* = développement

104 Nombres premiers. Propriétés et applications.

I Définition et premières propriétés.

Déf 1 : $p \in \mathbb{N}^*$ est premier si :
- $p \geq 2$
- ses seuls diviseurs positifs sont 1 et p.

On note $\mathbb{P}$ l'ensemble des nombres premiers.

Thm 2 : Il existe une infinité de nombres premiers.

Thm 3 : $\forall n \in \mathbb{Z}^* \setminus \{-1;1\}$, $\exists p \in \mathbb{P}$ tel que $p \mid n$. On dit que n est composé.

Thm 4 : $\forall n \geq 2$ entier naturel composé, n admet au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$ (crible d'Eratosthène).

II Applications.

① Théorème fondamental de l'arithmétique :

Thm 5 : $\forall n \geq 2$ entier naturel peut s'écrire de manière unique :

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

avec $\forall i \in [\![1;r]\!]$:

$$\begin{cases} p_i \in \mathbb{P} \quad \text{et} \quad p_1 < p_2 < \dots < p_r \\ \alpha_i \in \mathbb{N}^* . \end{cases}$$

Thm 6 : Application aux PGCD et PPCM :

Si $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ et $m = \prod_{k=1}^{r} p_k^{\beta_k}$

Alors :

$$\begin{cases} n \wedge m = \prod_{k=1}^{r} p_k^{\min(\alpha_k, \beta_k)} \\ n \vee m = \prod_{k=1}^{r} p_k^{\max(\alpha_k, \beta_k)} \end{cases}$$

② Fermat et Wilson :

Thm 7 : Petit thm de Fermat :

$$p \in \mathbb{P} \Rightarrow \forall a \in \mathbb{Z}, \begin{cases} a^p \equiv a \, [p] \\ p \nmid a \Rightarrow a^{p-1} \equiv 1 \, [p]. \end{cases}$$

Contre-exemple : Nombres de Carmichaël : $n \geq 3$ entier naturel non premier tq $\forall a \wedge n = 1$, $a^{n-1} \equiv 1 \, [n]$.

ex : 561.

Thm 8 : $\mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow n \in \mathbb{P}$.

Thm 9 : Thm de Wilson :
$p \in \mathbb{P} \Leftrightarrow (p-1)! \equiv -1 \, [p]$.

③ Autres :

Thm 10 : Thm des 2 carrés : *

$p \in \mathbb{P}$. LASSE :
1. $\exists a, b \in \mathbb{Z}$ tq $a^2 + b^2 = p$
2. $p \in \mathbb{Z}[i]$ non irréductible ds $\mathbb{Z}[i]$
3. -1 est un carré modulo p.
4. $p \equiv 1 \, [4]$ ou $p \equiv 2 \, [4]$.

Exemples : $(n \in \mathbb{N})$.

* Nombres de Fermat : $F_n = 2^{2^n} - 1$
- $\forall n, m \in \mathbb{N}$, $n \neq m \Rightarrow F_n \wedge F_m = 1$
- F_1 à $4 \in \mathbb{P}$, F_5 à $32 \notin \mathbb{P}$.

* Nombres de Mersenne : $M_n = 2^n - 1$
- $M_n \in \mathbb{P} \Rightarrow n \in \mathbb{P}$
- Réc. fausse : $M_{11} = 2047 \notin \mathbb{P}$

* R.S.A