2. PGCD, PPCM

2.3. Entiers premiers entre eux

Prop 46.

$1 \times n + (n-1) \times (-1) = 1$ $\qquad$ $(n+1) \times 1 + n \times (-1) = 1$

Prop 49 $\quad$ • Existence $\quad r \in \mathbb{Q}$, $r = \frac{a}{b}$ avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$

Posons $d = pgcd(a,b)$. Alors $a = da'$, $b = db'$ avec $pgcd(a',b') = 1$

et $b' > 0$. Donc $r = \frac{da'}{db'} = \frac{a'}{b'}$ et $a' \wedge b' = 1$.

• Unicité : $r = \frac{p_1}{q_1} = \frac{p_2}{q_2}$ avec $p_1 \wedge q_1 = 1$, $p_2 \wedge q_2 = 1$

et $p_1, p_2 \in \mathbb{Z}$, $q_1, q_2 \in \mathbb{N}^*$.

On a $p_1 q_2 = q_1 p_2$. Donc $q_2 | q_1 p_2$. Or q_2 et p_2 sont premiers entre eux. Donc par le théorème de Gauss, $q_2 | q_1$.

Mais $q_1 | p_1 q_2$, donc $q_1 | q_2$. Donc $q_1 = q_2$ (car $q_1, q_2 \geq 0$)

Donc $p_1 q_1 = q_1 p_2$, donc $p_1 = p_2$.

2. PGCD, PPCM

2.4. PPCM

$a\mathbb{Z} + b\mathbb{Z} = \underset{\uparrow pgcd(a,b)}{d}\mathbb{Z}$ $\quad d \in \mathbb{N}$ $\qquad$ $a\mathbb{Z} \cap b\mathbb{Z} = \underset{\uparrow ppcm(a,b)}{m}\mathbb{Z}$, $m \in \mathbb{N}$

$A \cap B \subset A$, $\quad A \cap B \subset B$

Prop. 58 $\quad pgcd(a,b) = pgcd(|a|,|b|)$, $\quad ppcm(a,b) = ppcm(|a|,|b|)$

Supp $a > 0$, $b > 0$. Posons $d = pgcd(a,b)$.

Alors $a = da'$, $b = db'$ avec $(a',b') \in \mathbb{N}^*$ et $pgcd(a',b') = 1$.

Alors $ab = d \times \underbrace{da'b'}_{ppcm(a,b)}$ $\qquad$ $d \times ppcm(a,b) = ab$

Posons $m = da'b'$.

1. $m = ab'$ donc $a | m$, $m = a'b$ donc $b | m$.

2. Soit $m' \in \mathbb{Z}$ tel que $a | m'$ et $b | m'$. Mq $m | m'$. $(m' = k\,m$ $= k\,da'b')$

Donc $m' = a \times u$ avec $u \in \mathbb{Z}$, $m' = b \times v$ avec $v \in \mathbb{Z}$.

Donc $au = bv$, donc $da'u = db'v$ donc $a'u = b'v$.

Donc $a' \mid b'v$ mais a' et b' sont premiers entre eux,
donc d'après le thm de Gauss, $a' \mid v$.

Donc $v = ka'$ avec $k \in \mathbb{Z}$.

Donc $m' = bv = db'ka' = k \times da'b' = km$. Donc $m \mid m'$.

Donc d'après la caractérisation du ppcm, $m = \text{ppcm}(a,b)$.

et

3. Nombres premiers

Cours 11 (3)

1. L'ensemble des nombres premiers

$p = \min\{\text{diviseurs} > 1 \text{ de } n\}$

p est premier et $p \mid n$. Donc $n = p \times q$ où $q \in \mathbb{N}$.

Donc q diviseur de n, et $q \geq 2$ et $p \leq q$

Donc $p^2 = p \times p \leq p \times q = n$. Donc $p \leq \sqrt{n}$.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19

⋮

... ~~100~~

3. Nombres premiers

2. Décomposition en produit de facteurs premiers

$v_2(8)=3$

$8 = 2^3$, $9 = 3^2$, $12 = 2^2 \times 3 = 3 \times 2^2$

$v_3(9) = 2$

$v_2(9) = 0$

$v_2(12) = 2$, $v_3(12) = 1$

$n = p_1^{\alpha_1} \cdots p_N^{\alpha_N}$.

si p premier et $p \mid a_1 \times \cdots \times a_n$ alors p divise l'un des a_i.

$$p_i \mid \underbrace{q_1 \times \cdots q_1}_{\beta_1} \times \underbrace{q_2 \times \cdots \times q_2}_{\beta_2} \times \cdots \times \underbrace{q_R \times \cdots \times q_R}_{\beta_R} \qquad p_i \mid q_j$$

360	2
180	2
90	2
45	3
15	3
5	5
1	

$360 = 2^3 \times 3^2 \times 5$.

147	3
49	7
7	7
1	

$$\begin{array}{r|l} 147 & 3 \\ \hline 27 & 49 \end{array}$$

$147 = 3^1 \times 7^2 \times 5^0$

$1575 = 3^2 \times 5^2 \times 7^1$

$$360 = 36 \times 10 = 6^2 \times 5 \times 2 = (3 \times 2)^2 \times 5 \times 2 = 2^3 \times 3^2 \times 5.$$

$\mathrm{pgcd}(147, 1575) = 3^1 \times 5^0 \times 7^1 = 3 \times 7 = 21$.

$\mathrm{ppcm}(147, 1575) = 3^2 \times 5^2 \times 7^2$

$c \in \mathbb{Z}$. $\quad c = \pm n$ où $n \in \mathbb{N}$.

$= \pm p_1^{\alpha_1} \cdots p_N^{\alpha_N}$. $\qquad 1 = p_1^0 \times \cdots \times p_N^0$.