TD 12 - Vendredi 20 novembre 2020

$n \in \mathbb{N}$ $\quad n = p_1 \cdots p_r = \prod_{i=1}^{r} p_i$ $\quad p_i$ premier

$= \prod_{j=1}^{s} q_j^{\alpha_j}$ où $\alpha_j \geq 0$ et q_j nombre premier $q_j \neq q_{j'}$ si $j \neq j'$

si $a = \prod p_i^{\alpha_i}$ $\quad \alpha_i \geq 0$ $\quad p_i \neq p_j$ si $i \neq j$

$b = \prod p_i^{\beta_i}$ $\quad \beta_i \geq 0$

alors $\quad pgcd(a,b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$

$ppcm(a,b) = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$

ex 4.4 1. $a = 66$, $b = 21$.

$66 = a = 6 \times 11$

$= 2 \times 3 \times 11$

$= 2 \times 3 \times 7^0 \times 11$

$21 = 3 \times 7 = 2^0 \times 3 \times 7 \times 11^0$

$pgcd(a,b) = 2^0 \times 3 \times 7^0 \times 11^0$

$= 3.$

$ppcm(a,b) = 2 \times 3 \times 7 \times 11$

$= 42 \times 11$

$= 462.$

2. $a = 54 = 6 \times 9$

$= 2^0 \times 3^3$

$b = 12 = 2^2 \times 3$

$pgcd(a,b) = 2 \times 3$

$= 6.$

$ppcm(a,b) = 2^2 \times 3^3$

$= 108.$

3. $a = 70$ $\quad b = 91 = 7 \times 13$

$= 2 \times 5 \times 7$

$pgcd(a,b) = 7$

$ppcm(a,b) = 2 \times 5 \times 7 \times 13$

$= 910.$

ex 4.5 : $\mathcal{P} = \{n \in \mathbb{N} \mid n \text{ est premier}\} \subset \mathbb{N}$

Mq $\mathcal{P}$ est infini.

Par l'absurde, on suppose que $\mathcal{P}$ est fini : $\mathcal{P} = \{p_1, \dots, p_n\}$, $p_i \neq p_j$ si $i \neq j$.

$q = p_1 \cdots p_n + 1$.

1- Soit $i \in \{1, \dots, n\}$. Si $p_i \mid q$, $p_i \mid q - p_1 \cdots p_n = 1$ donc $p_i = 1$: pas possible. Donc $p_i \nmid q$

2- $q \in \mathbb{N}$ donc il existe $p \in \mathcal{P}$ tel que $p \mid q$. $\exists i \in \{1, \dots, n\}$ tq $p = p_i$ et $p_i \mid q$. Or par 1-, c'est pas possible.

→ Contradiction et $\mathcal{P}$ est infini.

[Euclide ~ -400 av J.C]

exercice 4.6 : Soit $n \geq 2$ non premier. $a, b \geq 2$.

1. $\exists a, b \in \mathbb{N}$, $a, b \neq 1$ tq $n = ab$.

Par l'absurde, supposons $a > \sqrt{n}$ et $b > \sqrt{n}$. Alors $n = ab > \sqrt{n} \times \sqrt{n} = n$ absurde. Donc $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

autre façon de conclure : Par ex $a \leq b$. donc $n = ab \geq a^2$, $\sqrt{n} \geq a$

2. Il suffit de prendre un diviseur premier p de n :

$p \mid n$ donc $2 \leq p \leq n \leq \sqrt{n}$ ✓.

Comme $m \mid n$, $p \mid n$.

→ $n \in \mathbb{N}$ Pour mq n est premier, il suffit de faire les divisions euclidiennes $\frac{n}{r}$ pour $2 \leq r \leq \sqrt{n}$.

ex 4.7 : 1- $2 \leq n \leq 48$. Si n n'est pas premier, il existe p premier, $2 \leq p \leq \sqrt{n}$ tq $p \mid n$ (ex 4.6).

Or, $\sqrt{n} < \sqrt{49} = 7$ donc $2 \leq p < 7$ et p premier

$\Rightarrow p = 2$ ou 3 ou 5.

donc n est divisible par 2, 3 ou 5.

Soit $d \geq 1$

2- $\text{card}(A_d) = \text{card}\{n \in \mathbb{N} \mid 1 \leq n \leq 48 \text{ et } d \mid n\}$

$= \text{card}\{kd : 1 \leq kd \leq 48\}$

$= \text{card}\{kd : \frac{1}{d} \leq k \leq \frac{48}{d}\}$

$1 \leq k \leq \left[\frac{48}{d}\right]$

$= \text{card}\{k \in \mathbb{N} \mid 0 < \frac{1}{d} \leq k \leq \frac{48}{d}\}$

$= \left[\frac{48}{d}\right]$ = partie entière de $\frac{48}{d} = \max\{r \in \mathbb{N}, r \leq \frac{48}{d}\}$

3- $\text{pgcd}(2,3) = 1$ donc si $n \in \mathbb{N}$, $2 \mid n$ et $3 \mid n \Rightarrow 6 \mid n$.

Inversement, $6 \mid n \Rightarrow 2 \mid n$ et $3 \mid n$.

donc $A_2 \cap A_3 = A_6$.

4. De façon analogue, $A_2 \cap A_5 = A_{10}$

$A_3 \cap A_5 = A_{15}$

$A_2 \cap A_3 \cap A_5 = A_{30}$.

5- $\text{card}(A_2 \cup A_3 \cup A_5) = \text{card}(\{2 \leq n \leq 48, n \text{ non premier}\} \cup \{2,3,5\})$

$= \text{card}(A_2) + \text{card}(A_3) + \text{card}(A_5) - \text{card}(A_6) - \text{card}(A_{10})$

$- \text{card}(A_{15})$

$+ \text{card}(A_{30})$

$9 < \ell < 10$; $3 < \ell < 4$

$= \left[\frac{48}{2}\right] + \left[\frac{48}{3}\right] + \left[\frac{48}{5}\right] - \left[\frac{48}{6}\right] - \left[\frac{48}{10}\right] - \left[\frac{48}{15}\right] + \left[\frac{48}{30}\right]$

$= 24 + 16 + 9 - 8 - 4 - 3 + 1$

$= 35$

donc $\text{card}\{2 \leq n \leq 48,\ n \text{ premier}\} = 47 - 35 = 12$.

$n \neq 2, 3, 5.$

$= \{n \in \mathbb{N},\ 2 \leq n \leq 48\} \setminus (A_2 \cup A_3 \cup A_5)$

donc $\text{card}\{2 \leq n \leq 48,\ n \text{ premier}\} = 12 + 3 = 15$.

6 - 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

crible

~~1~~	~~1~~	2	3	~~4~~	~~5~~	~~6~~	7	~~8~~	~~9~~
10	11	12	13	~~14~~	~~15~~	16	17	~~18~~	19
~~20~~	~~21~~	22	23	24	25	~~26~~	~~27~~	28	29
~~30~~	31	~~32~~	~~33~~	34	~~35~~	~~36~~	37	~~38~~	~~39~~
~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~
~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59
~~60~~	61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	~~67~~	~~68~~	~~69~~
~~70~~	71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79
~~80~~	~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89
~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	~~97~~	~~98~~	~~99~~

$2 \leq n \leq 100$

n non premier,

$\exists p$ premier, $p \mid n$,

$p \leq \sqrt{100} = 10$

donc $p = 2, 3, 5, 7$

ex 4.8 : p nombre premier > 3 $\left[\text{Rq} \quad \begin{matrix} 2 \mid k(k+1) \\ r \mid s \cdot (s+1) \cdots (s+r-1) \end{matrix} \right]$ $r, s \in \mathbb{N}$

1. $(p-1)p(p+1)$ est un produit de 3 entiers consécutifs donc est divisible par 3.

p premier, $p > 3 \Rightarrow p \neq 3$ donc $3 \nmid p$ donc $\text{pgcd}(3, p) = 1$.

3 / $p(p-1)(p+1)$, par le lemme de Gauss, $3 \mid (p-1)(p+1) = p^2 - 1$.

2 - On veut $8 \mid p^2 - 1$. En effet, p est impair : $\exists k \in \mathbb{N}$, $p = 2k + 1$.

donc $p^2 = 4k^2 + 4k + 1$ et $p^2 - 1 = 4(k^2 + k) = 4k(k+1)$ est divisible par 8

donc $\begin{cases} 3 \mid p^2 - 1, \quad 8 \mid p^2 - 1 \\ \text{pgcd}(3, 8) = 1 \end{cases} \Rightarrow \boxed{3 \times 8 = 24 \mid p^2 - 1}$

divisible par 2 car produit de 2 nbres consécutifs.

$p^2 \equiv 1 \ [24]$.

4g. $d \in \mathbb{Z}$. $\mathbb{Z}/d\mathbb{Z}$ = quotient de $\mathbb{Z}$ par la rel d'eq

$n \sim m \iff n-m$ est divisible par d.

$\mathbb{Z}/d\mathbb{Z} = \{\bar{n} : n \in \mathbb{Z}\}$ $n \sim n' \iff n-n'$ ——

$= \{\bar{0}, \bar{1}, \dots, \overline{d-1}\}$ card $\mathbb{Z}/d\mathbb{Z} = d$.

$\mathbb{Z} \supset \bar{n} = \{n + kd : k \in \mathbb{Z}\}$

$= n + d\mathbb{Z}$

On peut construire sur $\mathbb{Z}/d\mathbb{Z}$ une addition $+$, multiplication $\times$.

$+ : \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$

$(\bar{n}, \bar{m}) \longmapsto \overline{n+m} =: \bar{n} + \bar{m}$

On peut aussi $\bar{n} = \overline{n'}$ avec $n \neq n'$. "n et n' sont 2 représentants de $\bar{n} \in \mathbb{Z}/d\mathbb{Z}$"

$\bar{m} = \overline{m'}$ avec $m \neq m'$.

on doit vérifier que $\overline{m'} + \overline{n'} = \overline{m'+n'}$

$\bar{m} + \bar{n} = \overline{m+n}$

Il faut vérifier que $\overline{m'+n'} = \overline{n+n}$.

On a $d \mid n-n'$ donc $(m+n) - (m'+n')$

$d \mid m-m'$. $= (m-m') + (n-n')$

$\vdots$ divisible par d.

donc $\overline{m+n} = \overline{m'+n'}$

$\times : \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$

$(c, c') \longmapsto \overline{nm}$ où n est tq $\bar{n} = c$

et m est tq $\bar{m} = c'$.

Il faut vérifier que $\overline{nm}$ ne dépend des choix de n et m.

si $\bar{n} = \overline{n'} = c$, $\bar{m} = \overline{m'} = c'$,

On veut mq $\overline{nm} = \overline{n'm'}$

Or, $d \mid n-n'$, $d \mid m-m'$ il s'agit de voir que $d \mid nm - n'm'$

$nm - n'm' = n(m-m') + nm' - n'm'$

$= n(m-m') + m'(n-n')$.

est divisible par d donc $\overline{nm} = \overline{n'm'}$.

$(\mathbb{Z}/d\mathbb{Z}, +, \times)$ bonnes propriétés : e.g.

$\bar{n} \times (\bar{m} + \bar{r}) = \bar{n}\bar{m} + \bar{n}\bar{r}$, ...

$\rightsquigarrow \mathbb{Z}/d\mathbb{Z}$ est un anneau

ex 4.9.

$d = 5$

$\bar{n}$ \ $\bar{m}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\mathbb{Z}/6\mathbb{Z}$.

Pour le 27/11 finir 4.9, 4.10, 4.11.