \in \mathbb{Z}$ tel que $a = 2n+1$. Alors $a^2 = 4n^2 + 4n + 1$

$$= 4n(n+1) + 1$$

l'un des 2 est pair !

donc 8 divise $4n(n+1)$

$$\equiv 1 \mod 8$$

Alternative : écrire la table des carrés mod 8

a	1	3	5	7
a^2	1	1	1	1

Exercice 6.12 1. Montrer que tout entier pair a vérifie $a^2 \equiv 0 \mod 4$.
2. Montrer que tout entier impair a vérifie $a^2 \equiv 1 \mod 8$.
3. Soient a, b, c trois entiers *impairs*.
   (a) Quel est le reste de la division de $a^2 + b^2 + c^2$ par 8 ? En déduire que ce n'est pas un carré d'un entier.

3.(a) D'après la question 2, on a

$$a^2+b^2+c^2 \equiv 1+1+1 \equiv 3 \mod 8.$$

Le reste demandé est 3.

Donc $a^2+b^2+c^2$ ne peut pas être le carré d'un entier d, car

$$d^2 \equiv \begin{cases} 0 \text{ ou } 4 \mod 8 & \text{si } d \text{ pair (ques. 1)} \\ 1 \mod 8 & \text{si } d \text{ impair (Q.2)} \end{cases}$$

(b) En développant $(a+b+c)^2$, montrer que $ab+bc+ac \equiv 3 \mod 4$. En déduire que ce n'est pas non plus le carré d'un entier.

(b) $(\underbrace{a+b+c}_{\text{impair}})^2 = \underbrace{a^2+b^2+c^2}_{\equiv 3 \mod 8} + 2ab+2ac+2bc$

$///$

$1 \mod 8$

par 2.

$1 \equiv 3+2ab+2ac+2bc \mod 8$

donc $2ab+2ac+2b \equiv 1-3 \equiv -2$

$\equiv 6 \mod 8.$

Ceci signifie qu'il existe $k \in \mathbb{Z}$ t.q.

$$2ab+2ac+2bc = 6+8k.$$

On déduit $ab+ac+bc = 3+4k$

c'est-à-dire $ab+ac+bc \equiv 3 \mod 4$.

Donc $ab+ac+bc$ ne peut pas être le carré d'un entier d, car $d^2 \equiv \begin{cases} 0 \mod 4 & (d \text{ pair}) \\ 1 \mod 4 & (d \text{ impair}) \end{cases}$

[Rem: si $n \equiv 1 \mod 8$ alors $n \equiv 1 \mod 4$!]

d'où $ab+ac+bc \not\equiv 3 \mod 4$ impossible !

$\| $

$d^2 \not\equiv 0$ ou $1 \mod 4$

Exercice 6.13 1. Montrer que si a et b sont premiers entre eux alors a et $a+b$ sont aussi premiers entre eux.
2. Montrer que si a est premier avec b et c, alors a est premier avec bc.
3. Montrer que si a et b sont premiers entre eux, alors pour tous entiers naturels k et l, a^k et b^l sont aussi premiers entre eux.

1. Méth 1 : si a et a+b ne sont pas premiers entre eux, leur pgcd d est $\neq 1$.

Alors $d|a$ et $d|a+b$

donc $a \equiv 0\ (d)$ et $a+b \equiv 0\ (d)$

donc $b \equiv (a+b)-a \equiv 0\ (d)$

donc a et b divisibles par d, contrad.

Méth 2

Proposition 6.3.2 — Algorithme d'Euclide. Soient $a, p, b, q \in \mathbb{Z}$ avec $b \neq 0$ et $0 \leq r < b$ tels que $a = bq + r$. Alors, $a \wedge b = b \wedge r$.

$$b = aq + r \quad 0 \leqslant r < a \qquad (1)$$

$$\Rightarrow a+b = a(q+1) + r \quad 0 \leqslant r < a \qquad (2)$$

donc $(a+b) \wedge a = a \wedge r = a \wedge b$

(2) (1)

Prop. 6.3.2 entraîne ces deux égalités

Méth 3 (Bézout)

$\Rightarrow \exists (u,v) \in \mathbb{Z}^2$ tq $au + bv = 1$

$\Rightarrow$ ... $au + (a+b)v - av = 1$

$\Rightarrow$ $a(u-v) + (a+b)v = 1$

(u' sous $a(u-v)$, v' sous $(a+b)v$)

$\Rightarrow$ (Bézout encore) a et $a+b$ prem. entre eux

2. Différentes manières de traduire le fait que a et b sont premiers entre eux :

* $\text{pgcd}(a,b) = 1$
* aucun nb premier ne divise a et b.
* il existe $u,v \in \mathbb{Z}$ tq $au + bv = 1$
* il n'y a aucun nb premier en commun parmi les facteurs des décomp. en facteurs premiers de a et b.