104 Nombres premiers. Propriétés et applications.

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

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

2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 47...

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

Preuve:
On note $D_n = \{k \mid n \,/\, k \in \mathbb{N}^*\}$.
$D_n \neq \emptyset$ car $\{1; n\} \subset D_n$.
Soit $p = \min(D_n \setminus \{1\})$.
* $p \notin \mathbb{P} \Rightarrow \exists k \in \mathbb{N}^*$ tel que $k \mid p$. Donc $k \mid n$, donc $k \in D_n \setminus \{1\}$, ce qui est absurde car p est le plus petit élément de $D_n \setminus \{1\}$. Donc $p \in \mathbb{P}$. ▨

Thm:
Il existe une infinité de nombres premiers.

Preuve:
On sait déjà que $\mathbb{P} \neq \emptyset$ (car $2 \in \mathbb{P}$).
Supposons $\mathbb{P}$ fini.
On peut alors écrire $\mathbb{P} = \{p_1, p_2, \dots, p_n\}$.
Posons $M = \prod_{k=1}^{n} p_k + 1$.

$M \geq 2$ donc $\exists i \in [\![1; n]\!]$ tel que $p_i \mid M$.
De plus $p_i \mid \prod_{k=1}^{n} p_k$ car $i \in [\![1; n]\!]$.

Donc $p_i \mid M - \prod_{k=1}^{n} p_k = 1$, ce qui est absurde. ▨

Définition:
$n \geq 2$ non premier est dit composé :
$\exists p \in \mathbb{P}$ et $q \geq 2$ tq $n = pq$.

Thm:
$\forall n \geq 2$ entier naturel composé, n admet au moins un diviseur premier p tq $2 \leq p \leq \sqrt{n}$.

Preuve: $D_n = \{k \mid n \,/\, k \in \mathbb{N}^*\}$.

Notons $p = \min(D_n \setminus \{1\})$. On sait que $p \in \mathbb{P}$ et $p \mid n$.

Donc $\exists q \in D_n \setminus \{1\}$ tel que $n = pq$.
On a $2 \leq q \leq n$ et $p \leq q$ par déf. de p.
Donc $p^2 \leq pq = n$, soit $p \leq \sqrt{n}$. ▨

Application: Crible d'Eratosthène.
ex: $n = 1861$. $\sqrt{n} \approx 43,1$
$2 \nmid n$, $3 \nmid n$, $5 \nmid n$, ..., $43 \nmid n$.
Donc $n \in \mathbb{P}$.

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

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

avec $\begin{cases} \forall i \in [\![1; r]\!],\ p_i \in \mathbb{P} \text{ et } p_1 < p_2 < \cdots < p_r \\ \forall i \in [\![1; r]\!],\ \alpha_i \in \mathbb{N}^* \end{cases}$.

Preuve:
* Existence : Récurrence forte :
  → Initialisation: $n = 2 = 2^1$, $P(2)$ est vérifiée.
  → Hérédité: Supposons $P(k)$ vérifiée $\forall k \in [\![2; n]\!]$.
    • Si $n+1 \in \mathbb{P}$, alors $n+1 = (n+1)^1$, c'est la décomposition.
    • Sinon :
$n+1 \notin \mathbb{P}$, donc il est composé et on peut écrire $n+1 = ab$ avec $a, b \in [\![2; n]\!]$.
Par hypothèse de récurrence appliquée à a et b, on a la décomposition de $n \Rightarrow P(n+1)$ vérifiée.
  → Conclusion : $P(n)$ est vérifiée $\forall n \geq 2$.
* Unicité: Récurrence forte :
  → Initialisation: $P(2)$ immédiatement vérifiée.
  → Hérédité : Supposons $P(k)$ vérifiée $\forall k \in [\![2; n]\!]$.
Si $n+1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_s^{\beta_s}$
a 2 décompositions en facteurs premiers.
$p_1 \in \mathbb{P}$ et $p_1 \mid q_1^{\beta_1} \cdots q_s^{\beta_s}$, donc $\exists k \in [\![1; s]\!]$ tel que $p_1 \mid q_k$. Or $q_k \in \mathbb{P}$ donc nécessairement $p_1 = q_k$.
On peut alors simplifier par p_1, et on a alors la décomp. d'un entier de $[\![2; n]\!]$, on peut alors conclure avec l'hyp. de récurrence.

▨

Définition: Décomp. en facteurs $\mathbb{P}$:

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

Alors:

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

Preuve:

* $\delta = \prod_{k=1}^{r} p_k^{\min(\alpha_k, \beta_k)}$.

$\min(\alpha_k, \beta_k) \leq \alpha_k$ et β_k

donc $\delta \mid n$ et $\delta \mid m$. Soit $d \mid n$ et m.

Donc $d = \prod_{k=1}^{r} p_k^{\gamma_k}$, avec $\gamma_k \in \mathbb{N}$ tels que $\gamma_k \leq \alpha_k$ et $\gamma_k \leq \beta_k$ $\forall k \in [\![1; r]\!]$.

D'où $\begin{cases} \gamma_k \leq \min(\alpha_k, \beta_k) \ \forall k \in [\![1; r]\!] \\ d \mid \delta \end{cases}$

Donc $\delta = \text{pgcd}(n, m)$.

* $n \vee m = \frac{nm}{n \wedge m} = \prod_{k=1}^{r} p_k^{\alpha_k + \beta_k - \min(\alpha_k, \beta_k)}$.

Or $\forall k \in [\![1; r]\!]$, $\alpha_k + \beta_k - \min(\alpha_k, \beta_k) = \max(\alpha_k, \beta_k)$. ▨

Petit thm de Fermat:

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

Preuve: (rmq: se fait aussi par récurrence mais triste).

* Soit $t = \text{ord}(a)$ dans $\mathbb{Z}/p\mathbb{Z}^*$, on suppose $p \nmid a$.

On a $\text{ord}(\mathbb{Z}/p\mathbb{Z}^*) = p - 1$.

Donc d'après le thm de Lagrange:

$t \mid p-1 \Rightarrow \exists k \in \mathbb{N}$ tq $p - 1 = tk$.

Donc $a^{p-1} = a^{tk} \equiv 1 \ [p]$.

* Équivalence des 2 énoncés:

$p \nmid a$: $a^{p-1} \equiv 1 \ [p] \iff a^p \equiv a \ [p]$.

car $a^p - a = a(a^{p-1} - 1)$

Or $p \mid a^p - a \iff \underbrace{p \mid a}_{\text{impossible par hyp.}}$ ou $p \mid a^{p-1} - 1$

▨

⚠ **Contre-exemple important:**

Définition:

$n \geq 3$ entier non premier est un nombre de Carmichaël si

$\forall a \wedge n = 1$, $a^{n-1} \equiv 1 \ [n]$

Ex: $n = 561 = 3 \times 11 \times 17 \notin \mathbb{P}$.

$a \wedge 561 = 1 \Rightarrow a \wedge \begin{cases} 3 \\ 11 \\ 17 \end{cases} = 1$

Or $560 = 2 \times 280 = 10 \times 56 = 16 \times 35$

donc par Fermat: $a^{560} \equiv 1 \ [3, 11 \text{ et } 17]$

soit $a^{560} \equiv 1 \ [561]$ ②

Thm:
$\mathbb{Z}/m\mathbb{Z}$ est un corps $\Leftrightarrow$ $m \in \mathbb{P}$.

Preuve:

⇐ $m \in \mathbb{P}$

Si $a \wedge m = 1$, d'après Bézout, $\exists b, c \in \mathbb{Z}$ tels que :

$$ab + mc = 1.$$

Donc $\overline{a}$ est inversible d'inverse $\overline{b}$.

⇒ Par contraposée :

$m \notin \mathbb{P} \Rightarrow \exists a, b \in [\![1; m[\![$ tels que $m = ab$.

Ainsi $\begin{cases} \overline{a} \mid \overline{0} \\ \overline{b} \mid \overline{0} \end{cases}$, ce qui n'est pas possible dans un corps.

■

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

Preuve:

⇒ $p \in \mathbb{P} \Rightarrow$ $(\mathbb{Z}/p\mathbb{Z})$ est un corps

$\forall \overline{k} \in (\mathbb{Z}/p\mathbb{Z})^*$, $\overline{k}$ est racine de $X^{p-1} - \overline{1}$

↳ d'après Fermat : $k \wedge p = 1 \Rightarrow k^{p-1} \equiv 1 \ [p]$.

$$\Rightarrow X^{p-1} - \overline{1} = \prod_{k=1}^{p-1} (X - \overline{k}).$$

Évaluons cette expression en 0 :

$$-\overline{1} = \prod_{k=1}^{p-1} (-\overline{k})$$

$$-\overline{1} = (-1)^{p-1} \cdot \overline{(p-1)!}$$

Ie : $(-1)^{p-1}(p-1)! \equiv -1 \ [p]$

- Si $p = 2$: $(-1)^1 \times 1! \equiv -1 \ [p]$ ok.
- Sinon : p est impair donc on a $p-1$ pair donc $(-1)^{p-1} = 1$ et l'expression devient :

$$(p-1)! \equiv -1 \ [p].$$

⇐ Soit $p \geq 2$ tel que $(p-1)! \equiv -1 \ [p]$.

Donc $\exists k \in \mathbb{Z}$ tq $(p-1)! = -1 + kp$.

Soit $d \in [\![1; p-1]\!]$ tel que $d \mid p$.

On $d \in [\![1; p-1]\!]$ donc $d \mid (p-1)!$, soit $\left.\begin{matrix} d \mid -1 + kp \\ d \mid p \end{matrix}\right\} \Rightarrow d \mid -1$, donc $d = 1$.

Donc $p \in \mathbb{P}$.

■

Exemples de nbs premiers particuliers :

* **Nombres de Fermat** : $F_n = 2^{2^n} - 1$, $n \in \mathbb{N}$.
  - ↳ $\forall n, m \in \mathbb{N}$, $n \neq m \Rightarrow F_n \wedge F_m = 1$
  - ↳ $\{F_1, \dots, F_4\} \subset \mathbb{P}$, $F_5 \notin \mathbb{P}$, …, $F_{32} \notin \mathbb{P}$, $F_{33} \overset{?}{\in} \mathbb{P}$
  - ↳ Polygones réguliers à n côtés : constructibles à la règle et au compas ssi n est de ptt d'une puiss. de 2 et d'un nb fini de nbs de Fermat premiers distincts.
* **Nombres de Mersenne** : $M_n = 2^n - 1$, $n \in \mathbb{N}$.
  - ↳ $M_n \in \mathbb{P} \Rightarrow n \in \mathbb{P}$
  - ↳ ⚠ Réciproque fausse ! ex : $11 \in \mathbb{P}$ et $M_{11} = 2047 = 23 \times 89 \notin \mathbb{P}$.

Thm des 2 carrés :

$p \in \mathbb{P}$. Les assertions suivantes sont équivalentes :

1. $\exists a, b \in \mathbb{Z}$ tels que $a^2 + b^2 = p$.
2. $p \in \mathbb{Z}[i]$ n'est pas irréductible dans $\mathbb{Z}[i]$.
3. -1 est un carré modulo p.
4. $p \equiv 1\ [4]$ ou $p \equiv 2\ [4]$.

Preuve : $2 = 1^2 + 1^2 = (1+i)(1-i)$ et $-1 \equiv 1 \equiv 1^2\ [2]$. On prend alors p impair (car 2 ok).

* (1) ⇒ (4) :

$$\left.\begin{array}{l} k \equiv 1\ [4] \Rightarrow k^2 \equiv 1\ [4] \\ k \equiv 2\ [4] \Rightarrow k^2 \equiv 0\ [4] \\ k \equiv 3\ [4] \Rightarrow k^2 \equiv 1\ [4] \\ k \equiv 0\ [4] \Rightarrow k^2 \equiv 0\ [4] \end{array}\right\} \Rightarrow p = a^2 + b^2 \equiv 1 \text{ ou } 2\ [4]$$

car $p \in \mathbb{P}$ donc $p \not\equiv 0\ [4]$.

* (4) ⇔ (3) :

Lemme : Notons $K = \{x^2 / x \in \underbrace{(\mathbb{Z}/p\mathbb{Z})^*}_{= \mathbb{F}_p^*}\}$.

Soit $p \in \mathbb{P} \setminus \{2\}$. Alors :

$$-1 \in K \iff p \equiv 1\ [4]$$

Preuve du lemme :

Soit $\varphi : (\mathbb{F}_p^*, \cdot) \longrightarrow (\mathbb{F}_p^*, \cdot)$, $x \longmapsto x^2$.

→ C'est un morphisme et $\mathrm{Im}(\varphi) = K$.

→ $\ker \varphi = \{x \in \mathbb{F}_p^* \mid x^2 = 1\} = \{-1; +1\}$

De plus, $\ker\varphi$ est un sous-groupe commutatif de $\mathbb{F}_p^*$, donc il est distingué.
Donc par thm d'isomorphisme on a :

$$\frac{|\mathbb{F}_p^*|}{|\ker\varphi|} = \frac{p-1}{2} = |\mathrm{Im}\,\varphi| = |K|.$$

On a donc $\boxed{x \in K \Leftrightarrow x^{\frac{p-1}{2}} = 1}$ car :
$\Rightarrow$ $x \in K \Rightarrow (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$ d'après le petit thm de Fermat
$\Leftarrow$ Le polynôme $X^{\frac{p-1}{2}} - 1$ admet au plus $\frac{p-1}{2}$ racines.
On $|K| = \frac{p-1}{2}$, donc ts les éléments de K sont racine de $X^{\frac{p-1}{2}} - 1$.

→ Finalement :

$$\begin{aligned} -1 \in K &\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow \frac{p-1}{2} \equiv 0\ [2] \\ &\Leftrightarrow p \equiv 1\ [4]. \end{aligned}$$

On a ainsi bien ④ ⇔ ③.

* ③ ⇒ ② :
③ $\Rightarrow \exists x \in \mathbb{N}^*$ tq $-1 \equiv x^2\ [p]$.
$\Rightarrow p \mid x^2+1$ et p est réductible dans $\mathbb{Z}[i]$ car :
Supposons p irréductible dans $\mathbb{Z}[i]$. Comme c'est un anneau principal, alors p est premier dans $\mathbb{Z}[i]$.
On $p \mid x^2+1 \Rightarrow p \mid (x+i)(x-i)$
$\Rightarrow p \mid x+i$ ou $p \mid x-i$ dans $\mathbb{Z}[i]$
En passant dans $\mathbb{Z}$, on a alors $\begin{cases} p \mid x \\ p \mid 1. \end{cases}$
$\Rightarrow x \wedge 1 \neq 1$, donc x et 1 ne sont pas premiers entre eux, ce qui est absurde.
↳ parce que 1...

* ② ⇒ ① :
Soit $p = xy$ avec $x, y \in \mathbb{Z}[i]$ non inversibles.
$\Rightarrow x, y \notin \mathbb{Z}[i]^\times$.
$\varphi(p) = p^2 = \varphi(x)\varphi(y) \Rightarrow \varphi(x) = \varphi(y) = p$.
↑ φ morph.

Prenons $x = a+ib$, alors $p = \varphi(x) = a^2+b^2$. ∎

Thm:

Il existe une infinité de nbs premiers de la forme $4n-1$ (ou $6n-1$), $n \in \mathbb{N}^*$.

Preuve:

Posons $P_{(4,-1)} = \{4n-1 \text{ premiers} \mid n \in \mathbb{N}\}$.

Supposons $P_{(4,-1)}$ fini, donc

$P_{(4,-1)} = \{p_1, \dots, p_r\}$, $r \in \mathbb{N}^*$ (car $3 \in P_{(4,-1)}$).

Un nombre impair est toujours congru à 1 ou -1 [4].

Posons $m = 4p_1p_2 \cdots p_r - 1 \equiv -1$ [4] et non premier.

Soit $j \in [\![1; r]\!]$ tel que $p_j \mid m$

Alors $p_j \mid 4p_1p_2 \cdots p_j \cdots p_r$

Donc $p_j \mid -1$, ce qui est absurde. ∎

Chiffrement R.S.A:

(Rivest, Shamir, Adleman - 1977).

$p, q \in \mathbb{P}$ distincts et $n = pq$.

Si $\exists e, d \in \mathbb{Z}$ tq $ed \equiv 1 [\varphi(n)]$

Alors:

$\forall m \in \mathbb{Z}$, $m^{ed} \equiv m [n]$.

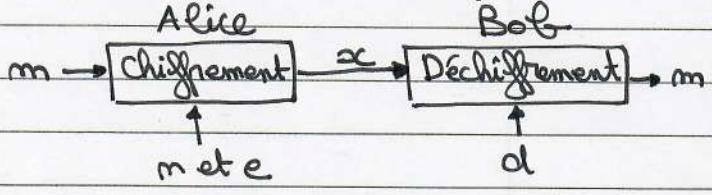
Rmq: φ est l'indicatrice d'Euler.
Dans ce cas, $\varphi(n) = (p-1)(q-1)$.
Toute la solidité repose sur la difficulté à calculer $\varphi(n)$.

Exemple:

m = message

d = clé privée (de Bob)

n et e = clé publique



Prenons $n = 5 \times 17 = 85$, $e = 5$ et $d = 13$

Alice chiffre par exemple le message $m = 10$ en faisant $x = m^e [n] = 10^5 [85] = 40 [85]$.

Bob déchiffre en faisant $x^d [n] = m^{ed} [n] = m [n]$

soit $40^{13} [85] = 10 [85]$.