

STRUCTURES DISCRETES

Math 030

Cours de Mr. Jean Doyen

2001 – Vanderick Jonathan

2002 – Louwers Fabian

2003 – Gigo

CHAPITRE I : Problèmes de dénombrement

But : Pouvoir répondre à des questions compliquées, telles que « Combien y a-t-il de ... ? »

1. Coefficients binomiaux

1.1 Définition:

$\binom{n}{k}$ = le nombre de sous-ensembles de cardinal k dans un ensemble fini de cardinal n . On suppose k et n entiers avec $0 \leq k \leq n$.

1.2 Cas limites:

$$\binom{n}{0} = 1 \text{ et } \binom{n}{n} = 1$$

1.3 Propriétés:

Symétrie: $\binom{n}{k} = \binom{n}{n-k}$

Démonstration :

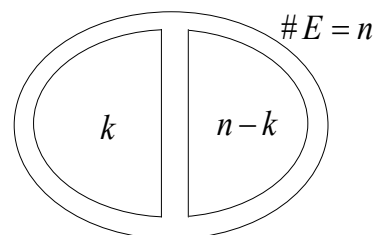
Soit E un ensemble de cardinal n . A tout sous-ensemble S de cardinal k correspond son complément \bar{S} , de cardinal $n-k$.

Si on appelle $P_k(E)$, l'ensemble de cardinal k dans E , la correspondance

$$S \leftrightarrow \bar{S}$$

est une bijection

$$\begin{aligned} P_k(E) &\rightarrow P_{n-k}(E) \\ \Rightarrow |P_k(E)| &= |P_{n-k}(E)| \\ \parallel &\quad \parallel \\ \binom{n}{k} &= \binom{n}{n-k} \end{aligned}$$



□

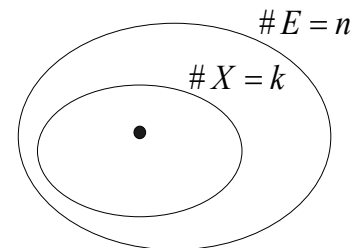
Réurrence multiplicative : $\boxed{\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1} \text{ où } 0 < k \leq n}$

Démonstration :

Soit E un ensemble de cardinal n .

Comptons de deux manières différentes le nombre de couples (x, X) où $x \in X \subseteq E$ et $|X| = k$.

$$\begin{array}{ccccc} \binom{n}{k} & * & k & = & n & * & \binom{n-1}{k-1} \\ \parallel & & \parallel & & \parallel & & \\ \text{nombre de} & & \text{nombre de} & & \text{nombre de} & & \\ \text{choix de} & & x \text{ dans un} & & \text{choix de} & & \\ X \text{ dans } E & & \text{tel } X & & x \text{ dans } E & & \end{array}$$



$$\Rightarrow \binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$$

□

Corollaire :

$$\begin{aligned} \binom{n}{k} &= \frac{n}{k} * \binom{n-1}{k-1} \\ &= \frac{n}{k} * \frac{n-1}{k-1} * \binom{n-2}{k-2} \\ &= \dots \\ &= \frac{n}{k} * \frac{n-1}{k-1} * \dots * \frac{n-k+1}{1} \end{aligned}$$

$$\boxed{\binom{n}{k} = \frac{n * (n-1) * (n-2) * \dots * (n-k+1)}{k!}}$$

Ou encore

$$\boxed{\binom{n}{k} = \frac{n!}{(n-k)!k!}}$$

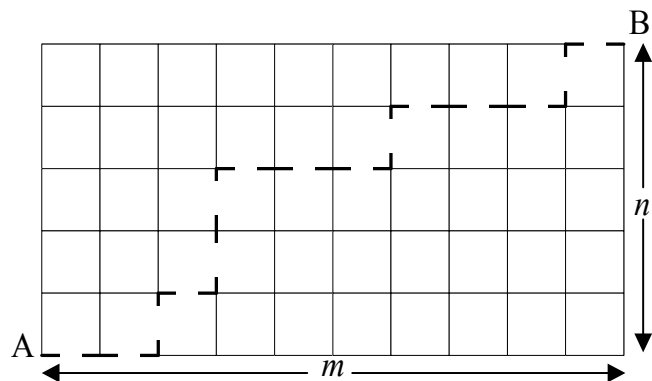
La formule reste valable pour $0 \leq k \leq n$, à condition de poser $0! = 1$. Il vient

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = 1$$

1.4 Quelques exemples :

1) Chemins minimaux dans un quadrillage $m \times n$

Quadrillage $m \times n$ formé de mn carrés 1×1 .



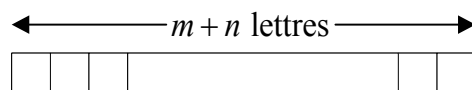
Combien y a-t-il de chemins de longueur minimale ($= m + n$) reliant les deux sommets opposés A et B du quadrillage ?

— \rightarrow : déplacement horizontal de une case vers la droite

\uparrow : déplacement vertical de une case vers le haut
|

Tout chemin minimal de A à B peut-être décrit univoquement par un mot de $m + n$ lettres formé de m lettres H et de n lettres V.

\Rightarrow Nombres de chemins minimaux de A à B
= nombre de tels mots



$= \binom{m+n}{m}$ = nombre de manières de choisir, parmi les $m + n$ cases, les m cases où l'on écrira un H.

$= \binom{m+n}{n}$ = V. (par symétrie)

Remarque : $\binom{m+n}{m} = \binom{m+n}{(m+n)-m} = \binom{m+n}{n}$

2) Solutions entières de certaines équations linéaires

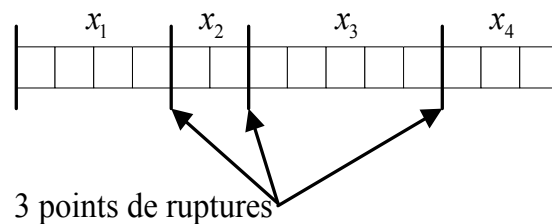
Combien l'équation

$$x_1 + x_2 + x_3 + x_4 = 14$$

possède-t-elle de solutions (x_1, x_2, x_3, x_4) en entier $x_i > 0$?

Exemples : (1, 1, 1, 11), (1, 11, 1, 1), (4, 2, 5, 3)...

Géométrisons le problème :



Nombre de solutions en entiers $x_i > 0$

= nombre de manières de choisir, parmi les 13 points de ruptures possibles, 3 points donnant naissance à 4 nouveaux morceaux de longueur x_1, x_2, x_3, x_4 entiers > 0 .

$$\text{Nombres de solutions} = \binom{13}{3} = \frac{13 \cdot 12 \cdot 11}{3 \cdot 2} = 286$$

Généralisation :

Nombre de solutions $(x_1, x_2, x_3, \dots, x_t)$ de l'équation

$$x_1 + x_2 + x_3 + \dots + x_t = u \quad (u \in \mathbb{N}^0)$$

en entiers $x_i > 0$?

$u - 1$ points de ruptures possibles et $t - 1$ points à choisir

$$\Rightarrow \text{nombre de solutions} = \binom{u-1}{t-1}$$

Variante :

Nombre de solutions $(x_1, x_2, x_3, \dots, x_t)$ de l'équation

$$x_1 + x_2 + x_3 + \dots + x_t = u \quad (u \in \mathbb{N}^0)$$

en entiers $x_i \geq 0$?

Astuce : on effectue un changement de variable :
posons

$$x'_i = x_i + 1 \quad (x'_i \in \mathbb{N}^0 \quad (\forall i = 1, 2, \dots, t))$$

Or

$$x_i = x'_i - 1 \quad (\forall i = 1, 2, \dots, t)$$

l'équation de départ s'écrit

$$\begin{aligned} x'_1 - 1 + x'_2 - 1 + \dots + x'_t - 1 &= u \\ \Rightarrow x'_1 + x'_2 + \dots + x'_t &= t + u \end{aligned}$$

avec des $x'_i \in \mathbb{N}^0$

$$\Rightarrow \text{nombre de solutions} = \binom{t+u-1}{t-1} = \binom{t+u-1}{u}$$

Application :

$E_n = \{e_1, e_2, \dots, e_n\}$ un ensemble de n objets.

Vieille terminologie :

$C(n, k)$ = combinaisons sans répétition

= nombre de manières de choisir k objets parmi ces n objets
sans ordre et sans répétition

$$\begin{aligned} &= \binom{n}{k} \\ &= \frac{n(n-1)(n-2)\dots(n-k+1)}{k!} \end{aligned}$$

$C^*(n, k)$ = combinaisons avec répétitions

= nombre de manières de choisir k objets parmi ces n objets
sans ordre mais en autorisant les répétitions (on peut choisir
plusieurs fois le même objet)

Soit x_i le nombre de fois où l'objet e_i est choisi ($x_i \in \mathbb{N}$).

Il suffit de connaître les valeurs des x_i où

$$x_1 + x_2 + \dots + x_n = k$$

$$\Rightarrow C^*(n, k) = \binom{n+k-1}{k} = \frac{(n+k-1)(n+k-2)\dots(n+1)n}{k!}$$

$$C(n, k) = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}$$

$$C^*(n, k) = \frac{n(n+1)(n+2)\dots(n+k-1)}{k!}$$

3) Entiers consécutifs dans un tirage du Lotto

Problème : Quelle est la probabilité qu'un tirage du Lotto belge ne contienne pas deux entiers consécutifs ? (= probabilité qu'un sous-ensemble de cardinal 6 choisi au hasard dans l'ensemble $\{1, 2, 3, \dots, 42\}$ ne contienne pas 2 entiers consécutifs).

Théorème :

$$\begin{aligned} & \# \text{ de sous-ensembles de cardinal } k \text{ de } \{1, 2, 3, \dots, n\} \text{ ne contenant pas deux entiers} \\ & \text{ consécutifs} \\ & = \# \text{ total de sous-ensembles de cardinal } k \text{ de l'ensemble } \{1, 2, 3, \dots, n-k+1\} \\ & = \binom{n-k+1}{k}. \end{aligned}$$

Démonstration :

Étant donnés k entiers $a_1 < a_2 < a_3 < \dots < a_k$ dans $\{1, 2, 3, \dots, n-k+1\}$ (notons que $a_k \leq n-k+1$) ; alors, $\{a_1, a_2+1, a_3+2, \dots, a_k+k-1\}$ est un sous-ensemble de cardinal k de $\{1, 2, 3, \dots, n\}$, car $(a_k \leq n-k+1 \Rightarrow a_k + (k-1) \leq n)$, et de plus, par construction, ce sous-ensemble ne contient jamais deux entiers consécutifs.

Réciproquement, étant donnés k entiers $b_1 < b_2 < b_3 < \dots < b_k$ dans $\{1, 2, 3, \dots, n\}$ tels que b_i et b_{i+1} ($i=1, 2, \dots, k$) ne soient jamais consécutifs, alors $\{b_1, b_2-1, b_3-2, \dots, b_k-(k-1)\}$ est un sous-ensemble de cardinal k de $\{1, 2, 3, \dots, n-k+1\}$.

□

$$\text{Réponse : } \frac{\binom{42-6+1}{6}}{\binom{42}{6}} = \frac{\binom{37}{6}}{\binom{42}{6}} \approx 0,44317$$

Donc la probabilité qu'un tirage du Lotto belge contienne au moins deux entiers consécutifs $\approx 0,55682 > \frac{1}{2}$.

1.5 Réurrence additive et triangle de Pascal :

$$1) \text{ Réurrence additive : } \boxed{\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \quad \text{si } 0 < k < n}$$

Démonstration :

Soit x un élément fixé dans un ensemble E de cardinal n .

$$\begin{aligned} \binom{n}{k} &= \# \text{ de sous-ensembles de cardinal } k \text{ dans } E \\ &= \# \text{ de sous-ensembles de cardinal } k \text{ ne contenant pas } x : \binom{n-1}{k} \\ &\quad + \# \text{ de sous-ensembles de cardinal } k \text{ contenant } x : \binom{n-1}{k-1} \end{aligned}$$

$$\begin{aligned} \binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1} \\ &\quad \parallel \qquad \qquad \parallel \\ &\quad \left(\begin{array}{l} \text{nbre de ss-ens ne contenant pas } x \\ \rightarrow k \text{ éléments à choisir parmi } n-1 \\ \text{(on ne peut pas choisir } x) \end{array} \right) \quad \left(\begin{array}{l} \text{nbre de ss-ens contenant } x \\ k-1 \text{ éléments à choisir (on} \\ \text{a déjà } x) \text{ parmi } n-1 \text{(on ne} \\ \text{peut plus choisir } x) \end{array} \right) \end{aligned}$$

□

2) Triangle de « Pascal » (1653)

$$\begin{array}{ccccccc}
 & & & & n=0 \rightarrow & \begin{Bmatrix} 1 \\ 1 \end{Bmatrix} & \swarrow k=1 \\
 & & & & n=1 \rightarrow & \begin{Bmatrix} 2 \\ 1 \end{Bmatrix} & & \begin{Bmatrix} 1 \\ 1 \end{Bmatrix} \swarrow k=2 \\
 & & & & n=2 \rightarrow & \begin{Bmatrix} 3 \\ 1 \end{Bmatrix} & & \begin{Bmatrix} 3 \\ 2 \end{Bmatrix} & & \begin{Bmatrix} 3 \\ 3 \end{Bmatrix} \swarrow k=3 \\
 & & \dots & & \dots & & \dots & & \dots & & \dots \\
 & & & & & \begin{Bmatrix} n \\ k-1 \end{Bmatrix} & & \begin{Bmatrix} n \\ k \end{Bmatrix} & & & & \\
 & & & & & \searrow \downarrow \swarrow & & & & & \\
 & & & & & \begin{Bmatrix} n+1 \\ k \end{Bmatrix} & & & & & &
 \end{array}$$

← symétrie →

$$\begin{array}{cccccccc}
 & & & & 1 & & & & \\
 & & & & 1 & & 1 & & \\
 & & & & 1 & & 2 & & 1 & & \\
 & & & & 1 & & 3 & & 3 & & 1 & \\
 & & & & 1 & & 4 & & 6 & & 4 & & 1 & \\
 & & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
 & \dots & & \dots & \dots & & \dots & & \dots & & \dots & & \dots & & \dots &
 \end{array}$$

$$\binom{n}{k} = \binom{n}{n-k}$$

Extension du triangle de Pascal :

...	0	0	0	1	0	0	0	0	...
...	0	0	0	1	1	0	0	0	...
...	0	0	1	2	1	0	0	0	...
...	0	0	1	3	3	1	0	0	...
...	0	1	4	6	4	1	0	0	...
...

⇒ Demi-plan de Pascal

Ceci conduit à une extension de la définition des coefficients binomiaux :

$$\binom{n}{k} = 0 \quad \text{si} \quad \begin{cases} k < 0 \\ \text{ou} \\ k > n \end{cases}$$

alors la récurrence additive $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ est vraie $\forall k \in \mathbb{Z}$.

3) i) $\boxed{\sum_{k=0}^n \binom{n}{k} = 2^n}$

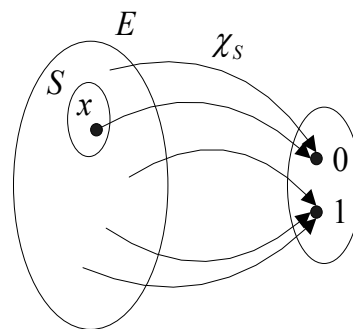
que l'on peut encore écrire $\sum_{k=-\infty}^{+\infty} \binom{n}{k} = 2^n$ ou encore $\sum_k \binom{n}{k} = 2^n$.

Démonstration :

$\sum_{k=0}^n \binom{n}{k} = \#$ total de sous-ensembles d'un ensemble E de cardinal n .

Chaque sous-ensemble S de E est univoquement déterminé par sa fonction caractéristique

$$\chi_S(x) = \begin{cases} 1 & \text{si } x \in S \\ 0 & \text{si } x \notin S \end{cases}$$



Le nombre de sous-ensemble de E est donc égal au nombre de fonctions $\chi_S : E \rightarrow \{0, 1\}$.

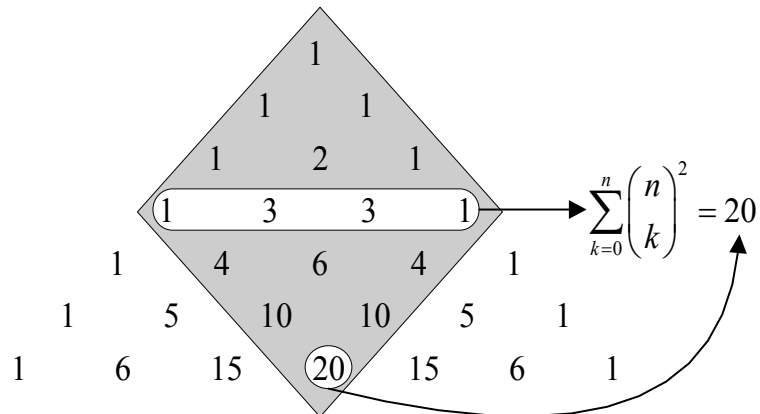
Pour chacun des n éléments x de E , il y a 2 choix possibles pour $\chi_S(x)$: 0 ou 1.

Donc en tout $\underbrace{2 * 2 * \dots * 2}_{n \text{ facteurs}} = 2^n$.

Fonction caractéristique $\Rightarrow 2^n$ sous-ensembles

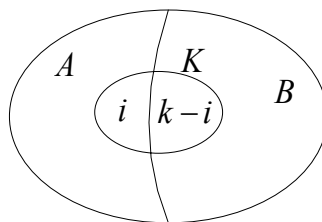
□

$$\text{ii) } \boxed{\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}}$$



Démonstration :

$$|A| = a \quad |B| = b \quad |K| = k$$



K est un sous-ensemble de $A \cup B$.

Comptons de deux manières différentes le nombre de sous-ensembles K de cardinal k de $A \cup B$.

Première manière : $\binom{a+b}{k}$

Seconde manière : $\sum_{i=0}^k \binom{a}{i} \binom{b}{k-i}$ (i fixé)

↓
car K est peut-être "tiré"
plus dans A ou dans B

$$\Rightarrow \boxed{\sum_{i=0}^k \binom{a}{i} \binom{b}{k-i} = \binom{a+b}{k}}$$

Cas particulier : $a = b = k = n$

$$\begin{aligned} \Rightarrow \sum_{i=0}^n \binom{n}{i} \binom{n}{n-i} &= \binom{n+n}{n} \\ &= \binom{n}{i} \text{ par symétrie} \\ \Rightarrow \sum_{i=0}^n \binom{n}{i}^2 &= \binom{2n}{n} \end{aligned}$$

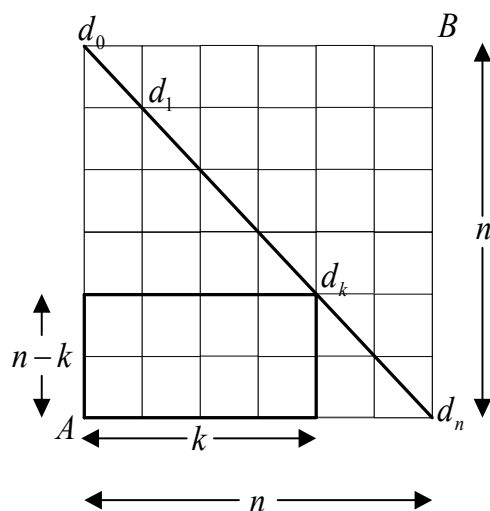
□

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} &= 2^n \\ \sum_{k=0}^n \binom{n}{k}^2 &= \binom{2n}{n} \end{aligned}$$

Problème non résolu :

$$\sum_{k=0}^n \binom{n}{k}^3 = ?$$

1.6 Problème de Roméo et Juliette



$d_0, d_1, d_2, \dots, d_n$ = points diagonaux du quadrillage $n \times n$.

A l'instant $t = 0$, Roméo est en A et Juliette en B . Ils se dirigent l'un vers l'autre à la même vitesse. S'ils se rencontrent, ce sera donc nécessairement en un des $n+1$ points diagonaux $d_0, d_1, d_2, \dots, d_n$.

Roméo choisit au hasard un des chemins minimaux de A à un des points de la diagonale. Juliette choisit indépendamment un chemin minimum de B à un des points de la diagonale.

Quelle est la probabilité d'une rencontre ?

$$p(\text{rencontre}) = p(\text{rencontre en } d_0 \text{ ou } d_1 \text{ ou } \dots \text{ ou } d_n)$$

$$= \sum_{k=0}^n p(\text{rencontre en } d_k)$$

$$p(\text{rencontre en } d_k) = p(\text{R se trouve en } d_k \text{ après } n \text{ étapes et J se trouve en } d_k \text{ après } n \text{ étapes})$$

$$= p(\text{R se trouve en } d_k \text{ après } n \text{ étapes}) * p(\text{J se trouve en } d_k \text{ après } n \text{ étapes})$$

$$= \frac{\overbrace{\binom{n}{k}}^{\text{chemins favorables}}}{\underbrace{\sum_{k=0}^n \binom{n}{k}}_{\text{chemins possibles menant en } n \text{ étapes à un point de la diagonale}}} * \frac{\binom{n}{k}}{\sum_{k=0}^n \binom{n}{k}}$$

chemins possibles menant en n étapes à un point de la diagonale

$$= \frac{\binom{n}{k}}{2^n} * \frac{\binom{n}{k}}{2^n}$$

$$= \frac{1}{2^{2n}} \binom{n}{k}^2$$

$$= \frac{1}{4^n} \binom{n}{k}^2$$

$$\Rightarrow p(\text{rencontre}) = \sum_{k=0}^n \frac{1}{4^n} \binom{n}{k}^2$$

$$= \frac{1}{4^n} \underbrace{\sum_{k=0}^n \binom{n}{k}^2}_{= \binom{2n}{n}}$$

$$= \frac{1}{4^n} \binom{2n}{n}$$

Remarque : on verra que $\binom{2n}{n} \sim \frac{4^n}{\sqrt{\pi n}}$

$$\Rightarrow p(\text{rencontre}) \sim \frac{1}{4^n} \frac{4^n}{\sqrt{\pi n}} = \frac{1}{\sqrt{\pi n}}$$

1.7 Formule dite « du binôme de Newton »

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \quad \forall x, y \in \mathbb{C}, n \in \mathbb{N}_0$$

(origine du terme coefficients binomiaux)

$$\begin{aligned} (x+y)^n &= \overbrace{(x+y)(x+y)(x+y)\dots(x+y)}^{n \text{ facteurs}} \\ &= \sum_{k=0}^n \boxed{?} x^k y^{n-k} \end{aligned}$$

Le coefficient du terme en $x^k y^{n-k} = \#$ de manières de choisir parmi les n facteurs du produit les k facteurs où l'on prendra un x (les $n-k$ autres donneront un y), c'est-à-dire

$$\binom{n}{k}.$$

Applications :

1) Nombre total de sous-ensembles d'un ensemble de cardinal n

$$\sum_{k=0}^n \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n$$

$$\boxed{\sum_{k=0}^n \binom{n}{k} = 2^n}$$

$$2) \quad \sum_{k=0}^n (-1)^k \binom{n}{k} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \dots + (-1)^n \binom{n}{n}$$

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} (-1)^k (1)^{n-k} = (-1+1)^n = 0$$

$$\boxed{\sum_{k=0}^n (-1)^k \binom{n}{k} = 0}$$

$$3) \quad \binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \dots = ?$$

Astuce :

$$\begin{aligned}
 (1+i)^n &= \binom{n}{0} + i \binom{n}{1} + i^2 \binom{n}{2} + i^3 \binom{n}{3} + i^4 \binom{n}{4} + i^5 \binom{n}{5} + \dots \\
 &= \underbrace{\left(\binom{n}{0} + i \binom{n}{1} - \binom{n}{2} - i \binom{n}{3} \right)}_{\text{Période}} + \underbrace{\left(\binom{n}{4} + i \binom{n}{5} - \binom{n}{6} - i \binom{n}{7} \right)}_{\text{Période}} + \dots \\
 &= \left[\sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) \right]^n \\
 &= 2^{\frac{n}{2}} \left(\cos \frac{n\pi}{4} + i \sin \frac{n\pi}{4} \right) \\
 &= 2^{\frac{n}{2}} \cos \frac{n\pi}{4} + i 2^{\frac{n}{2}} \sin \frac{n\pi}{4}
 \end{aligned}$$

$$\begin{aligned}
 \Rightarrow \binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \dots &= 2^{\frac{n}{2}} \cos \frac{n\pi}{4} \\
 \binom{n}{1} - \binom{n}{3} + \binom{n}{5} - \binom{n}{7} + \dots &= 2^{\frac{n}{2}} \sin \frac{n\pi}{4}
 \end{aligned}$$

Remarque :

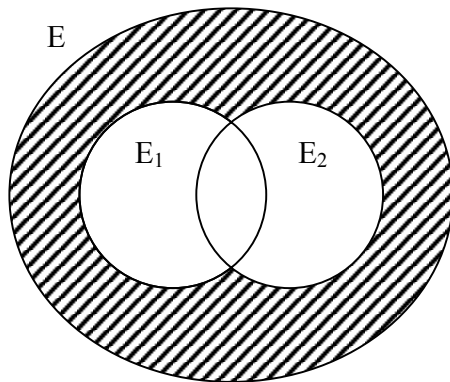
Newton, à 23 ans, a généralisé la formule aux cas des exposants quelconques (non-nécessairement positifs et non nécessairement entiers) :

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k \quad \text{où} \quad \binom{\alpha}{k} = \frac{\alpha * (\alpha-1) * (\alpha-2) * \dots * (\alpha-k+1)}{k!}$$

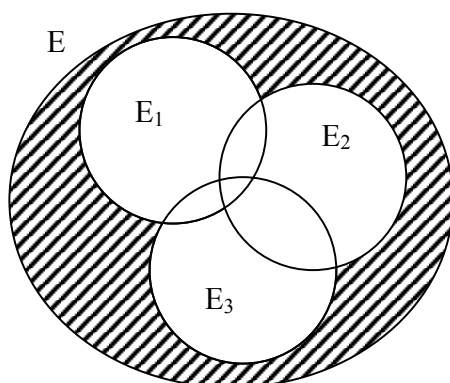
Formule de la série du binôme qui converge pour $-1 < x < 1$.

2. Formule d'inclusion – exclusion.

2.1 Introduction.



$$\begin{aligned} |\overline{E_1 \cup E_2}| &= \text{Le complément du cardinal de la réunion.} \\ &= |E| - (|E_1| + |E_2|) + (|E_1 \cap E_2|) \\ &= \text{Partie hachurée.} \end{aligned}$$



$$|\overline{E_1 \cup E_2 \cup E_3}| = |E| - (|E_1| + |E_2| + |E_3|) + (|E_1 \cap E_2| + |E_1 \cap E_3| + |E_2 \cap E_3|) - (|E_1 \cap E_2 \cap E_3|)$$

2.2 Théorème.

Si $E_1, E_2, E_3, \dots, E_n$ sont des sous ensembles d'un ensemble **fini** E , alors :

$$\begin{aligned} |\overline{E_1 \cup E_2 \cup E_3 \cup \dots \cup E_n}| &= |E| - \sum_i |E_i| + \sum_{i_1 < i_2} |E_{i_1} \cap E_{i_2}| - \sum_{i_1 < i_2 < i_3} |E_{i_1} \cap E_{i_2} \cap E_{i_3}| \\ &+ \dots + (-1)^k \sum_{i_1 < i_2 < \dots < i_k} |E_{i_1} \cap E_{i_2} \cap \dots \cap E_{i_k}| \\ &+ \dots + (-1)^n \sum_{i_1 < i_2 < \dots < i_n} |E_{i_1} \cap E_{i_2} \cap \dots \cap E_{i_n}| \end{aligned}$$

2.3 Démonstration.

Si $x \in E$ n'appartient à aucun des E_i , il est compté une fois dans le membre de gauche (partie hachurée) et une fois dans le membre de droite ($|E|$) dans les autres il n'est jamais compté car il ne fait pas partie des E_i .

Si $x \in E$ appartient à **exactement** k des E_i (avec $1 \leq k \leq n$), alors il est compté :

0 fois dans le membre de gauche et combien de fois dans le membre de droite ?

$\Rightarrow +1$ fois dans le terme $|E|$

- k fois dans le terme $\sum_i |E_i|$

+ $\binom{k}{2}$ fois dans le terme $\sum_{i_1 < i_2} |E_{i_1} \cap E_{i_2}|$

- $\binom{k}{3}$ fois dans le terme $\sum_{i_1 < i_2 < i_3} |E_{i_1} \cap E_{i_2} \cap E_{i_3}|$

⋮

+ $(-1)^k \binom{k}{k} = (-1)^k 1$ ce qui est logique car il n'est compté qu'une et une seule fois dans

les k ensembles qui le contiennent.

\Rightarrow donc en tout x est compté $1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \dots + (-1)^k \binom{k}{k}$ fois dans le membre de droite

Or $1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \dots + (-1)^k \binom{k}{k}$

= $(1-1)^k$ (cf Binôme de Newton)

= **0**

□

2.4 Applications.

2.4.1 Dérangement de n objets.

Si $A = \{a_1, a_2, \dots, a_n\}$ est un ensemble de n objets, on appelle **dérangement** de ces objets toute permutation des n objets qui n'en laisse aucun en place (= permutation sans point fixe).

Question : Parmi les $n!$ permutations possibles des n objets, combien sont des dérangements ?

Notations :

E_n = ensemble des $n!$ permutations des n objets

E_1 = ensemble des permutations fixant l'objet a_1

E_2 = ensemble des permutations fixant l'objet a_2

...

Solution du problème :

$$D_n = |\overline{E_1 \cup E_2 \cup E_3 \cup \dots \cup E_n}|$$

$$\begin{aligned}
&= |E| - n|E_1| + \underbrace{\binom{n}{2}}_{\substack{\text{car il y a } \binom{n}{2} \\ \text{sous-ensembles} \\ E_1 \cap E_2}} |E_1 \cap E_2| + \dots + (-1)^k \binom{n}{k} |E_1 \cap E_2 \cap \dots \cap E_k| + \dots + (-1)^n \binom{n}{n} |E_1 \cap E_2 \cap \dots \cap E_n| \\
&= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! + \dots + (-1)^k \binom{n}{k}(n-k)! + \dots + (-1)^n \binom{n}{n}(n-n)!
\end{aligned}$$

$$\text{Or } \boxed{\binom{n}{i}(n-i)! = \frac{n!}{i!(n-i)!}(n-i)! = \frac{n!}{i!}}$$

$$\begin{aligned}
D_n &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \dots + (-1)^k \frac{n!}{k!} + \dots + (-1)^n \frac{n!}{n!} \\
&= n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^k \frac{1}{k!} + \dots + (-1)^n \frac{1}{n!} \right)
\end{aligned}$$

On sait que pour tout x :

$$e^x = \frac{1}{1} + \frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots + \frac{x^n}{n!}$$

si $x = -1$

$$e^{-1} = \frac{1}{1} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!}$$

$$\frac{1}{n!} \approx \frac{1}{e} 10^{-7}$$

Donc :

$$\boxed{D_n \approx \frac{n!}{e}} \quad \text{Si } n \text{ est suffisamment grand.}$$

$$D_n \approx \left\lfloor \frac{n!}{e} \right\rfloor \quad \text{où } \lfloor x \rfloor \text{ est l'entier le plus proche de } x.$$

$$D_n = n! \underbrace{\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^k \frac{1}{k!} + \dots + (-1)^n \frac{1}{n!} \right)}_{\text{Série alternée décroissante}}$$

Rappel :

Une série alternée décroissante est une série du type :

$$\sum_{k=0}^{\infty} (-1)^k a_k = a_0 - a_1 + a_2 - a_3 + \dots$$

où les nombres réels a_k sont tels que :

$$a_0 \geq a_1 \geq a_2 \geq \dots \geq 0 \text{ et } \lim_{k \rightarrow \infty} a_k = 0$$

On démontre que :

- Toute série alternée décroissant converge
- Si $\alpha = \sum_{k=0}^{\infty} (-1)^k a_k$ est la somme de cette série, alors :

$$|\alpha - (a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n)| < a_{n+1}$$

Càd que la valeur absolue de l'erreur commise en tronquant la série est plus petite que le α et terme négligé (a_{n+1})

$$\Rightarrow \left| \frac{1}{e} - \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right) \right| < \frac{1}{(n+1)!}$$

$$\left| \frac{n!}{e} - D_n \right| < \frac{n!}{(n+1)!} = \frac{1}{\underbrace{n+1}_{\substack{\text{(car } n \text{ est au} \\ \text{min} = 1)}}} \leq \frac{1}{2}$$

$$\Rightarrow \left| D_n - \frac{n!}{e} \right| < \frac{1}{2} \quad \forall n \geq 1$$

$$\Rightarrow \text{Donc } D_n \text{ est bien l'entier le plus proche de } \frac{n!}{e}.$$

$$\text{Rmq : } \frac{1}{e} \approx 0,367$$

Donc si n est grand, il y a 36,7% de permutations de n objets qui ne fixent aucun objets.

Applications :

Si la secrétaire met les lettres dans les enveloppes au hasard, quelle est la probabilité qu'aucun des destinataires ne reçoivent la lettre qui lui était adressée ?

$$\text{Solution : } \frac{\overbrace{D_n}^{\substack{\text{(Aucune lettre} \\ \text{à sa place)}}}}{\underbrace{n!}_{\substack{\text{(Nombre de façons} \\ \text{de placer toutes les} \\ \text{lettres)}}}} = \frac{1}{1} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \approx \frac{1}{e} = 0,367$$

Si $n = 10$, l'erreur commise est inférieur à 10^{-7} .

2.4.2 Fonction φ d'Euler.

Soient n entier ≥ 1 .

$\varphi(n)$ = nombre d'entiers $k \in \{1, 2, \dots, n\}$ tels que $\text{pgcd}(k, n) = 1$.

Problème :

Que vaut $\varphi(n)$?

- $n=1$: $\varphi(n)=1$
- $n \geq 2$: soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ la décomposition en facteurs premiers de n .

Remarque :

Tout entier k tel que le $\text{pgcd}(k,n) > 1$ est divisible par au moins un des nombres premier p_i .

Formule :

Soit $E = \{1, 2, \dots, n\}$

$E_1 =$ nombre entiers $\in E$ divisible par p_1

$E_2 =$ nombre entiers $\in E$ divisible par p_2

\vdots

$E_r =$ nombre entiers $\in E$ divisible par p_r

$$\Rightarrow \varphi(n) = |\overline{E_1 \cup E_2 \cup \dots \cup E_r}|$$

$$\text{Or } |E| = n, |E_i| = \frac{n}{p_i}, |E_{i_1} \cap E_{i_2}| = \frac{n}{p_{i_1} p_{i_2}}$$

$$\Rightarrow \varphi(n) = n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \dots + \frac{n}{p_r}\right) + \left(\frac{n}{p_1 p_2} + \frac{n}{p_2 p_3} + \dots + \frac{n}{p_{r-1} p_r}\right) - \dots + (-1)^n \frac{n}{p_1 p_2 \dots p_r}$$

$$\Rightarrow n \left(1 - \left(\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_r}\right) + \left(\frac{1}{p_1 p_2} + \frac{1}{p_2 p_3} + \dots + \frac{1}{p_{r-1} p_r}\right) + \dots + \left((-1)^r \frac{r}{p_1 p_2 \dots p_r}\right)\right)$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

$$= n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

Si $n \geq 2$ et
 $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$

2.4.3 Applications, injections et surjection.

Soient E et K deux ensembles finis non vides.

Posons :

$$|E| = n \text{ et } |K| = k$$

Il n'est pas restrictif de supposer que :

$$K = \{1, 2, \dots, k\}$$

1. Le nombre d'applications.

Quel est le nombre d'applications : $f : E \rightarrow K$?

Comme chacun des n éléments de E doit avoir une image dans K et qu'il y a k images possibles pour chaque élément de E , il y a k^n applications $f : E \rightarrow K$.

2. Le nombre d'injections.

Quel est le nombre d'injections : $f : E \rightarrow K$?

Le premier élément de E a k images possibles dans K , le deuxième élément de E a $(k-1)$ images possibles dans K, \dots , le n ème élément de E a $(k-n+1)$ images possibles dans K .

La solution est donc :

$$k * (k-1) * \dots * (k-n+1)$$

Un cas **particulier** est le suivant :

Si $n = |E| = |K| = k$ alors pour chaque élément de E on a **une et une seule** image dans k . Mais comme les cardinaux sont les même, on a **une et une seule** « image » de K dans $E \Rightarrow$ on a donc une bijection

\Rightarrow le nombre d'injections est $n !$.

3. Le nombre de surjections.

Quel est le nombre de surjections : $f : E \rightarrow K$?

Tout élément de K doit être l'image d'au moins un élément de E .

Pour trouver la réponse nous allons utiliser la formule d'inclusion exclusion.

Soit A l'ensemble de toutes les applications de E dans K .

$$|A| = k^n$$

Soit A_i l'ensemble des applications de $f : E \rightarrow K$ telles que $i \notin f(E)$, càd que l'élément i de K ne sera jamais l'image d'un élément de E , on a donc :

$$|A_i| = (k-1)^n$$

Soit $A_{i_1} \cap A_{i_2}$ l'ensemble des applications de $f : E \rightarrow K$ qui n'ont pas d'images sur $i_1 i_2$:

$$|A_{i_1} \cap A_{i_2}| = (k-2)^n$$

Par la formule d'inclusion-exclusion on obtient :

Nombre de surjections $f : E \rightarrow K$

$$\begin{aligned}
 &= |\overline{A_1 \cup A_2 \cup \dots \cup A_k}| = k^n - \underbrace{k(k-1)^n}_{\substack{k = \text{le nombre} \\ \text{de } A_i \\ \text{les } A_i \text{ ont le même} \\ \text{cardinal} \rightarrow k(\#A_i)}} + \binom{k}{2}(k-2)^n - \binom{k}{3}(k-3)^n + \dots + (-1)^k \binom{k}{k}(k-k)^n \\
 &= \sum_{j=0}^k (-1)^j \binom{k}{j} (k-j)^n \stackrel{\substack{\equiv \\ \text{on pose :} \\ i=k-j}}{=} \sum_{i=0}^k (-1)^{k-i} \binom{k}{k-i} (i)^n \\
 &= \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} (i)^n
 \end{aligned}$$

\Rightarrow Le nombre de surjections de E sur K (si $|E|=n$ et $|K|=k$)

$$= \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} (i)^n$$

Corollaire :

Lorsque $n=k$, toute surjection de E vers K est nécessairement une bijection.

$$\Rightarrow n! = \sum_{i=0}^n (-1)^{n-i} \binom{n}{i} (i)^n$$

2.4.4 Partitions d'un ensemble.

$\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ = nombre de partitions d'un ensemble de n éléments en k classes.

La somme des partitions recouvre tout l'ensemble et les partitions sont disjointes en supposant $1 \leq k \leq n$.

Attention :

les classes ne sont pas numérotées, on ne tient donc pas compte de l'ordre dans lequel on « écrit » les classes.

Ex :

$\left\{ \begin{matrix} 4 \\ 2 \end{matrix} \right\}$ = nombre de partitions d'un ensemble de 4 éléments ayant 2 classes.

$$E = \{a, b, c, d\}$$

$$\bullet \{a, b, c\} \{d\} \quad \bullet \{a, b\} \{c, d\}$$

$$\bullet \{d, a, b\} \{c\} \quad \bullet \{a, c\} \{b, d\}$$

$$\bullet \{c, d, a\} \{b\} \quad \bullet \{a, d\} \{b, c\}$$

$$\bullet \{b, d, c\} \{a\}$$

$$\left\{ \begin{matrix} 4 \\ 2 \end{matrix} \right\} = 7$$

2.4.4.1 Les nombres de Stirling de 2^{ème} espèce.

$$\left\{ \begin{matrix} n \\ 1 \end{matrix} \right\} = 1, \left\{ \begin{matrix} n \\ n \end{matrix} \right\} = 1, \left\{ \begin{matrix} n \\ n-1 \end{matrix} \right\} = \binom{n}{2}$$

Calcul par récurrence :

$$\left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} = \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\} + k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \quad (2 \leq k \leq n)$$

Démonstration :

Soit $|E|=n+1$ et soit $x \in E$.

$$\begin{aligned} \left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} &= \text{nombre de partitions de } E \text{ en } k \text{ classes.} \\ &= \text{nombre de partitions de } E \text{ en } k \text{ classes dont l'une est le singleton } \\ &\quad \{x\} + \text{le nombre de partitions de } E \text{ en } k \text{ classes dont aucune est le} \\ &\quad \text{singleton } \{x\} \\ &= \text{si } x \text{ constitue une classe, il nous en faut encore } k-1 \text{ pour avoir les} \\ &\quad k \text{ classes : } k-1 \text{ classes parmi } n \text{ éléments (} n \text{ car on a déjà l'élément } x \text{ qui} \\ &\quad \text{constitue une classe) : } \left\{ \begin{matrix} n+1-1 \\ k-1 \end{matrix} \right\} \\ &\quad + \text{oublions } x \text{ car } x \text{ ne peut être 1 partitions, il nous faut donc construire } k \\ &\quad \text{classes parmi } n \text{ éléments : } \left\{ \begin{matrix} n \\ k \end{matrix} \right\}, \text{ il reste à placer l'élément } x \text{ dans une} \\ &\quad \text{des } k \text{ classes, on a donc } k \text{ choix .} \\ &= \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\} + k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \end{aligned}$$

□

Cette récurrence permet de construire le triangle de Stirling de 2^{ème} espèce.

$$\begin{array}{ccccccc} n=0 & \rightarrow & \left\{ \begin{matrix} 1 \\ 1 \end{matrix} \right\} & \swarrow & k=1 & & \\ & & & & & & \\ n=1 & \rightarrow & \left\{ \begin{matrix} 2 \\ 1 \end{matrix} \right\} & & & \left\{ \begin{matrix} 1 \\ 1 \end{matrix} \right\} & \swarrow & k=2 \\ & & & & & & & \\ n=2 & \rightarrow & \left\{ \begin{matrix} 3 \\ 1 \end{matrix} \right\} & & \left\{ \begin{matrix} 3 \\ 2 \end{matrix} \right\} & & \left\{ \begin{matrix} 3 \\ 3 \end{matrix} \right\} & \swarrow & k=3 \\ & & \dots & & \dots & & \dots & & \dots \\ & & & & \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\} & & \left\{ \begin{matrix} n \\ k \end{matrix} \right\} & & \\ & & & & \searrow & + & \swarrow & & \\ & & & & \left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} & & & & \end{array}$$

Calcul directe de $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$:

Toute surjection $f : E \rightarrow K = \{1, 2, \dots, k\}$ détermine une partition de E en k classes (à savoir les images réciproques des éléments de K).

Réciproquement : toute partition de E en k classes détermine $k!$ surjections $f : E \rightarrow K$ ($\#$ surjection $E \rightarrow K$) = $k! \cdot (\#$ partitions de E en k classes)

$$\Rightarrow \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \frac{1}{k!} \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} (i)^n$$

Remarque :

$B_n = n^{\text{ème}}$ nombre de Bell

= nombre total de partitions d'un ensemble de n éléments

$$= \sum_{k=1}^n \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$$

$$B_n = \sum_{k=1}^n \frac{1}{k!} \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} (i)^n$$

2.4.5 Permutation de n objets en k cycles.

Rappel :

Toute permutation d'un ensemble fini de n objets se décompose en cycles.

$$\left[\begin{matrix} n \\ k \end{matrix} \right] = \text{nombre de partitions de } n \text{ objets ayant exactement } k \text{ cycles. } (1 \leq k \leq n)$$

Exemple :

$$\left[\begin{matrix} n \\ n \end{matrix} \right] = 1 \text{ et } \left[\begin{matrix} n \\ 1 \end{matrix} \right] = (n-1)!$$

2.4.5.1 Les nombres de Stirling de 1^{ère} espèce :

Calcul par récurrence :

$$\left[\begin{matrix} n+1 \\ k \end{matrix} \right] = \left[\begin{matrix} n \\ k-1 \end{matrix} \right] + n \left[\begin{matrix} n \\ k \end{matrix} \right]$$

Démonstration :

$$|E| = n+1 \quad \text{et} \quad x \in E$$

$$\begin{bmatrix} n+1 \\ k \end{bmatrix} = \text{le nombre de permutations des } n+1 \text{ objets ayant } k \text{ cycles.}$$

= le nombre de permutations des $n+1$ objets ayant k cycles et une boucle en x

+

le nombre de permutations des $n+1$ objets ayant k cycles sans boucle en x .

$$\begin{bmatrix} n \\ k-1 \end{bmatrix} = \text{le nombre de permutations parmi les } n \text{ objets ayant } k-1 \text{ cycles}$$

= le premier terme.

En effet s'il y a déjà un cycle en x il nous reste à faire $k-1$ cycles parmi $(n+1)-1$ objets.

$$\begin{bmatrix} n \\ k \end{bmatrix} = \text{le nombre de permutations parmi les } n \text{ ayant } k \text{ cycles}$$

= le deuxième terme sans un facteur.

En effet, oublions momentanément x et on calcule le nombre de k cycles parmi les n objets. On doit maintenant rajouter x dans un cycle car il ne peut y avoir un cycle en x (et aussi car on a déjà fait les k cycles).

Imaginons les objets comme des points et un cycle comme un circuit fermé de sommets où les liens entre les sommets sont des flèches. Il ne peut y avoir qu'une flèche entrante et sortant pour chaque sommet.

Donc pour n sommets, il y a n flèches liants les sommets quelque soit le nombre de cycles.

Pour insérer x dans un cycle, il faut « casser » une flèche en 2 de façon à introduire x dans un cycle, il y a donc n choix de flèches à « casser ».

$$\begin{bmatrix} n \\ k \end{bmatrix} n = \text{le deuxième terme.}$$

□

En résumé :

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

$$\left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} = \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\} + k \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$$

$$\left[\begin{matrix} n+1 \\ k \end{matrix} \right] = \left[\begin{matrix} n \\ k-1 \end{matrix} \right] + n \left[\begin{matrix} n \\ k \end{matrix} \right]$$

Nombre de façons de placer n objets dans k boîtes :

Si aucune ne peut être vide :

Si les boîtes sont différentes :

Si les objets sont différents : $k! \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$

Si les objets sont les même : $\binom{n-1}{k-1}$

Si les boîtes sont les même :

Si les objets sont différents : $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$

Si les objets sont les même : $p_k(n)$

Si au moins une boîte peut être vide :

Si les boîtes sont différentes :

Si les objets sont différents : k^n

Si les objets sont les même : $\binom{n+k-1}{k-1}$

Si les boîtes sont les même :

Si les objets sont différents : pas de formule concise

Si les objets sont les même : $p_k(n) - p_{k-1}(n)$

3. Fonctions génératrices, nombres de Fibonacci, et nombres de Catalan

3.1 Nombres de Fibonacci

Problème : Combien y a-t-il de mots de n bits (= n -uples de 0 et 1) dans lesquels on ne trouve jamais deux « 1 » côte à côte.

Soit a_n ce nombres de mots.

$$n = 1 \quad \begin{array}{|c|} \hline 0 \\ \hline 1 \\ \hline \end{array} \quad a_1 = 2$$

$$n = 2 \quad \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array} \quad a_2 = 3$$

$$n = 3 \quad \begin{array}{|c|c|c|} \hline 0 & 0 & 0 \\ \hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline \hline 0 & 0 & 1 \\ \hline 1 & 0 & 1 \\ \hline \end{array} \quad a_3 = 5$$

a_{n+2} = nombre de mots de $n + 2$ bits terminant par 0
+ nombre de mots de $n + 2$ bits terminants par 1

$$= \# \overbrace{\begin{array}{|c|c|c|} \hline & & \\ \hline \end{array}}^{n+1} \quad (= a_{n+1})$$

$$+ \# \underbrace{\begin{array}{|c|c|c|} \hline & & \\ \hline \end{array}}_n \quad (= a_n)$$

\Rightarrow relation de récurrence : $a_{n+2} = a_{n+1} + a_n \quad \forall n \geq 1, a_1 = 2, a_2 = 3$

Analogie avec la suite des nombres de Fibonacci F_0, F_1, F_2, \dots définis par la récurrence

$$\boxed{\begin{array}{l} F_{n+2} = F_{n+1} + F_n \quad \forall n \geq 0, \\ F_0 = 0, F_1 = 1 \end{array}}$$

On en déduit que $a_n = F_{n+2}, \forall n \geq 1$. Le problème est donc déplacé : que vaut F_n ?

⇒ Construire la série formelle (idée de Nicolas de Bernouilli et Abraham de Moivre, début du XVIII^{ème} siècle) :

$$F_0 + F_1x + F_2x^2 + F_3x^3 + \dots + F_{n+2}x^{n+2} + \dots$$

$f(x) = \sum_{n=0}^{\infty} F_n x^n$ est la fonction génératrice de la suite $F_0, F_1, F_2, \dots, F_{n+2}, \dots$

(n'est définie que pour les valeurs de x pour lesquelles la série converge).

$$f(x) = \underbrace{0}_{F_0} + \underbrace{x}_{F_1} + \underbrace{F_1}_{F_2=F_1} x^2 + (F_1 + F_2)x^3 + (F_2 + F_3)x^4 + \dots + (F_n + F_{n+1})x^{n+2} + \dots$$

$$= x + x(F_1x + F_2x^2 + F_3x^3 + \dots + F_{n+1}x^{n+1} + \dots)$$

$$+ x^2(F_1x + F_2x^2 + F_3x^3 + \dots + F_{n+1}x^{n+1} + \dots)$$

$$= x + x * f(x) + x^2 * f(x)$$

$$\Leftrightarrow f(x)(1 - x - x^2) = x$$

$$\Rightarrow f(x) = \frac{x}{1 - x - x^2}$$

En développant $f(x)$ en série de MacLaurin, on trouve la valeur de F_n comme coefficient de x^n :

$$\overbrace{\frac{x}{1 - x - x^2}}^{\text{fonction rationnelle}} = \frac{x}{(1 - \alpha x)(1 - \beta x)}$$

$$= \frac{x}{1 - (\alpha + \beta)x + \alpha\beta x^2} \quad \begin{cases} \alpha + \beta = 1 & \alpha = \frac{1 + \sqrt{5}}{2} = 1,618\dots \\ \alpha\beta = -1 & \beta = \frac{1 - \sqrt{5}}{2} = -0,618\dots \end{cases}$$

$$\Rightarrow \alpha > |\beta| \text{ et } \alpha - \beta = \sqrt{5}$$

$$f(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \alpha x)(1 - \beta x)} = \frac{x}{\sqrt{5}} \left(\alpha \frac{1}{1 - \alpha x} - \beta \frac{1}{1 - \beta x} \right)$$

$$\left| \text{Rappel : } \frac{1}{1 - u} = \sum_{n=0}^{\infty} u^n \text{ qui converge lorsque } |u| < 1 \right.$$

$$\begin{aligned} \Rightarrow f(x) &= \frac{x}{\sqrt{5}} \left(\underbrace{\alpha \sum_{n=0}^{\infty} \alpha^n x^n}_{\substack{\text{converge pour} \\ |\alpha x| < 1 \Rightarrow |x| < \frac{1}{\alpha}}} - \underbrace{\beta \sum_{n=0}^{\infty} \beta^n x^n}_{\substack{\text{converge pour} \\ |\beta x| < 1 \Rightarrow |x| < \frac{1}{|\beta|} \\ \text{car } \beta < 0}} \right) \\ &\quad \text{converge pour } |x| < \frac{1}{\alpha} = -\beta \text{ car } \alpha > |\beta| \Rightarrow \frac{1}{\alpha} < \frac{1}{|\beta|} \\ &= \frac{1}{\sqrt{5}} \left(\sum_{n=0}^{\infty} \alpha^{n+1} x^{n+1} - \sum_{n=0}^{\infty} \beta^{n+1} x^{n+1} \right) \\ &= \sum_{n=0}^{\infty} \underbrace{\frac{1}{\sqrt{5}} (\alpha^{n+1} - \beta^{n+1})}_{=F_{n+1}} x^{n+1} \end{aligned}$$

Tous les calculs faits ont un sens lorsque $|x| < -\beta = 0,618\dots$

$$\Rightarrow F_n = \frac{1}{\sqrt{5}} (\alpha^n - \beta^n)$$

Formule de Binet (déjà connue de Bernouilli, de Moivre et Euler) :

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) \quad \forall n \geq 0$$

$$\text{Rem : } \left| \frac{1-\sqrt{5}}{2} \right| < 1 \Rightarrow \left| \frac{1-\sqrt{5}}{2} \right|^n < 1 \quad \forall n \geq 1$$

$$\text{Or } \sqrt{5} > 2 \Rightarrow \frac{1}{\sqrt{5}} \left| \frac{1-\sqrt{5}}{2} \right|^n < \frac{1}{2}, \quad \forall n \geq 1 \text{ et même } \forall n \geq 0$$

$$\underbrace{F_n}_{\text{entier}} = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \underbrace{\frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n}_{< \frac{1}{2} \text{ en valeur absolue}}$$

\Rightarrow sur la droite réelle, la distance entre l'entier F_n et le nombre réel $\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n$ est $< \frac{1}{2}$ dès que $n \geq 1$.

Conclusion :

F_n est l'entier le plus proche de $\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n \forall n \geq 1$ car la distance de F_n à ce nombre réel est toujours $< \frac{1}{2}$.

On pose $\varphi = \left(\frac{1+\sqrt{5}}{2} \right)$ (nombre d'or – golden ratio) :

$$F_n = \left\lfloor \frac{\varphi^n}{\sqrt{5}} \right\rfloor \quad \forall n \geq 0$$

En fait, si n pair $\Rightarrow F_n = \left\lfloor \frac{\varphi^n}{\sqrt{5}} \right\rfloor$, si n impair $\Rightarrow F_n = \left\lceil \frac{\varphi^n}{\sqrt{5}} \right\rceil$.

F_n a un comportement exponentiel en base φ au facteur $\frac{1}{\sqrt{5}}$ près.

3.2 Nombres de Catalan

Motivation :

La multiplication matricielle est associative, mais point de vue algorithmique, la manière de parenthéser un produit de matrices $M_1 \times M_2 \times M_3 \times \dots \times M_n = M$ peut avoir un effet non-négligeable sur le nombre total d'opérations à effectuer. En général on essaye de minimiser le nombre de multiplications de coefficients.

Avec l'algorithme classique de multiplication matricielle :

$$\begin{array}{c}
 \left. \begin{array}{c} p \times q \\ \left(\left(\right) \right) \\ \underbrace{\hspace{2cm}} \\ q \end{array} \right\} p \\
 * \\
 \left. \begin{array}{c} q \times r \\ \left(\left(\right) \right) \\ \underbrace{\hspace{2cm}} \\ r \end{array} \right\} q \\
 = \\
 \left. \begin{array}{c} p \times r \\ \left(\left(\right) \right) \\ \underbrace{\hspace{2cm}} \\ r \end{array} \right\} p
 \end{array}$$

chacun des $p \cdot q$ coefficients de la matrice de gauche est multiplié par r coefficients de la matrice de droite

$\Rightarrow p \cdot q \cdot r$ multiplications de coefficients

Exemple : $M_1 \times M_2 \times M_3 \times M_4$
 $\quad \quad \quad [10 \times 20] \quad [20 \times 50] \quad [50 \times 1] \quad [1 \times 100]$

Si on calcule le produit dans l'ordre :

- $(M_1 \times (M_2 \times (M_3 \times M_4)))$ il faudra faire $5\,000 + 100\,000 + 20\,000 = 125\,000$ multiplications.

- $((M_1 \times M_2) \times (M_3 \times M_4))$ il faudra faire $10\,000 + 5\,000 + 50\,000 = 65\,000$ multiplications.

- $((M_1 \times (M_2 \times M_3)) \times M_4)$ il faudra faire $1\,000 + 200 + 1\,000 = 2\,200$ multiplications.

- $(M_1 \times ((M_2 \times M_3) \times M_4))$ il faudra faire $1\,000 + 2\,000 + 20\,000 = 23\,000$ multiplications.

- ...

Définition :

C_n = Le nombre de manières de parenthéser un produit de n facteurs $(x_1 * x_2 * x_3 * \dots * x_n)$,
 = le $n^{\text{ème}}$ nombre de Catalan

$n = 1$: (M_1) $C_1 = 1$

$n = 2$: $(M_1 \times M_2)$ $C_2 = 1$

$n = 3$: $((M_1 \times M_2) \times M_3)$
 $(M_1 \times (M_2 \times M_3))$ $C_3 = 2$

$n = 4$: $(\bullet \times (\bullet \times (\bullet \times \bullet)))$
 $(\bullet \times ((\bullet \times \bullet) \times \bullet))$
 $((\bullet \times \bullet) \times (\bullet \times \bullet))$
 $((\bullet \times \bullet) \times \bullet) \times \bullet$
 $((\bullet \times (\bullet \times \bullet)) \times \bullet)$ $C_4 = 5$

Essayons de fabriquer une relations de récurrence satisfaite par les C_n .

Lorsqu'il y a n facteurs, le dernier produit effectué est formé des k premiers facteurs (parenthésés de C_k façons) multipliés par les $n - k$ derniers facteurs (parenthésés de C_{n-k} façons), et ce, pour $k = 1, \dots, n - 1$.

$\underbrace{\left(\bullet \bullet \bullet \bullet \right)}_k$ $\underbrace{\left(\bullet \bullet \bullet \bullet \bullet \bullet \right)}_{n-k}$
 C_k parenthésages C_{n-k} parenthésages

$$\text{Ex : } n = 4 : \left(\begin{array}{c} \bullet \\ \underbrace{\hspace{1.5cm}} \\ 3 \\ \bullet \end{array} \right)$$

$$\left(\begin{array}{c} \bullet \\ \underbrace{\hspace{1.5cm}} \\ 3 \\ \bullet \end{array} \right)$$

$$\left(\begin{array}{c} \bullet \\ \underbrace{\hspace{1.5cm}} \\ 3 \\ \bullet \end{array} \right)$$

$$\left(\begin{array}{c} \bullet \\ \underbrace{\hspace{1.5cm}} \\ 3 \\ \bullet \end{array} \right)$$

$$\left(\begin{array}{c} \bullet \\ \underbrace{\hspace{1.5cm}} \\ 3 \\ \bullet \end{array} \right)$$

Calcul par récurrence :

$$\boxed{\begin{array}{l} C_n = C_1 C_{n-1} + C_2 C_{n-2} + \dots + C_k C_{n-k} + \dots + C_{n-1} C_1 \quad \forall n \geq 2 \\ C_n = \sum_{k=1}^{n-1} C_k C_{n-k} \quad \text{C.I. : } C_1 = 1 \end{array}}$$

Rem : C_n est l'analogue discret d'une convolution $\int f(t)(x-t)dt$.

Ecrivons la fonction génératrice des C_n :

$$\begin{aligned} f(x) &= \sum_{n=1}^{\infty} C_n x^n \\ &= \underbrace{C_1}_{=1} x + \sum_{n=2}^{\infty} C_n x^n \\ &= x + \sum_{n=2}^{\infty} (C_1 C_{n-1} + C_2 C_{n-2} + \dots + C_k C_{n-k} + \dots + C_{n-1} C_1) * \underbrace{x^n}_{=x^k x^{n-k}} \\ &= x + \left(\sum_{k=1}^{\infty} C_k x^k \right) * \left(\sum_{k=1}^{\infty} C_k x^k \right) \\ &= x + f(x) * f(x) \end{aligned}$$

$$\Rightarrow f(x) = x + (f(x))^2$$

$$\Leftrightarrow (f(x))^2 - f(x) + x = 0$$

$$\Rightarrow f(x) = \left\langle \begin{array}{l} \frac{1 + \sqrt{1-4x}}{2} \\ \frac{1 - \sqrt{1-4x}}{2} \end{array} \right\rangle \rightarrow \text{à rejeter car } f(0) = 0 \text{ (car } f(x) = C_1x + C_2x^2 + \dots)$$

$$\Rightarrow f(x) = \frac{1 - \sqrt{1-4x}}{2} = \frac{1}{2} - \frac{1}{2}(1-4x)^{1/2}$$

Reste à développer $f(x)$ en série de McLaurin.

$$\text{Rappel: } (1+u)^r = \sum_{n=0}^{\infty} \binom{r}{n} u^n \text{ (série du binôme qui converge pour } |u| < 1)$$

$$\binom{\frac{1}{2}}{0} = 1$$

$$\binom{\frac{1}{2}}{n} = \frac{\frac{1}{2} * \left(\frac{1}{2} - 1\right) * \left(\frac{1}{2} - 2\right) * \dots * \left(\frac{1}{2} - n + 1\right)}{n!}$$

$$\Rightarrow f(x) = \frac{1}{2} - \frac{1}{2}(1-4x)^{1/2}$$

$$= \frac{1}{2} - \frac{1}{2} \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} (-4x)^n \quad (\text{converge pour } |-4x| < 1 \Rightarrow |x| < \frac{1}{4})$$

$$= \frac{1}{2} - \frac{1}{2} \underbrace{\binom{\frac{1}{2}}{0}}_{=1} (-4x)^0 - \frac{1}{2} \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4x)^n$$

$$= -\frac{1}{2} \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-1)^n 4^n x^n$$

$$= \sum_{n=1}^{\infty} C_n x^n$$

$$\begin{aligned}
C_n &= -\frac{1}{2}(-1)^n \binom{\frac{1}{2}}{n} 4^n \\
&= (-1)^{n+1} \frac{1}{2} \frac{\overbrace{\frac{1}{2} \left(\frac{1}{2}-1\right) \left(\frac{1}{2}-2\right) \dots \left(\frac{1}{2}-n+1\right)}^{n \text{ facteurs}} 2^n 2^n}{n!} \\
&\quad \left(\text{on injecte les } n \text{ facteurs } 2 \text{ dans les } n \text{ facteurs } \left(\frac{1}{2}-n+1\right) \right) \\
&= (-1)^{n+1} \frac{1}{2} \frac{1(1-2)(1-4)(1-6)\dots(1-2n+2)2^n}{n!} \\
&= (-1)^{n+1} \frac{1}{2} \frac{\overbrace{(-1)(-3)(-5)\dots(-(2n-3))}^{n-1 \text{ facteurs}} 2^n}{n!} \\
&= \underbrace{(-1)^{n+1} (-1)^{n-1}}_{=(-1)^{2n}=1} \frac{1}{2} \frac{1 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot (2n-3) \cdot 2^n}{n!} \\
&= \frac{1}{2} \frac{1 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot (2n-3) \cdot \overbrace{2^n \cdot n!}^{=2 \cdot 4 \cdot 6 \cdot \dots \cdot (2n)}}{n! n!} \\
&= \frac{1}{2} \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \dots \cdot (2n-3) \cdot (2n-2) \cdot (\cancel{2n})}{\cancel{2} n! n!} \\
&= \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \dots \cdot (2n-3) \cdot (2n-2) \cdot n}{n! n!} \\
&= \frac{(2n-2)! n}{n! n!} \\
&= \frac{(2n-2)!}{(n-1)! (n-1)!} \frac{\cancel{n}}{\cancel{n} \cdot n} \\
C_n &= \frac{1}{n} \binom{2n-2}{n-1}
\end{aligned}$$

Remarque : Reste valable pour $n = 1$ car $C_1 = 1 = \frac{1}{1} \binom{2 \cdot 1 - 2}{1 - 1} = 1 \binom{0}{0} = 1 \cdot 1 = 1$

Conclusion :

$$\boxed{C_n = \frac{1}{n} \binom{2n-2}{n-1} \quad \forall n \geq 1 \quad \text{ou} \quad C_{n+1} = \frac{1}{n+1} \binom{2n}{n} \quad \forall n \geq 0}$$

n	C_n	F_n
1	1	1
2	1	1
3	2	2
4	5	3
5	14	5
6	42	8
7	132	13
8	429	21
9	1430	34
10	4862	55

On démontrera que $C_{n+1} \sim \frac{4^n}{n\sqrt{\pi n}}$.

Exemple : Que vaut $C_{100} = \frac{1}{100} \binom{198}{99} \approx \frac{4^{99}}{99\sqrt{99\pi}}$?

Si on peut écrire et analyser un parenthésage par seconde, le temps nécessaire $\approx 23 * 10^{55}$ secondes $\approx 7 * 10^{48}$ années (considérant que l'âge de l'univers $\approx 10^{10}$ années).

3.3 En résumé

Fonction génératrice des nombres de Fibonacci F_n

$$\sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2}$$

converge pour $|x| < \left| \frac{1-\sqrt{5}}{2} \right| = 0,618\dots$

Fonction génératrice des nombres de Catalan C_n

$$\sum_{n=1}^{\infty} C_n x^n = \frac{1-\sqrt{1-4x}}{2}$$

converge pour $|x| < \frac{1}{4}$

3.4 Nombres de Fibonacci et nombre d'or

$$\boxed{F_{n+2} = F_{n+1} + F_n \quad \forall n \geq 0, \\ F_0 = 0, F_1 = 1}$$

$$F_n = 0, 1, 1, 2, 3, 5, 8, 13, 21, \dots$$

On a vu que $\boxed{F_n = \frac{1}{\sqrt{5}}(\varphi^n - \bar{\varphi}^n), \forall n \geq 0 \quad \text{ou} \quad F_n = \lfloor \frac{\varphi^n}{\sqrt{5}} \rfloor, \forall n \geq 0}$ (formule de Binet)

où

$$\boxed{\varphi = \frac{1+\sqrt{5}}{2} = 1,6180339887\dots \quad (\text{nombre d'or})}$$

$$\bar{\varphi} = \frac{1-\sqrt{5}}{2} = -0,6180339887\dots$$

Remarque : φ et $\bar{\varphi}$ sont les 2 racines de $x^2 = x + 1$

Vers 1600, Képler a remarqué que $\frac{F_2}{F_1}, \frac{F_3}{F_2}, \frac{F_4}{F_3}, \dots, \frac{F_{n+1}}{F_n}, \dots \xrightarrow{n \rightarrow \infty} \varphi$

Ceci fournit une suite très simple d'approximations **rationnelles** de φ

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \dots \rightarrow \varphi$$

Démonstration :

$$\begin{aligned} \frac{F_{n+1}}{F_n} &= \frac{\frac{1}{\sqrt{5}}(\varphi^{n+1} - \bar{\varphi}^{n+1})}{\frac{1}{\sqrt{5}}(\varphi^n - \bar{\varphi}^n)} \\ &= \frac{\varphi - \bar{\varphi} \left(\frac{\bar{\varphi}}{\varphi}\right)^n}{1 - \left(\frac{\bar{\varphi}}{\varphi}\right)^n} \end{aligned}$$

$$\text{Or } 0 < \left| \frac{\bar{\varphi}}{\varphi} \right| < 1$$

$$\Rightarrow \left(\frac{\bar{\varphi}}{\varphi}\right)^n \xrightarrow{n \rightarrow \infty} 0 \quad \text{donc} \quad \frac{F_{n+1}}{F_n} = \frac{\varphi - \bar{\varphi} \left(\frac{\bar{\varphi}}{\varphi}\right)^n}{1 - \left(\frac{\bar{\varphi}}{\varphi}\right)^n} \xrightarrow{n \rightarrow \infty} \varphi$$

Remarque : La suite des $\frac{F_{n+1}}{F_n} \rightarrow \varphi$ en oscillant autour de φ .

$$\text{En fait, } \begin{cases} \frac{F_{n+1}}{F_n} > \varphi & \text{si } n \text{ est pair} \\ \frac{F_{n+1}}{F_n} < \varphi & \text{si } n \text{ est impair} \end{cases}$$

Supposons n pair

$$\frac{F_{n+1}}{F_n} = \frac{\varphi - \bar{\varphi} \left(\frac{\bar{\varphi}}{\varphi}\right)^n}{1 - \left(\frac{\bar{\varphi}}{\varphi}\right)^n}$$

$$\frac{\bar{\varphi}}{\varphi} < 0 \Rightarrow \left(\frac{\bar{\varphi}}{\varphi}\right)^n > 0 \text{ car } n \text{ pair}$$

$$\bar{\varphi} < 0 \Rightarrow \varphi - \bar{\varphi} \left(\frac{\bar{\varphi}}{\varphi}\right)^n > \varphi$$

$$\text{Mais } 1 - \left(\frac{\bar{\varphi}}{\varphi}\right)^n < 1$$

$$\Rightarrow \frac{F_{n+1}}{F_n} = \frac{\varphi - \bar{\varphi} \left(\frac{\bar{\varphi}}{\varphi}\right)^n}{1 - \left(\frac{\bar{\varphi}}{\varphi}\right)^n} > \varphi$$

Fractions continuées (parfois appelées à tort fractions continues)

φ est racine de l'équation $x^2 = x + 1$

$$\text{On a } \varphi^2 = \varphi + 1$$

$$\Rightarrow \varphi = 1 + \frac{1}{\varphi}$$

$$\Rightarrow \varphi = 1 + \frac{1}{1 + \frac{1}{\varphi}}$$

$$\Rightarrow \varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\dots}}}}$$

Conséquence : La suite des nombres rationnels $1, 1 + \frac{1}{1}, 1 + \frac{1}{1 + \frac{1}{1}}, 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}, \dots \longrightarrow \varphi$

Autre exemple : Que vaut la fraction continuée

$$x = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\dots}}}} \quad ?$$

$$\text{Astuce : } x+1 = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\dots}}}$$

$$\Rightarrow x+1 = 2 + \frac{1}{x+1}$$

$$\Leftrightarrow x-1 = \frac{1}{x+1}$$

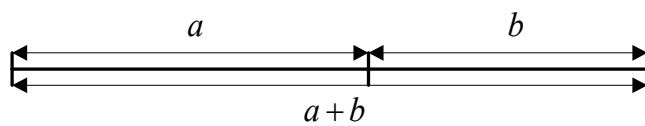
$$\Leftrightarrow x^2 - 1 = 1$$

$$\Leftrightarrow x^2 = 2$$

$$\Rightarrow x = \pm\sqrt{2}$$

Quelques apparitions de φ en math

1) Partager un segment en deux morceaux de sorte que



$$\frac{\text{grand}}{\text{moyen}} = \frac{\text{moyen}}{\text{petit}}$$

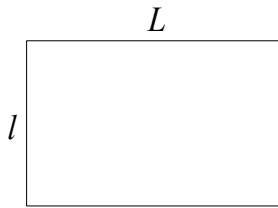
$$\Rightarrow \frac{a+b}{a} = \frac{a}{b}$$

$$\Leftrightarrow \frac{\frac{a}{b} + 1}{\frac{a}{b}} = \frac{a}{b}$$

$$\Leftrightarrow \frac{a}{b} + 1 = \left(\frac{a}{b}\right)^2$$

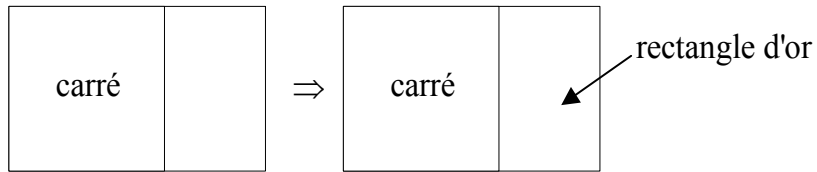
$$\boxed{\Rightarrow \frac{a}{b} = \varphi}$$

On appelle rectangle d'or, tout rectangle

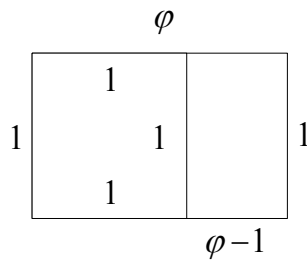


tel que $\frac{L}{l} = \varphi$

Propriété :



Démonstration :

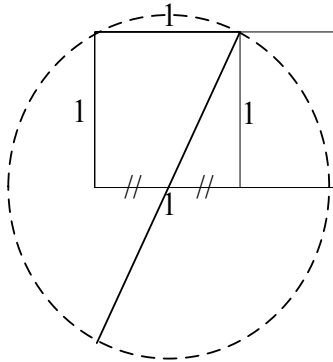


$$\frac{\varphi}{1} = \frac{1}{\varphi - 1} \Leftrightarrow \varphi^2 - \varphi = 1$$

$$\Leftrightarrow \varphi^2 = \varphi + 1$$

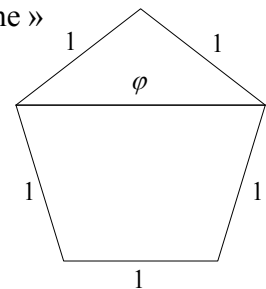
□

2) Construction rapide d'un rectangle d'or



$$r = \sqrt{\frac{1}{4} + 1} = \sqrt{\frac{5}{4}} = \frac{\sqrt{5}}{2}$$

Luca Pacioli a écrit en 1509 un livre intitulé « De divina proportione » dans lequel il démontre que dans tout pentagone régulier convexe :



et il en déduit, avec l'aide de Léonardo da Vinci, une construction simple.

CHAPITRE II : Relations de récurrence

1. Récurrences linéaires homogènes à coefficients constants

1.1 Définition :

Une relation de récurrence de la forme

$$a_0 u_{n+k} + a_1 u_{n+k-1} + \dots + a_k u_n = 0 \quad \forall n \geq 0 \quad (*)$$

où les a_i sont des constantes réelles, avec $a_0 \neq 0$, est une **récurrence linéaire homogène d'ordre k** (analogue discret d'une équation différentielle linéaire homogène d'ordre k).

Exemple : $u_{n+2} - u_{n+1} - u_n = 0 \quad \forall n \geq 0$, conditions initiales $u_0 = 0, u_1 = 1$ est la récurrence associée à la suite des nombres de Fibonacci.

Remarque : L'inconnue est une suite u_1, u_2, u_3, \dots de nombres réels.

Méthode de résolution :

On associe à (*) son *polynôme caractéristique*

$$\boxed{a_0 \lambda^k + a_1 \lambda^{k-1} + \dots + a_k} \quad (\text{de degré } k)$$

1.2 Théorème :

Si l'équation caractéristique admet les racines distinctes

$$\alpha_1, \alpha_2, \dots, \alpha_r$$

de multiplicités

$$m_1, m_2, \dots, m_r$$

alors :

$$u_n = P_1(n) \alpha_1^n + P_2(n) \alpha_2^n + \dots + P_r(n) \alpha_r^n$$

où $P_i(n)$ est un polynôme en n de degré $\leq m_i - 1$ ($i = 1, \dots, r$).

Exemples :

1) Résoudre :

$$\begin{cases} u_{n+2} - u_{n+1} - u_n = 0 & \forall n \geq 0 \\ u_0 = 0 \\ u_1 = 1 \end{cases}$$

$$\text{Equation caractéristique : } \lambda^2 - \lambda - 1 = 0 \Rightarrow \lambda = \frac{1 \pm \sqrt{5}}{2}$$

$$\Rightarrow \begin{cases} \alpha_1 = \frac{1 + \sqrt{5}}{2} & m_1 = 1 \\ \alpha_2 = \frac{1 - \sqrt{5}}{2} & m_2 = 1 \end{cases}$$

$$\Rightarrow u_n = A \left(\frac{1 + \sqrt{5}}{2} \right)^n + B \left(\frac{1 - \sqrt{5}}{2} \right)^n$$

$$\text{Conditions initiales : } \begin{cases} u_0 = 0 = A + B \\ u_1 = 1 = A \left(\frac{1 + \sqrt{5}}{2} \right) + B \left(\frac{1 - \sqrt{5}}{2} \right) \end{cases}$$

$$\Leftrightarrow \begin{cases} 0 = A + B & (I) \\ 2 = A(1 + \sqrt{5}) + B(1 - \sqrt{5}) & (II) \end{cases}$$

$$(II) - (I) \Rightarrow 2 = A\sqrt{5} - B\sqrt{5} \Rightarrow A - B = \frac{2}{\sqrt{5}}$$

$$\begin{cases} A + B = 0 \\ A - B = \frac{2}{\sqrt{5}} \end{cases} \Rightarrow \begin{cases} A = \frac{1}{\sqrt{5}} \\ B = -\frac{1}{\sqrt{5}} \end{cases}$$

$$\Rightarrow u_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right)$$

2) $u_{n+4} - 5u_{n+3} + 6u_{n+2} + 4u_{n+1} - 8u_n = 0 \quad \forall n \geq 0$

$$u_0 = 0, u_1 = -9, u_2 = -1, u_3 = 21$$

$$\text{Equation caractéristique : } \lambda^4 - 5\lambda^3 + 6\lambda^2 + 4\lambda - 8 = 0 \Leftrightarrow (\lambda - 2)^3 (\lambda + 1) = 0$$

$$\Rightarrow \begin{cases} \alpha_1 = 2 & m_1 = 3 \\ \alpha_2 = -1 & m_2 = 1 \end{cases}$$

$$\Rightarrow u_n = (An^2 + Bn + C)2^n + D(-1)^n \quad (\text{solution générale})$$

$$\begin{cases} u_0 = 0 = C + D \\ u_1 = -9 = 2A + 2B + 2C - D \\ u_2 = -1 = 16A + 8B + 4C + D \\ u_3 = 21 = 72A + 24B + 8C - D \end{cases} \longrightarrow \begin{cases} A = 1 \\ B = -1 \\ C = -3 \\ D = 3 \end{cases}$$

$$\boxed{\Rightarrow u_n = (n^2 - n - 3)2^n + 3(-1)^n}$$

3) Avec l'alphabet $\{A, B, C\}$ combien peut-on écrire de mots de n lettres dans lesquels on a ni 2 B côte à côte, ni 2 C côte à côte ?

Soit u_n le nombre de tels mots de n lettres :

$$u_1 = 3(A \text{ ou } B \text{ ou } C)$$

$$u_2 = 7(AA, AB, AC, BA, BC, CA, CB)$$

$$u_n = \# \text{ mots de } n \text{ lettres se terminant par } A \quad \overbrace{\boxed{}}^{n-1} \boxed{A} = A_n$$

$$+ \# \text{ mots de } n \text{ lettres se terminant par } B \quad \boxed{} \boxed{B} = B_n$$

$$+ \# \text{ mots de } n \text{ lettres se terminant par } C \quad \boxed{} \boxed{C} = C_n$$

$$\Rightarrow u_n = A_n + B_n + C_n$$

Mais

$$A_n = u_{n-1}$$

$$B_n = A_{n-1} + C_{n-1}$$

$$C_n = A_{n-1} + B_{n-1}$$

$$\Rightarrow u_n = u_{n-1} + \underbrace{A_{n-1}}_{=u_{n-2}} + \underbrace{C_{n-1} + A_{n-1} + B_{n-1}}_{=u_{n-1}}$$

$$\Rightarrow u_n = 2u_{n-1} + u_{n-2} \Rightarrow \begin{cases} u_n - 2u_{n-1} - u_{n-2} = 0 \\ u_1 = 3 \\ u_2 = 7 \end{cases}$$

$$\text{Equation caractéristique : } \lambda^2 - 2\lambda - 1 = 0 \Rightarrow \lambda = 1 \pm \sqrt{2}$$

$$\left. \begin{array}{l} \alpha_1 = 1 + \sqrt{2} \quad m_1 = 1 \\ \alpha_2 = 1 - \sqrt{2} \quad m_2 = 1 \end{array} \right\} \Rightarrow u_n = \alpha(1 + \sqrt{2})^n + \beta(1 - \sqrt{2})^n$$

Conditions initiales :

$$u_1 = 3 = \alpha(1 + \sqrt{2}) + \beta(1 - \sqrt{2})$$

$$u_2 = 7 = \alpha(1 + \sqrt{2})^2 + \beta(1 - \sqrt{2})^2$$

\Rightarrow On a deux équations linéaires à deux inconnues α et β !

Essayons d'obtenir un système en α et β plus simple à résoudre.

Astuce : La suite recherchée est du type : $\underbrace{?}_{u_0}, \underbrace{3}_{u_1}, \underbrace{7}_{u_2}, \underbrace{17}_{u_3}, \dots, u_n, \dots$

En toute rigueur, dans le problème posé, u_0 n'a pas de sens. Néanmoins, si on calcule la valeur de u_0 vérifiant la condition $u_2 = 2u_1 + u_0$, càd : $7 = 2 \cdot 3 + u_0 \Rightarrow u_0 = 1$

$$n = 0: u_0 = 1 = \alpha + \beta \quad (*)$$

$$n = 1: u_1 = 3 = \alpha(1 + \sqrt{2}) + \beta(1 - \sqrt{2}) \quad (**)$$

$$(**) - (*) \Rightarrow 2 = \alpha\sqrt{2} - \beta\sqrt{2} \Rightarrow \alpha - \beta = \frac{2}{\sqrt{2}} = \sqrt{2}$$

$$\left. \begin{array}{l} \alpha + \beta = 1 \\ \alpha - \beta = \sqrt{2} \end{array} \right\} \Rightarrow \begin{cases} \alpha = \frac{1 + \sqrt{2}}{2} \\ \beta = \frac{1 - \sqrt{2}}{2} \end{cases}$$

$$\Rightarrow u_n = \frac{1 + \sqrt{2}}{2} (1 + \sqrt{2})^n + \frac{1 - \sqrt{2}}{2} (1 - \sqrt{2})^n$$

$$= \frac{1}{2} \left((1 + \sqrt{2})^{n+1} + (1 - \sqrt{2})^{n+1} \right)$$

$$\sqrt{2} = 1,4142\dots$$

$$\rightarrow |1 - \sqrt{2}| = 0,5857\dots < 1$$

$$\Rightarrow |1 - \sqrt{2}|^{n+1} < 1 \quad \forall n \geq 0$$

$$\Rightarrow \frac{1}{2} |1 - \sqrt{2}|^{n+1} < \frac{1}{2} \quad \forall n \geq 0$$

$$\underbrace{u_n}_{\text{entier}} = \underbrace{\frac{1}{2} (1 + \sqrt{2})^{n+1}}_{\text{réel}} + \underbrace{\frac{1}{2} (1 - \sqrt{2})^{n+1}}_{\text{réel}}$$

$$\Rightarrow u_n = \left\lfloor \frac{1}{2} (1 + \sqrt{2})^{n+1} \right\rfloor$$

4) De combien de manières différentes peut-on paver un rectangle $3 \times n$ avec des dominos 2×1 ?

Soit u_n le nombre de tels pavages.

Si $n = 2m + 1$ est impair, $u_n = 0$ (car le nombre total de carrés 1×1 à couvrir vaut $3n = 6m + 3$ (impair) et chaque domino couvre deux carrés \Rightarrow impossible).

\rightarrow supposons que n est pair ($n = 2m$)

$$u_{2m} = \# \text{ pavages} \quad \begin{array}{c} \text{Diagram: } 3 \times 2m \text{ rectangle with a } 2 \times 1 \text{ domino at the bottom right corner.} \\ \text{Diagram: } 3 \times 2m \text{ rectangle with a } 2 \times 1 \text{ domino at the top right corner.} \end{array} = a_m$$

$$+ \# \text{ pavages} \quad \begin{array}{c} \text{Diagram: } 3 \times 2m \text{ rectangle with a } 2 \times 1 \text{ domino at the bottom right corner.} \\ \text{Diagram: } 3 \times 2m \text{ rectangle with a } 2 \times 1 \text{ domino at the top right corner.} \end{array} = a_m \text{ (par symétrie)}$$

$$+ \# \text{ pavages} \quad \begin{array}{c} \text{Diagram: } 3 \times 2m \text{ rectangle with three } 2 \times 1 \text{ dominos stacked vertically on the right side.} \end{array} = b_m$$

$$\boxed{u_{2m} = 2a_m + b_m \quad \forall m \geq 1}$$

$$\text{avec } a_1 = 1 \quad \begin{array}{c} \text{Diagram: } 3 \times 2 \text{ rectangle with a } 2 \times 1 \text{ domino at the top right corner.} \\ \text{Diagram: } 3 \times 2 \text{ rectangle with a } 2 \times 1 \text{ domino at the bottom right corner.} \end{array}$$

$$\text{avec } b_1 = 1 \quad \begin{array}{c} \text{Diagram: } 3 \times 2 \text{ rectangle with three } 2 \times 1 \text{ dominos stacked vertically on the right side.} \end{array}$$

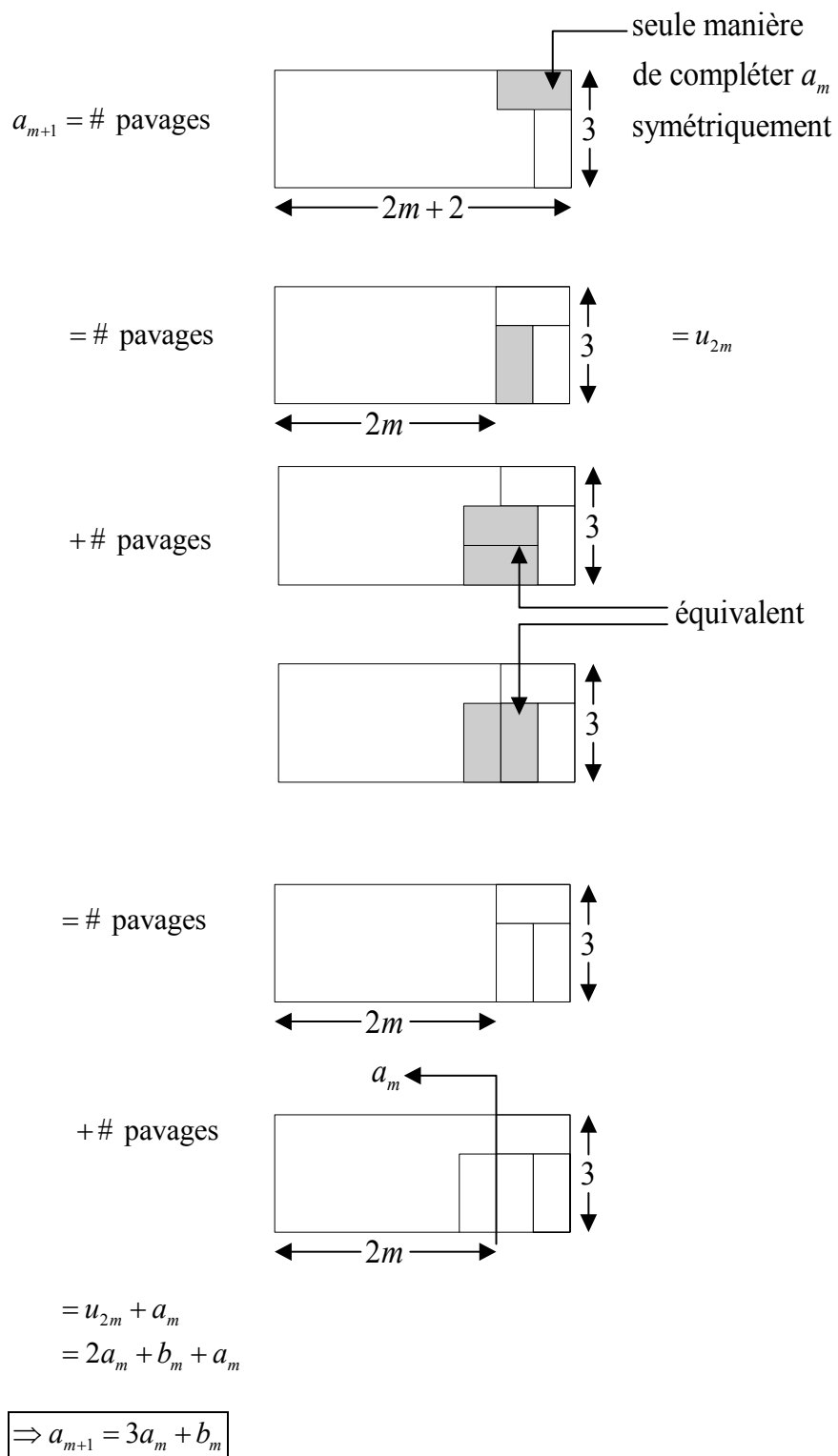
Cherchons des relations entre les a_m et les b_m

$$b_{m+1} = \# \text{ pavages} \quad \begin{array}{c} \text{Diagram: } 3 \times (2m+2) \text{ rectangle with three } 2 \times 1 \text{ dominos stacked vertically on the right side.} \\ \text{Diagram: } 3 \times (2m+2) \text{ rectangle with three } 2 \times 1 \text{ dominos stacked vertically on the right side.} \end{array}$$

$$= u_{2m+2}$$

$$= 2a_{m+1} + b_{m+1}$$

$$\boxed{\Rightarrow b_{m+1} = 2a_m + b_m}$$



Résumé :

$$\boxed{\begin{array}{l} u_{2m} = 2a_m + b_m \\ a_{m+1} = 3a_m + b_m \\ b_{m+1} = 2a_m + b_m = u_{2m} \\ \\ \underbrace{a_1 = 1 = b_1}_{u_2=3} \end{array}}$$

On en tire

$$\left. \begin{array}{l} a_2 = 3a_1 + b_1 = 4 \\ b_2 = 2a_1 + b_1 = 3 \end{array} \right\} \rightarrow u_4 = 2a_2 + b_2 = 11$$

Essayons d'éliminer les a_m et les b_m , pour ne plus avoir que des u_{2m} :

$$\begin{aligned} u_{2m+4} &= 2a_{m+2} + b_{m+2} \\ &= 2(3a_{m+1} + b_{m+1}) + 2a_{m+1} + b_{m+1} \\ &= 6a_{m+1} + 2b_{m+1} + 2a_{m+1} + b_{m+1} \\ &= 8a_{m+1} + 3b_{m+1} \\ &= (8a_{m+1} + 4b_{m+1}) - b_{m+1} \\ &= 4(\underbrace{2a_{m+1} + b_{m+1}}_{u_{2m+2}}) - \underbrace{b_{m+1}}_{u_{2m}} \\ &= 4u_{2m+2} - u_{2m} \end{aligned}$$

$$\boxed{\Rightarrow u_{2m+4} - 4u_{2m+2} + u_{2m} = 0 \quad \forall m \geq 1} \quad \text{avec } u_2 = 3 \text{ et } u_4 = 11$$

Posons $u_{2m} = x_m$, on a alors

$$x_{m+2} - 4x_{m+1} + x_m = 0 \quad \forall m \geq 1$$

Equation caractéristique :

$$\lambda^2 - 4\lambda + 1 = 0 \quad \Rightarrow \lambda = 2 \pm \sqrt{3}$$

$$\Rightarrow x_m = A(2 + \sqrt{3})^m + B(2 - \sqrt{3})^m$$

$$\boxed{\Rightarrow u_{2m} = A(2 + \sqrt{3})^m + B(2 - \sqrt{3})^m \quad \forall m \geq 1}$$

Astuce :

$$u_4 - 4u_2 + u_0 = 0$$

$$\Rightarrow 11 - 12 + u_0 = 0$$

$$\boxed{\Rightarrow u_0 = 1}$$

$$\left. \begin{array}{l} 2m = 0 \Rightarrow u_0 = 1 = A + B \\ 2m = 2 \Rightarrow u_2 = 3 = A(2 + \sqrt{3}) + B(2 - \sqrt{3}) \end{array} \right\} \Rightarrow \begin{cases} A = \frac{1}{2} \left(1 + \frac{\sqrt{3}}{3} \right) = \frac{3 + \sqrt{3}}{6} \\ B = \frac{1}{2} \left(1 - \frac{\sqrt{3}}{3} \right) = \frac{3 - \sqrt{3}}{6} \end{cases}$$

Finalemment

$$\boxed{\begin{array}{l} u_{2m} = \frac{3 + \sqrt{3}}{6} (2 + \sqrt{3})^m + \frac{3 - \sqrt{3}}{6} (2 - \sqrt{3})^m \\ u_{2m+1} = 0 \end{array}}$$

Remarques :

$$1) \quad 2 - \sqrt{3} = 0,26794\dots \Rightarrow 0 < 2 - \sqrt{3} < 1 \\ \Rightarrow 0 < (2 - \sqrt{3})^m \leq 1 \quad \forall m \geq 0$$

$$2) \quad \frac{3 - \sqrt{3}}{6} = 0,21132\dots \Rightarrow 0 < \frac{3 - \sqrt{3}}{6} < \frac{1}{2} \\ \Rightarrow 0 < \frac{3 - \sqrt{3}}{6} (2 - \sqrt{3})^m < \frac{1}{2} \quad \forall m \geq 0$$

$$\underline{\text{Conclusion}} : \boxed{u_{2m} = \left\lceil \frac{3 + \sqrt{3}}{6} (2 + \sqrt{3})^m \right\rceil \quad \forall m \geq 0}$$

2. Réurrences linéaires non-homogènes à coefficients constants

$$a_0 * u_{n+k} + a_1 * u_{n+k-1} + \dots + a_k * u_n = f(n) \quad \forall n \geq 0 \quad (I)$$

Réurrence linéaire homogène associée à (I) :

$$a_0 * u_{n+k} + a_1 * u_{n+k-1} + \dots + a_k * u_n = 0 \quad \forall n \geq 0 \quad (II)$$

Théorème :

La solution générale de (I) s'obtient en ajoutant à la solution générale de (II) une solution particulière de (I).

Problème :

Avec l'alphabet latin $\{A, B, \dots, Z\}$, combien peut-on écrire de mots de n lettres ayant un nombre impair de lettres A ?

Soit u_n le nombre total de mots.

$$u_1 = 1$$

$$\begin{array}{l}
 u_n = \# \text{ mots } \overbrace{\boxed{}}^{n-1} \boxed{A} = A_n \\
 + \# \text{ mots } \overbrace{\boxed{}}^{n-1} \boxed{B} = B_n \\
 \dots \\
 + \# \text{ mots } \overbrace{\boxed{}}^{n-1} \boxed{Z} = Z_n
 \end{array}$$

$$\Rightarrow u_n = A_n + B_n + \dots + Z_n$$

On a $B_n = C_n = \dots = Z_n$ (mots de $n-1$ lettres ayant un nombre impair de A).

$$\Rightarrow u_n = A_n + 25u_{n-1}$$

A_n = nombre de mots de $n-1$ lettres ayant un nombre pair de A
 = nombre total de mots de $n-1$ lettres
 - nombre de mots de $n-1$ lettres ayant un nombre impair de A

$$A_n = 26^{n-1} - u_{n-1}$$

$$\Rightarrow u_n = 26^{n-1} - u_{n-1} + 25u_{n-1}$$

$$\Rightarrow u_n = 26^{n-1} + 24u_{n-1}$$

On a $\boxed{u_n - 24u_{n-1} = 26^{n-1}}$ (I) avec $u_1 = 1$.

(récurrence linéaire non homogène à coefficients constants, du 1^{er} ordre)

1^{ère} étape : Trouver la solution générale de la récurrence homogène associée :

$$u_n - 24u_{n-1} = 0 \quad (\text{II})$$

Equation caractéristique :

$$\lambda - 24 = 0 \quad \Rightarrow \lambda = 24$$

Solution générale de (II) : $\boxed{u_n = A * 24^n}$

2^{ème} étape : Trouver une solution particulière de (I). Le second membre étant de type « exponentielle », essayons de trouver une solution particulière de la forme :

$$u_n = K * 26^n$$

En remplaçant dans (I), on obtient

$$K * 26^n - 24 * K * 26^{n-1} = 26^{n-1}$$

$$\Rightarrow 2K = 1$$

$$\Rightarrow K = \frac{1}{2}$$

Solution particulière de (I) : $\boxed{u_n = \frac{1}{2} * 26^n}$

Conclusion : Solution générale de (I) : $\boxed{u_n = A * 24^n + \frac{1}{2} * 26^n}$

$$\text{Or, } u_1 = 1 = A * 24 + \frac{1}{2} * 26$$

$$1 = A * 24 + 13$$

$$-12 = A * 24$$

$$-\frac{1}{2} = A$$

$$\Rightarrow u_n = -\frac{1}{2} * 24^n + \frac{1}{2} * 26^n$$

$$\Rightarrow \boxed{u_n = \frac{1}{2} (26^n - 24^n)}$$

Exemple :

$$u_{n+2} - 6u_{n+1} + 9u_n = 2^n + n \quad (\text{I})$$

Réurrence homogène associée :

$$u_{n+2} - 6u_{n+1} + 9u_n = 0 \quad (\text{II})$$

Equation caractéristique :

$$\lambda^2 - 6\lambda + 9 = 0$$

$$(\lambda - 3)^2 = 0$$

$$\Rightarrow \lambda_1 = 3 \text{ (racine double)}$$

$$u_n = (An + B) * 3^n \quad \text{S.G. de (II)}$$

Reste donc à trouver une solution particulière de (I). Le second membre est une somme d'une exponentielle en n (de base 2) et d'un polynôme en n . Cherchons-en une de la forme :

$$u_n = a2^n + bn + c$$

En remplaçant dans (I), on trouve

$$\underbrace{a * 2^{n+2}}_{a * 2^n * 2^2} + b(n+2) + c$$

$$-6a * 2^{n+1} - 6b(n+1) - 6c$$

$$+9a * 2^n + 9bn + 9c = 2^n + n$$

$$4a * 2^n - 12 * 2a^n + 9 * 2a^n + bn - 6bn + 9bn$$

$$+2b - 6b + c - 6c + 9c = 2^n + n$$

$$a * 2^n + 4bn - 4b + 4c = 2^n + n$$

$$\Rightarrow \begin{cases} a = 1 \\ b = \frac{1}{4} \\ c = \frac{1}{4} \end{cases}$$

$$u_n = 2^n + \frac{1}{4}(n+1) \quad \text{S.P. de (I)}$$

$$\text{Solution générale de (I) : } \boxed{u_n = (An + B) * 3^n + 2^n + \frac{1}{4}(n+1)}$$

$$\begin{aligned}
\Rightarrow a_n &= \binom{2n-2}{n-1} - \text{nombre de chemins minimaux de } A'' \text{ à } B' \\
&= \binom{2n-2}{n-1} - \binom{n+n-2}{n} \\
&= \binom{2n-2}{n-1} - \binom{2n-2}{n} \\
&= \frac{(2n-2)!}{(n-1)!(n-1)!} - \frac{(2n-2)!}{(n-2)!n!} \\
&= \frac{(2n-2)!}{(n-1)!(n-2)!} * \left(\frac{1}{n-1} - \frac{1}{n} \right) \\
&= \frac{(2n-2)!}{(n-1)!(n-2)!} * \frac{1}{(n-1)n} \\
&= \frac{1}{n} * \frac{(2n-2)!}{(n-1)!(n-1)!} \\
&= \frac{1}{n} \binom{2n-2}{n-1} = C_n \quad \forall n \geq 2
\end{aligned}$$

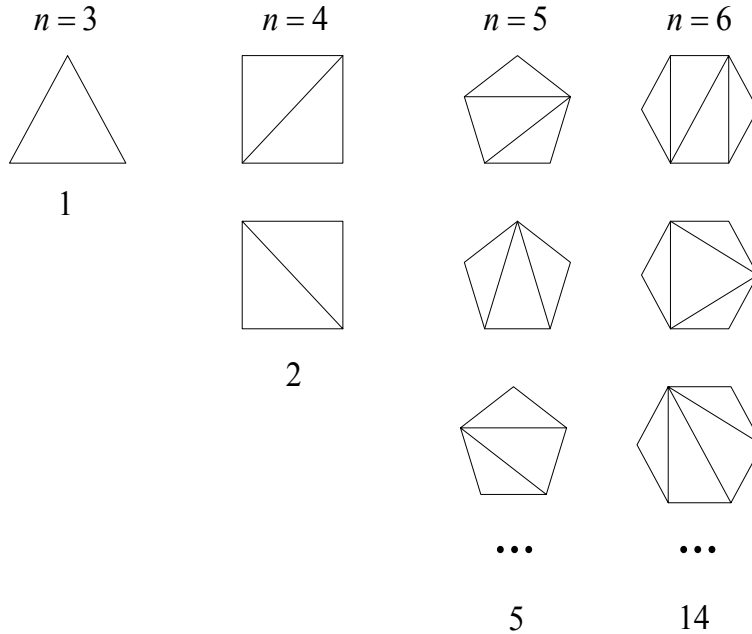
Pour $n = 1$, on voit que $a_1 = 1$ et $\frac{1}{1} \binom{2 \cdot 1 - 2}{1 - 1} = 1 \cdot \binom{0}{0} = 1$

Conclusion: $a_n = \frac{1}{n} \binom{2n-2}{n-1} = C_n \quad \forall n \geq 1$

3.2. Triangulations d'un n -gone convexe

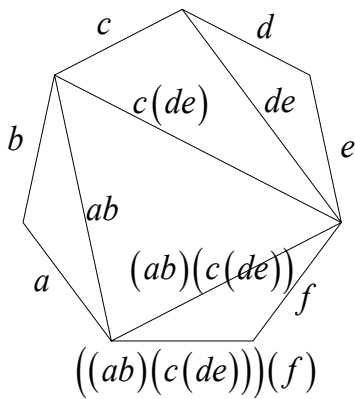
Problème (Euler) :

De combien de façons différentes peut-on découper un n -gone régulier convexe ($n \geq 3$) en triangles, en traçant des diagonales qui ne se coupent jamais à l'intérieur du n -gone ?



Il semble que ce nombre soit égal à C_{n-1} . Comment le montrer ?

Astuce : pour fixer les idées, posons $n = 7$



L'un des côtés du 7-gone, choisi arbitrairement, est appelé la base. A chacun des 6 côtés restants, associons une lettre (d'un alphabet de 6 lettres) ($\rightarrow n-1$ lettres).

Toute triangulation d'un n -gone, dans lequel on a choisi une base, détermine univoquement un parenthésage d'un produit de $n-1$ facteurs.

Réciproquement, la donnée d'un parenthésage de $n-1$ facteurs permet de reconstruire univoquement la triangulation correspondante.

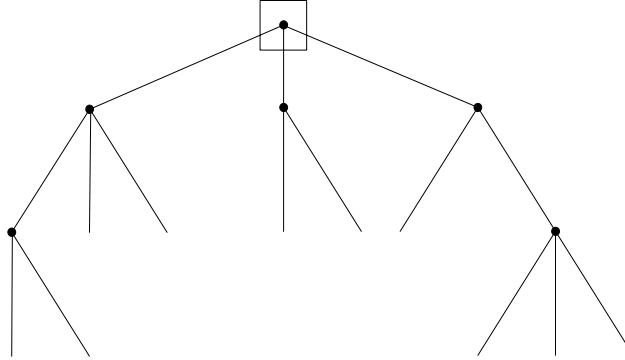
Triangulation du 7-gone \Leftrightarrow parenthésage du produit $abcdef$ de 6 facteurs

Conclusion : Le nombre de triangulations d'un n -gone convexe est le même que le nombre de parenthésages d'un produit de $n-1$ facteurs, donc vaut C_{n-1} .

3.3. Arbre binaire de n sommets

Arbre = graphe non dirigé connexe sans circuit.

Arbre à racine = arbre dans lequel un des sommets est appelé racine.



Un *arbre binaire* est un arbre tel que

- tout fils d'un sommet est qualifié de gauche ou de droit
- tout sommet a au plus un fils gauche et au plus un fils droit

Soit A_n = nombre d'arbres binaires de n sommets

$n = 1$



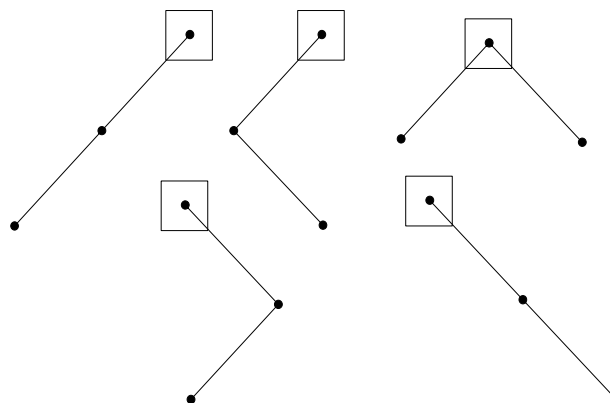
$A_1 = 1$

$n = 2$

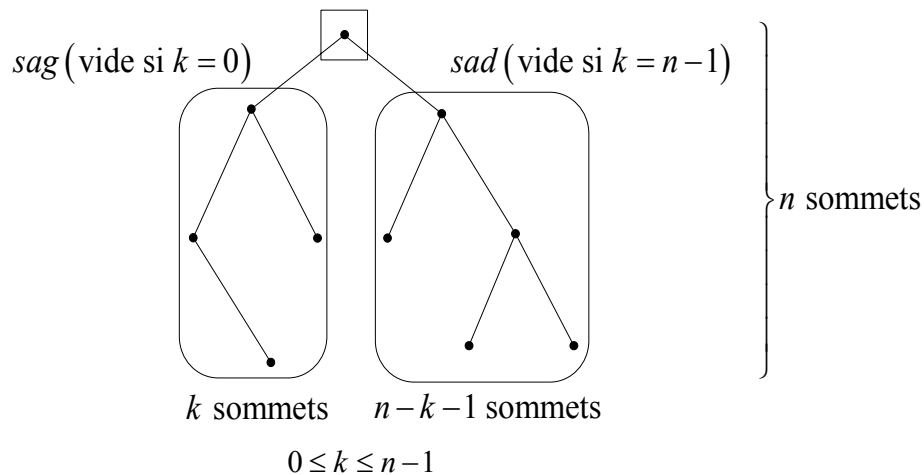


$A_2 = 2$

$n = 3$



$A_3 = 5$



Astuce : Tout arbre binaire de n sommets s'obtient en suspendant à la racine un arbre binaire gauche de k ($k = 0, 1, \dots, n - 1$) sommets et un arbre binaire droit de $n - 1 - k$ sommets.

$$\begin{aligned} \Rightarrow A_n &= A_0 * A_{n-1} + A_1 * A_{n-2} + \dots + A_{n-1} * A_0 \\ &\text{où } A_0 = 1 \text{ (par convention)} \quad \forall n \geq 1 \end{aligned}$$

Changement de variable : posons $A_n = A'_{n+1}$, alors

$$\begin{aligned} A'_{n+1} &= A'_1 * A'_n + A'_2 * A'_{n-1} + \dots + A'_n * A'_1 \\ &\text{où } A'_1 = 1 \end{aligned}$$

Analogie avec la récurrence des nombres de Catalan :

$$\begin{aligned} C_{n+1} &= C_1 * C_n + C_2 * C_{n-1} + \dots + C_n * C_1 \\ &\text{où } C_1 = 1 \end{aligned}$$

$$\Rightarrow A_n = C_{n+1} = \frac{1}{n+1} \binom{2n}{n}$$

Conclusion :

Il y a exactement $C_{n+1} = \frac{1}{n+1} \binom{2n}{n}$ arbres binaires de n sommets.

CHAPITRE III : Comportements asymptotiques

Considérons deux fonctions $f, g : \mathbb{N}_0 \rightarrow \mathbb{R}$

Définition :

Soit F l'ensemble des fonctions

$$f : \mathbb{N}_0 \rightarrow \mathbb{R} : n \rightarrow f(n)$$

qui sont non nulles lorsque n est suffisamment grand.

Soit $f, g \in F$.

On dit que f a le même comportement asymptotiquement que g si

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$$

ce que l'on écrit $f(n) \sim g(n)$ (ou $f \sim g$).

Propriétés

- 1) $f(n) \sim f(n), \quad \forall f \in F$ (réflexivité)
- 2) $f(n) \sim g(n) \Rightarrow g(n) \sim f(n)$ (symétrie)
- 3) $f(n) \sim g(n)$ et $g(n) \sim h(n) \Rightarrow f(n) \sim h(n)$ (transitivité)

Donc la relation \sim est une relation d'équivalence dans F .

Ceci partitionne F en classes de fonctions ayant le même comportement asymptotique.

Remarque importante :

Si $f(n) \sim g(n)$, alors l'**erreur relative** commise en remplaçant $f(n)$ par $g(n)$ tend vers 0 quand $n \rightarrow \infty$. En effet,

$$\left. \begin{array}{l} \text{erreur absolue} \\ \frac{f(n) - g(n)}{f(n)} \end{array} \right\} \text{erreur relative}$$

$$\lim_{n \rightarrow \infty} \frac{f(n) - g(n)}{f(n)} = 1 - \lim_{n \rightarrow \infty} \frac{g(n)}{f(n)} = 1 - 1 = 0$$

Mais *l'erreur absolue* ne tend pas nécessairement vers 0, elle peut même tendre vers l'infini.

Exemples :

$$1) \quad (n+1)^2 \sim n^2 \text{ car } \lim_{n \rightarrow \infty} \frac{(n+1)^2}{n^2} = 1$$

$$\text{Erreur absolue} = (n+1)^2 - n^2 = 2n+1 \xrightarrow{n \rightarrow \infty} \infty$$

$$2) \quad (n+1)^2 \sim n^2 + 2n$$

$$\text{Erreur absolue} = 1$$

$$3) \quad (n+1)^2 \sim n^2 + 2n + 1$$

$$\text{Erreur absolue} = 0$$

1. Nombres de Fibonacci

$$\text{On a vu que } F_n = \lfloor \frac{\varphi^n}{\sqrt{5}} \rfloor \quad \text{où } \varphi = \frac{1+\sqrt{5}}{2}$$

$$\Rightarrow \left| F_n - \frac{1}{\sqrt{5}} \varphi^n \right| < \frac{1}{2}$$

$$\Rightarrow \frac{F_n - \frac{1}{\sqrt{5}} \varphi^n}{F_n} \xrightarrow{n \rightarrow \infty} 0 \quad (\text{car } F_n \xrightarrow{n \rightarrow \infty} \infty)$$

$$\Rightarrow \lim_{n \rightarrow \infty} \left(\frac{F_n - \frac{1}{\sqrt{5}} \varphi^n}{F_n} \right) = 0$$

$$\Rightarrow \lim_{n \rightarrow \infty} \frac{\frac{1}{\sqrt{5}} \varphi^n}{F_n} = 1$$

$$\boxed{\Rightarrow F_n \sim \frac{1}{\sqrt{5}} (\varphi)^n} \quad (\text{car l'erreur absolue reste } < \frac{1}{2})$$

Utilité :

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \lim_{n \rightarrow \infty} \frac{\overbrace{\frac{F_{n+1}}{1} * \frac{1}{\sqrt{5}} \varphi^{n+1}}^{=1}}{\underbrace{\frac{F_n}{1} * \frac{1}{\sqrt{5}} \varphi^n}_{=1}} = \lim_{n \rightarrow \infty} \frac{\frac{1}{\sqrt{5}} \varphi^{n+1}}{\frac{1}{\sqrt{5}} \varphi^n} = \varphi$$

En pratique tout se passe comme si on remplaçait F_n et F_{n+1} par leur comportement asymptotique.

2. Coefficients binomiaux $\binom{2n}{n}$ et nombres de Catalan

Partons de la formule de Wallis découverte en 1655

$$\begin{aligned} \frac{\pi}{2} &= \frac{2 * 2 * 4 * 4 * 6 * 6 * 8 * 8 * 10 * 10 * \dots}{1 * 3 * 3 * 5 * 5 * 7 * 7 * 9 * 9 * 11 * \dots} \\ &= \lim_{n \rightarrow \infty} \frac{\overbrace{2 * 2 * 4 * 4 * 6 * 6 * \dots * (2n) * (2n)}^{2n \text{ facteurs}}}{1 * 3 * 3 * 5 * 5 * 7 * \dots * (2n-1) * (2n+1)} \\ &= \prod_{k=1}^{\infty} \frac{(2k)(2k)}{(2k-1)(2k+1)} \end{aligned}$$

Corollaire :

$$\begin{aligned} \frac{\pi}{2} &= \lim_{n \rightarrow \infty} \frac{\overbrace{2 * \boxed{2 * 2} * 2 * 4 * \boxed{4 * 4} * 4 * \dots * (2n) * \boxed{(2n) * (2n)} * (2n)}^{4n \text{ facteurs}}}{1 * \boxed{2 * 2} * 3 * 3 * \boxed{4 * 4} * 5 * \dots * (2n-1) * \boxed{(2n) * (2n)} * (2n+1)} \\ &= \lim_{n \rightarrow \infty} \frac{2^{4n} * (n!)^4}{((2n)!)^2 (2n+1)} \\ &= \lim_{n \rightarrow \infty} \frac{2^{4n}}{\left(\frac{(2n)!}{n!n!}\right)^2} \\ &= \lim_{n \rightarrow \infty} \frac{2^{4n}}{\binom{2n}{n}^2} = \frac{\pi}{2} \end{aligned}$$

En divisant les deux membres par $\frac{\pi}{2}$, on a :

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{\overbrace{2^{4n}}^{f(n)} * \frac{2}{\pi}}{\underbrace{\binom{2n}{n}}_{g(n)}} &= 1 \\ \Rightarrow \binom{2n}{n} &\sim \frac{2^{4n} * 2}{(2n+1) * \pi} \\ \Rightarrow \binom{2n}{n} &\sim \frac{2^{2n} * \sqrt{2}}{\sqrt{2n+1} * \sqrt{\pi}} \\ &\sim \frac{4^n}{\sqrt{n + \frac{1}{2}} * \sqrt{\pi}} \\ &\sim \frac{4^n}{\sqrt{n} * \sqrt{\pi}} \quad (\text{car } \sqrt{n + \frac{1}{2}} \sim \sqrt{n}) \\ &\sim \frac{4^n}{\sqrt{\pi n}} \end{aligned}$$

Conclusion : $\boxed{\binom{2n}{n} \sim \frac{4^n}{\sqrt{\pi n}}}$

Applications :

1) Problème de Roméo et Juliette

$$p(\text{rencontre}) = \frac{\binom{2n}{n}}{4^n} \sim \frac{4^n}{4^n \sqrt{\pi n}} \sim \frac{1}{\sqrt{\pi n}}$$

2) On lance 100 fois une pièce de monnaie. Quelle est la probabilité d'obtenir 50 piles et 50 faces ?

$$\binom{100}{50} * \left(\frac{1}{2}\right)^{50} * \left(\frac{1}{2}\right)^{50} \approx \frac{4^{50}}{\sqrt{50\pi}} * \frac{1}{2^{100}} = \frac{1}{\sqrt{50\pi}}$$

$$\frac{1}{\sqrt{50\pi}} = \frac{1}{5\sqrt{2\pi}} \approx \frac{1}{5 * 2,5} = 0,08 \quad (\sqrt{2\pi} \approx \sqrt{6,28} \approx \sqrt{6,25} = 2,5)$$

Vraie valeur = 0,0796...

3) Nombres Catalan

$$\begin{aligned} C_{n+1} &= \frac{1}{n+1} \binom{2n}{n} \\ &\sim \frac{1}{n+1} * \frac{4^n}{\sqrt{\pi n}} \quad \left(\text{or } \frac{1}{n+1} \sim \frac{1}{n} \right) \\ &\sim \frac{4^n}{n\sqrt{\pi n}} \end{aligned}$$

$$\boxed{C_{n+1} \sim \frac{4^n}{n\sqrt{\pi n}}}$$

3. Nombres harmoniques

Définition :

Le $n^{\text{ème}}$ nombre harmonique :

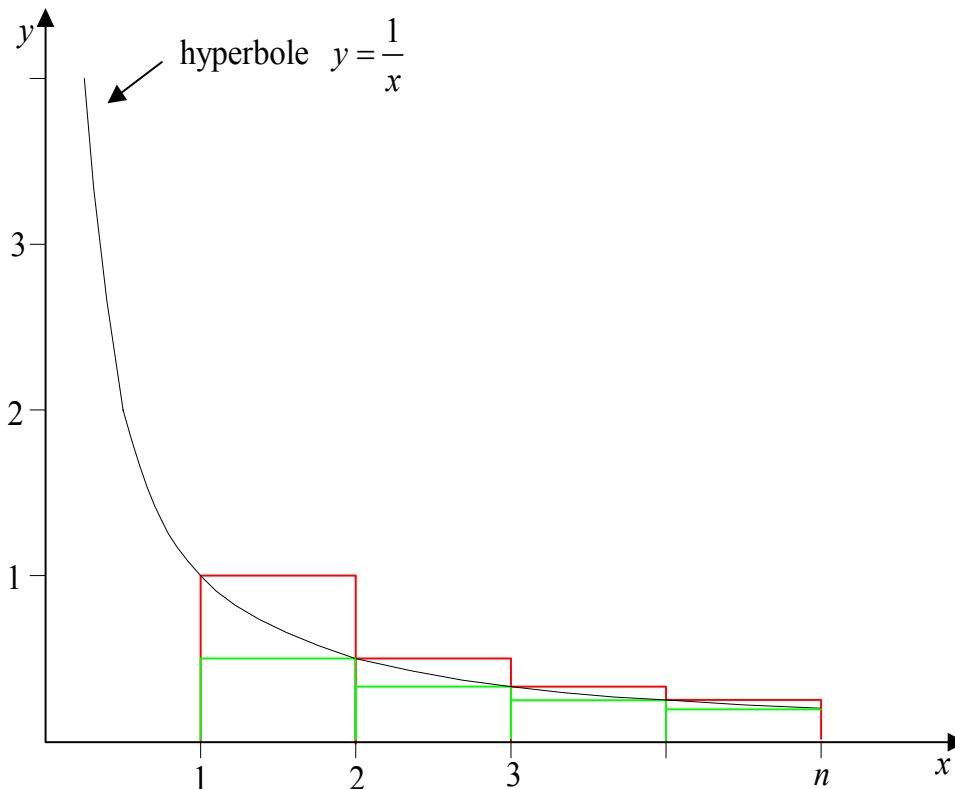
$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} = \sum_{k=1}^n \frac{1}{k}$$

$n^{\text{ème}}$ somme partielle de la série harmonique :

$$\sum_{k=1}^{\infty} \frac{1}{k} = \infty$$

Remarque importante : $H_1 < H_2 < H_3 < \dots < H_{n-1} < H_n$

Essayons de trouver le comportement asymptotique de H_n



Aire sous le **grand** escalier entre 1 et n (en rouge sur le graphe)

$$= 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n-1} = H_{n-1}$$

Aire sous l'hyperbole entre 1 et n

$$= \int_1^n \frac{1}{x} dx = \log_e n - \log_e 1 = \log_e n$$

Aire sous le **petit** escalier entre 1 et n (en vert sur le graphe)

$$= \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} = H_n - 1$$

$$\Rightarrow H_n - 1 < \log_e n < H_{n-1} \quad \forall n > 1$$

$$\text{Or } H_{n-1} < H_n \Rightarrow H_n - 1 < \log_e n < H_n \quad \forall n > 1$$

$$\boxed{\Rightarrow \log_e n < H_n < (\log_e n) + 1} \quad \forall n > 1$$

$$\Rightarrow 1 < \frac{H_n}{\log_e n} < 1 + \frac{1}{\log_e n} \quad \forall n \geq 1$$

$$\Rightarrow 1 \leq \lim_{n \rightarrow \infty} \frac{H_n}{\log_e n} \leq 1 + \overbrace{\lim_{n \rightarrow \infty} \frac{1}{\log_e n}}{=0}$$

$$\Rightarrow 1 \leq \lim_{n \rightarrow \infty} \frac{H_n}{\log_e n} \leq 1$$

$$\Rightarrow \lim_{n \rightarrow \infty} \frac{H_n}{\log_e n} = 1$$

$$\boxed{\Rightarrow H_n \sim \log_e n}$$

Calculons l'erreur absolue commise en remplaçant H_n par $\log_e n$.

Posons $a_n = H_n - \log_e n$.

On a $\boxed{a_n > 0, \forall n \geq 1}$ $\left(\begin{array}{l} \text{car } H_n > \log_e n, \forall n > 1 \\ \text{et } H_1 > \log_e 1 \end{array} \right)$

Montrons que la suite des a_n est strictement décroissante (c'est-à-dire $a_{n+1} < a_n, \forall n \geq 1$).

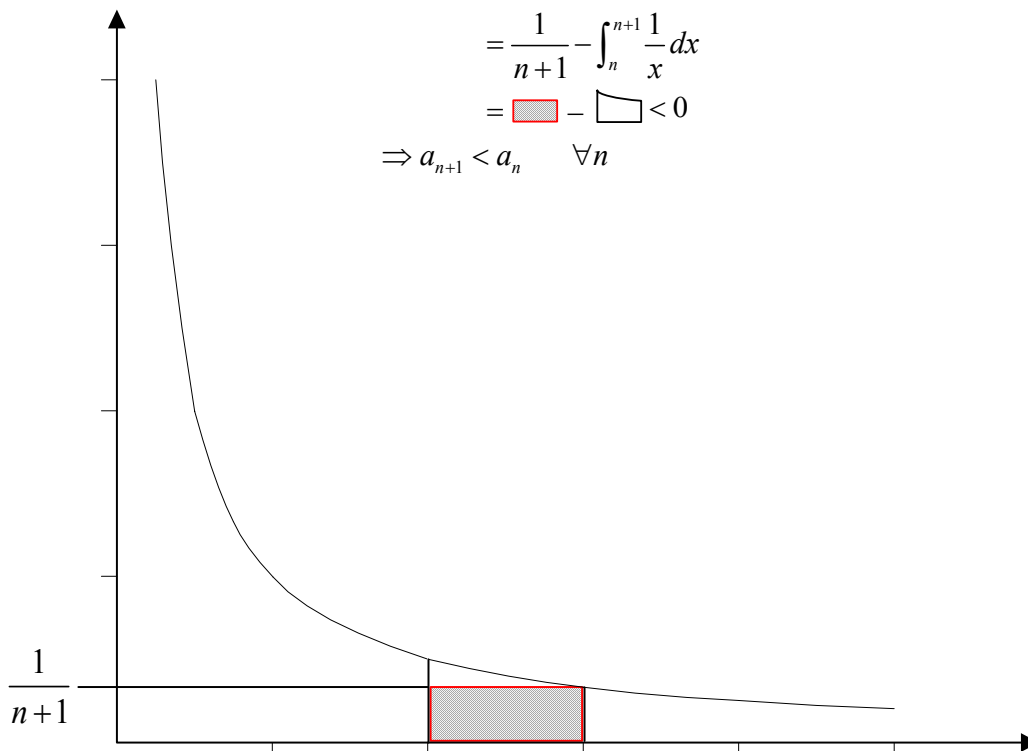
$$a_{n+1} - a_n = (H_{n+1} - \log_e(n+1)) - (H_n - \log_e n)$$

$$= (H_{n+1} - H_n) - (\log_e(n+1) - \log_e n)$$

$$= \frac{1}{n+1} - \int_n^{n+1} \frac{1}{x} dx$$

$$= \boxed{\text{rectangle}} - \boxed{\text{curved area}} < 0$$

$$\Rightarrow a_{n+1} < a_n \quad \forall n$$



On a donc : $a_1 > a_2 > a_3 > \dots > a_n > a_{n+1} > \dots > 0$

On en conclut que la suite des a_n converge.

Posons

$$\begin{aligned} \gamma &= \lim_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} (H_n - \log_e n) \\ &= \lim_{n \rightarrow \infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \log_e n \right) \end{aligned}$$

γ s'appelle la **constante d'Euler**.

On a $0 \leq \gamma < 1$.

En fait, $\gamma = 0,57721566490153286060\dots$ (γ est il rationnel ou irrationnel ? : non résolu)

Conséquence :

$$\begin{aligned} \gamma &= \lim_{n \rightarrow \infty} (H_n - \log_e n) \\ \Rightarrow 0 &= \lim_{n \rightarrow \infty} \underbrace{(H_n - (\log_e n + \gamma))}_{\varepsilon_n} \end{aligned}$$

L'erreur absolue commise en remplaçant H_n par $\log_e n + \gamma$ tend vers 0 lorsque $n \rightarrow \infty$.

On a donc :

$$\begin{aligned} H_n &= \log_e n + \gamma + \varepsilon_n \quad \text{où } \varepsilon_n \xrightarrow{n \rightarrow \infty} 0 \\ &\text{où } \varepsilon_n \text{ égale l'erreur absolue commise en remplaçant } H_n \text{ par } \log_e n + \gamma \end{aligned}$$

En particulier, on a aussi : $H_n \sim \log_e n + \gamma$

Remarque : $\log_e n + \gamma \sim \log_e n$ (car $\lim_{n \rightarrow \infty} \frac{\log_e n + \gamma}{\log_e n} = 1$)

On a donc aussi : $H_n \sim \log_e n$

On peut démontrer que :

$$\begin{aligned} H_n &= \log_e n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \varepsilon'_n \\ &\text{où } 0 < \varepsilon'_n < \frac{1}{256n^6} \end{aligned}$$

4. Comportement asymptotique de $n!$ et formule de Stirling

En 1750, de Moivre et Stirling montrent que

$$n! \underset{\substack{\text{vaut à} \\ \text{peu près}}}{\approx} \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

Au XX^{ème} siècle, on a démontré un résultat plus précis (auteur(s) inconnu(s))

Théorème :

$$\boxed{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n}} \quad \forall n \geq 1}$$

$$\Rightarrow e^{\frac{1}{12n+1}} < \frac{n!}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} < e^{\frac{1}{12n}} \quad \forall n \geq 1$$

$$\Rightarrow \lim_{n \rightarrow \infty} e^{\frac{1}{12n+1}} \leq \lim_{n \rightarrow \infty} \frac{n!}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} \leq \lim_{n \rightarrow \infty} e^{\frac{1}{12n}}$$

$$\Rightarrow 1 \leq \lim_{n \rightarrow \infty} \frac{n!}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} \leq 1$$

$$\Rightarrow \lim_{n \rightarrow \infty} \frac{n!}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} = 1$$

$$\boxed{\Rightarrow n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n}$$

Conséquence :

L'erreur **relative** commise en remplaçant $n!$ par $\sqrt{2\pi n} \left(\frac{n}{e}\right)^n$ tend vers 0 lorsque $n \rightarrow \infty$

Mais l'erreur **absolue** tend vers l'infini lorsque $n \rightarrow \infty$.

En effet :

$$\begin{aligned}
 \text{erreur absolue} &= n! - \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \\
 &> \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} - \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \\
 &= \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \left(e^{\frac{1}{12n+1}} - 1\right) \quad (\text{or } e^x \geq 1+x \quad \forall x \in \mathbb{R}) \\
 &\geq \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \left(1 + \frac{1}{12n+1} - 1\right)
 \end{aligned}$$

$$\begin{aligned}
 \Rightarrow n! - \sqrt{2\pi n} \left(\frac{n}{e}\right)^n &> \underbrace{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n}_{\xrightarrow{n \rightarrow \infty} \infty} \underbrace{\frac{1}{12n+1}}_{\xrightarrow{n \rightarrow \infty} 0} \xrightarrow{n \rightarrow \infty} \infty \\
 \Rightarrow n! - \sqrt{2\pi n} \left(\frac{n}{e}\right)^n &\xrightarrow{n \rightarrow \infty} \infty
 \end{aligned}$$

On a ainsi prouvé que $n! - \sqrt{2\pi n} \left(\frac{n}{e}\right)^n > 0$

Conséquence : $\sqrt{2\pi n} \left(\frac{n}{e}\right)^n < n!$

n	$n!$	$\sqrt{2\pi n} \left(\frac{n}{e}\right)^n$
5	120	118,008...
10	3 628 800	3 598 015,401...
20	$\approx 2,4329 * 10^{18}$	$\approx 2,4218 * 10^{18}$

5. Nombres premiers et fonction $\pi(n)$

Définition : Un nombre naturel n est dit premier s'il a exactement 2 diviseurs différents (à savoir 1 et n).

Suite des nombres premiers : 2, 3, 5, 7, 11, 13, 17, ..., 97, ..., $\underbrace{p_k}_{k^{\text{ème}} \text{ nombre premier}}$, ..., 345676543, ...

Théorème (Euclide, III^{ème} siècle av. J.C.) :

Il existe une infinité de nombres premiers.

Démonstration :

Par l'absurde. Supposons qu'il n'y en ait qu'un nombre fini, et soit

$$P = \{2, 3, 5, \dots, p_k\} \text{ l'ensemble de tous les nombres premiers}$$

$$\text{Posons } N = (2 * 3 * 5 * 7 * 11 * \dots * p_k) + 1$$

Remarque (1) : Aucun p_i ne divise N , car

$$p_i | (2 * 3 * 5 * \dots * p_i * \dots * p_k) \Rightarrow p_i \nmid (2 * 3 * 5 * \dots * p_i * \dots * p_k) + 1$$

Remarque (2) : $N \geq 2$ (trivial).

Donc N est divisible par au moins 1 nombre premier.

\Rightarrow Contradiction entre les remarques (1) et (2).

Définition : Si n est un entier > 0 ,

$$\boxed{\pi(n) = \text{le nombre de nombres premiers } \leq n}$$

Exemples :

$$\pi(10) = 4$$

$$\pi(100) = 25$$

$$\pi(p_k) = k$$

$$\pi(n) \xrightarrow{n \rightarrow \infty} \infty \quad (\text{Conséquence immédiate du théorème d'Euclide})$$

Problème : Soit $a < b$, entiers > 0 . Combien y a-t-il de nombres premiers dans l'intervalle $]a, b]$?

$$\text{Réponse : } \pi(b) - \pi(a)$$

Gauss (à 15 ans) conjecture que $\pi(n) \sim \frac{n}{\log_e n}$.

Théorème (Hadamard et de la Vallée Poussin, 1896) :

$$\boxed{\pi(n) \sim \frac{n}{\log_e n}}$$

Théorème (Rosser et Schœnfeld, 1962) :

$$\frac{n}{\log_e n - \frac{1}{2}} < \pi(n) < \frac{n}{\log_e n - \frac{3}{2}} \quad \forall n \geq 67$$

Application : Test de primalité = test permettant de répondre à la question « Un entier n donné est-il oui ou non premier ? ».

Combien de temps faudrait-il pour prouver la primalité d'un entier n en testant la non-divisibilité de n par tous les nombres premiers $\leq \sqrt{n}$? (hyp. : on en teste 10^6 par seconde)

Supposons $n \approx 10^k$.

$$\pi(\sqrt{n}) \approx \frac{\sqrt{n}}{\log_e \sqrt{n}} = \frac{10^{k/2}}{\frac{k}{2} \log_e 10}$$

$$\text{temps machine} \approx \frac{10^{k/2}}{\left(\frac{k}{2} \log_e 10\right) * 10^6} \text{ sec.}$$

$$\approx \frac{10^{k/2}}{\left(\frac{k}{2} \log_e 10\right) * 10^6 * 60 * 60 * 24 * 365} \text{ années}$$

$$\approx \frac{10^{k/2}}{k} * 2,75 \cdot 10^{-14} \text{ années}$$

$$n \approx 10^{30} \Rightarrow \text{temps machine} \approx 11 \text{ mois}$$

$$n \approx 10^{50} \Rightarrow \text{temps machine} \approx 5,5 \cdot 10^9 \text{ années}$$

$$n \approx 10^{100} \Rightarrow \text{temps machine} \approx 2,75 \cdot 10^{34} \text{ années}$$

$$\text{âge de l'univers} \approx 10^{10} \text{ années}$$

Loi de raréfaction des nombres premiers

Remarque : Si on va suffisamment loin dans \mathbb{N} , on trouve des intervalles de longueur arbitrairement grande ne contenant aucun nombre premier.

En effet, quel que soit $n \geq 2$, aucun des entiers

$$\underbrace{n!+2, n!+3, n!+4, \dots, n!+n}_{n-1 \text{ entiers consécutifs}}$$

n'est un nombre premier, car $n!+i$, ($2 \leq i \leq n$) est divisible par i et est $> i$, donc n'est pas premier.

Soit p_k le $k^{\text{ème}}$ nombre premier.

Corollaire du théorème d'Hadamard et de la Vallée Poussin : $p_k \sim k \cdot \log_e k$

Démonstration :

$$\text{On sait que } \pi(n) \sim \frac{n}{\log_e n}$$

$$\Rightarrow \lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \log_e n} = 1$$

$$\Rightarrow \lim_{n \rightarrow \infty} \frac{\pi(n) \cdot \log_e n}{n} = 1 \quad (*)$$

Prenons le \log_e des deux membres :

$$\log_e \left(\lim_{n \rightarrow \infty} \frac{\pi(n) \cdot \log_e n}{n} \right) = 0$$

Comme le \log_e est une fonction continue, on peut permuter \log_e et $\lim_{n \rightarrow \infty}$.

$$\Rightarrow \lim_{n \rightarrow \infty} \left(\log_e (\pi(n)) + \log_e (\log_e n) - \log_e n \right) = 0$$

Comme $\log_e n \xrightarrow{n \rightarrow \infty} \infty$, on a :

$$\lim_{n \rightarrow \infty} \left(\frac{\log_e (\pi(n))}{\log_e n} + \frac{\log_e (\log_e n)}{\log_e n} - 1 \right) = 0$$

Et $\frac{\log_e (\log_e n)}{\log_e n} \xrightarrow{n \rightarrow \infty} 0$ (règle de l'Hospital)

$$\Rightarrow \lim_{n \rightarrow \infty} \frac{\log_e (\pi(n))}{\log_e n} = 1 \quad (**)$$

On a donc :

$$\begin{cases} \lim_{n \rightarrow \infty} \frac{\pi(n) \cdot \log_e n}{n} = 1 & (*) \\ \lim_{n \rightarrow \infty} \frac{\log_e(\pi(n))}{\log_e n} = 1 & (**) \end{cases}$$

En multipliant (*) par (**), on obtient :

$$\boxed{\lim_{n \rightarrow \infty} \frac{\pi(n) \cdot \log_e(\pi(n))}{n} = 1}$$

En se limitant à la suite correspondant aux valeurs qui sont des nombres premiers, on trouve :

$$\lim_{k \rightarrow \infty} \frac{\pi(p_k) \cdot \log_e(\pi(p_k))}{p_k} = 1$$

Or $\pi(p_k) = k$

$$\Rightarrow \lim_{k \rightarrow \infty} \frac{k \cdot \log_e k}{p_k} = 1$$

$$\boxed{\Rightarrow p_k \sim k \cdot \log_e k}$$

□

CHAPITRE IV : Arithmétique et codage modulaire

1. Définition (Gauss, 1801) :

Si m est un entier > 0 et si $a, b \in \mathbb{Z}$, on pose

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a - b$$

se lit « a est congru à b modulo m ».

Notation simplifiée : $a \equiv b(m)$

Exemples :

1)

$$\begin{aligned} 2003 &\equiv 3 \pmod{10} \equiv -7 \pmod{10} \\ &\equiv 13 \pmod{10} \equiv -17 \pmod{10} \\ &\equiv 23 \pmod{10} \equiv -27 \pmod{10} \\ &\equiv 33 \pmod{10} \equiv \dots \end{aligned}$$

2) Numéros de comptes en banque ou de CCP : 310-0299356- $\underbrace{03}_{\substack{\text{2 chiffres} \\ \text{de contrôle}}}$

$$3100299356 \equiv \underbrace{03}_{\substack{\text{reste de la} \\ \text{division} \\ \text{par } 97}} \pmod{\underbrace{97}_{\substack{\text{plus grand} \\ \text{nombre } 1\text{er} \\ \text{à } 2 \text{ chiffres}}}}$$

2. Propriétés élémentaires

1) $a \equiv b \pmod{2} \Leftrightarrow a$ et b ont la même parité.

$$2) \boxed{a \equiv 0 \pmod{m} \Leftrightarrow m \mid a}$$

3) Tout entier $a \in \mathbb{Z}$ est $\equiv \pmod{m}$ à un et un seul des entiers $\in \{0, 1, 2, \dots, m-1\} = \underbrace{\mathbb{Z}_m}_{\substack{\text{ensemble} \\ \text{des entiers} \\ \text{modulo } m}}$

En effet, l'algorithme de division euclidienne donne :

$$a = mq + r \quad \text{avec } 0 \leq r < m.$$

Comme $a - r = m.q$, on a $a \equiv r \pmod{m}$.

« Réduire » un entier $a \in \mathbb{Z}$ modulo m , c'est le remplacer par le $r \in \mathbb{Z}_m$ correspondant.

4) La relation « $\equiv (\text{mod } m)$ » est une relation d'équivalence. En effet :

- (i) $a \equiv a (\text{mod } m)$ car $m | a - a = 0$
- (ii) $a \equiv b (\text{mod } m) \Rightarrow b \equiv a (\text{mod } m)$ car $m | a - b \Rightarrow m | b - a$
- (iii) $a \equiv b (\text{mod } m)$ et $b \equiv c (\text{mod } m) \Rightarrow a \equiv c (\text{mod } m)$

Conclusion : \equiv se comporte comme une égalité !

5) Proposition :

$$\left. \begin{array}{l} a \equiv b (\text{mod } m) \\ c \equiv d (\text{mod } m) \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \text{(i) } a + c \equiv b + d (\text{mod } m) \\ \text{(ii) } a \cdot c \equiv b \cdot d (\text{mod } m) \end{array} \right.$$

Démonstration :

- (i) exercice
- (ii) $a \cdot c - b \cdot d = a \cdot c - b \cdot c + b \cdot c - b \cdot d$

Corollaire

$$\text{(i) } a \equiv b (\text{mod } m) \Rightarrow a + c \equiv b + c (\text{mod } m) \quad \forall c \in \mathbb{Z}$$

$$\begin{aligned} \text{(ii) } a \equiv b (\text{mod } m) &\Rightarrow a \cdot c \equiv b \cdot c (\text{mod } m) && \forall c \in \mathbb{Z} \\ &\text{car } a \equiv b (\text{mod } m) \\ &\text{et } c \equiv c (\text{mod } m) \end{aligned}$$

$$\begin{aligned} \text{(iii) } a \equiv b (\text{mod } m) &\Rightarrow a^k \equiv b^k (\text{mod } m) && \forall c \in \mathbb{Z} \\ &\left. \begin{array}{l} \text{car } a \equiv b (m) \\ a \equiv b (m) \\ \dots \\ a \equiv b (m) \end{array} \right\} k \text{ fois} \end{aligned}$$

3. Applications

1) $2^{70} + 3^{70}$ est-il divisible par 13 ?

$$13 | 2^{70} + 3^{70} \Leftrightarrow 2^{70} + 3^{70} \equiv 0 (\text{mod } 13)$$

$$2^{70} \equiv ? (\text{mod } 13) \quad (*)$$

$$3^{70} \equiv ? (\text{mod } 13) \quad (**)$$

$$\Rightarrow 2^{70} + 3^{70} \equiv ? (\text{mod } 13)$$

(*)

$$2^6 \equiv 64 = 65 - 1 \equiv -1 \pmod{13}$$

$$\Rightarrow 2^{70} = 2^{66+4} = 2^{6 \cdot 11 + 4} = (2^6)^{11} \cdot 2^4$$

$$2^6 \equiv -1 \pmod{13}$$

$$(2^6)^{11} \equiv (-1)^{11} \pmod{13}$$

$$(2^6)^{11} \cdot 2^4 \equiv (-1)^{11} \cdot 16 \pmod{13} \equiv -16 \pmod{13} \equiv -3 \pmod{13}$$

$$\Rightarrow 2^{70} \equiv -3 \pmod{13}$$

(**)

$$3^3 = 27 = 26 + 1 \equiv 1 \pmod{13}$$

$$3^{70} = 3^{3 \cdot 23 + 1} = (3^3)^{23} \cdot 3 \equiv 1^{23} \cdot 3 \pmod{13} \equiv 3 \pmod{13}$$

$$\Rightarrow 3^{70} \equiv 3 \pmod{13}$$

$$\Rightarrow 2^{70} + 3^{70} \equiv -3 + 3 \pmod{13} \equiv 0 \pmod{13}$$

2) Nombres de Fermat

Nombres de la forme $F_m = 2^{2^m} + 1$.

$$F_0 = 2^{2^0} + 1 = 2 + 1 = 3 \quad \text{premier}$$

$$F_1 = 2^{2^1} + 1 = 4 + 1 = 5 \quad \text{premier}$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17 \quad \text{premier}$$

$$F_3 = \dots = 257 \quad \text{premier}$$

$$F_4 = \dots = 65537 \quad \text{premier}$$

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1$$

Euler a montré que $641 \mid 2^{32} + 1 \Rightarrow 2^{32} + 1$ pas premier !

Démonstration (Gauss) :

$$\begin{aligned} \underline{640} &\equiv -1 \pmod{641} \\ &= 5 \cdot 128 \\ &= 5 \cdot 2^7 \end{aligned}$$

$$\Rightarrow 5 \cdot 2^7 \equiv -1 \pmod{641}$$

$$\Rightarrow (5 \cdot 2^7)^4 \equiv (-1)^4 \pmod{641}$$

$$\Rightarrow 5^4 \cdot 2^{28} = 1 \pmod{641}$$

$$\begin{aligned}
\text{Or } 5^4 &= 625 = 641 - 16 \\
&\equiv -16 \pmod{641} \\
&\equiv -2^4 \pmod{641} \\
\left. \begin{aligned} 5^4 \cdot 2^{28} &\equiv 1 \pmod{641} \\ 5^4 &\equiv -2^4 \pmod{641} \end{aligned} \right\} \rightarrow -2^4 \cdot 2^{28} \equiv 1 \pmod{641} \\
\Rightarrow -2^{32} &\equiv 1 \pmod{641} \\
\Rightarrow -2^{32} + 2^{32} &\equiv 1 + 2^{32} \pmod{641} \\
\Rightarrow 0 &\equiv 2^{32} + 1 \pmod{641}
\end{aligned}$$

□

4. Rappels sur le PGCD

Si $a, b \in \mathbb{Z}$ sont deux entiers non simultanément nuls, on pose :

$$\boxed{(a, b) = \text{PGCD de } a \text{ et } b}$$

(autre notation : $\text{gcd}(a, b)$)

On a donc $(a, b) > 0$ car $1|a$ et $1|b \Rightarrow (a, b) \geq 1 > 0$

Exemples : $(49, 77) = 7$
 $(-12, 80) = 4$

Remarques : $\underset{\neq 0}{(a, 0)} = |a|$
 $(0, 0) = ?$ n'a pas de sens

5. Théorème de Bézout

Si $a, b \in \mathbb{Z}$ ne sont pas simultanément nuls, il existe $u, v \in \mathbb{Z}$ tels que $a.u + b.v = (a, b)$

Corollaire (2) du théorème de Bézout :

$$x|a.b \text{ et } (x, a) = 1 \Rightarrow x|b$$

Corollaire (5) :

Si $x, y, a \in \mathbb{Z}$, alors

$$\boxed{x|a \text{ et } y|a \text{ et } (x, y) = 1 \Rightarrow x.y|a}$$

Démonstration :

$$y|a \Rightarrow \exists \alpha \in \mathbb{Z} : a = \alpha.y$$

$$x|a \Rightarrow \left. \begin{array}{l} x|\alpha.y \\ (x, y) = 1 \end{array} \right\} \xrightarrow{\text{corollaire 2}} x|\alpha \Rightarrow \exists \beta \in \mathbb{Z} : \alpha = \beta.x$$

$$\text{Donc } a = \alpha.y = \beta.x.y \Rightarrow x.y|a$$

6. Le petit théorème de Fermat

$$\boxed{p \text{ premier} \Rightarrow p|a^p - a \quad \forall a \in \mathbb{N}}$$

Autrement dit :

$$\boxed{p \text{ premier} \Rightarrow a^p \equiv a \pmod{p} \quad \forall a \in \mathbb{N}}$$

Démonstration (Euler, 1736)

Par induction sur a .

Vrai pour $a = 0$ et $a = 1$ (trivial)

Vrai pour $a \stackrel{?}{\Rightarrow}$ vrai pour $a + 1$

Hypothèse d'induction : $p|a^p - a$

A démontrer : $p|(a+1)^p - (a+1)$

$$(1+a)^p = 1 + \binom{p}{1}a + \binom{p}{2}a^2 + \dots + \binom{p}{k}a^k + \dots + \binom{p}{p-1}a^{p-1} + a^p$$

Or, chacun des coefficients binomiaux $\binom{p}{k}$ (avec $1 \leq k \leq p-1$) est divisible par p , car :

$$\binom{p}{k} = \frac{p.(p-1).(p-2).\dots.(p-k+1)}{k.(k-1).(k-2).\dots.1}$$

Le numérateur contient un facteur p . Comme p est un nombre premier, ses seuls diviseurs sont 1 et p .

Comme le plus grand facteur du dénominateur vaut k et que $k \leq p-1$, le facteur p du numérateur ne pourra se simplifier avec aucun facteur du dénominateur.

$$\Rightarrow \binom{p}{k} \text{ est un multiple de } p, \forall k = 1, 2, \dots, p-1.$$

$$(1+a)^p = 1 + \underbrace{\binom{p}{1}a + \binom{p}{2}a^2 + \dots + \binom{p}{k}a^k + \dots + \binom{p}{p-1}a^{p-1}}_{\text{multiple de } p} + a^p$$

$$\Rightarrow (1+a)^p = 1 + m.p + a^p$$

$$\Rightarrow (1+a)^p - (1+a) = \underbrace{m.p}_{\text{multiple de } p} + \underbrace{a^p - a}_{\text{multiple de } p \text{ par l'hypothèse d'induction}}$$

$$\Rightarrow p \mid (1+a)^p - (1+a)$$

Autres formulations possibles de l'énoncé :

$$p \text{ premier} \Rightarrow p \mid a^p - a = a \cdot (a^{p-1} - 1)$$

$$\left. \begin{array}{l} p \text{ premier} \\ \text{et} \\ p \nmid a \end{array} \right\} \Rightarrow p \mid a^{p-1} - 1$$

$$\left. \begin{array}{l} p \text{ premier} \\ \text{et} \\ p \nmid a \end{array} \right\} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

Exemple : Quel est le reste de la division de 6^{740} par 19 ?

$$\text{Autrement dit : } 6^{740} \equiv ? \pmod{19}$$

$$\left. \begin{array}{l} 19 \text{ premier} \\ \text{et} \\ 19 \nmid 6 \end{array} \right\} \Rightarrow 6^{18} \equiv 1 \pmod{19}$$

$$\begin{aligned}
\Rightarrow 6^{740} &= 6^{18 \cdot 41 + 2} = (6^{18})^{41} \cdot 6^2 \\
&\equiv 1^{41} \cdot 36 \pmod{19} \\
&\equiv 36 \pmod{19} \\
&\equiv 17 \pmod{19}
\end{aligned}$$

7. Tests de primalité

Un test de primalité est un algorithme permettant de décider si, oui ou non, un entier $n > 0$ donné est un nombre premier.

7.1 Démonstration

Petit théorème de Fermat :

$$p \text{ premier} \Rightarrow a^p \equiv a \pmod{p} \quad \forall a \in \mathbb{N}$$

Ceci est équivalent à

$$\exists a \in \mathbb{N} \text{ t.q. } a^n \not\equiv a \pmod{n} \Rightarrow n \text{ pas premier}$$

Exemples :

1) $n = 91$ est-il premier ?

Choisissons $a = 2$.

$$2^{91} \equiv ? \pmod{91}$$

Rappel :

$$2^1 \equiv 2 \pmod{91}$$

$$2^2 \equiv 4 \pmod{91}$$

$$2^4 \equiv 16 \pmod{91}$$

$$2^8 = 16^2 = 256 \equiv -17 \pmod{91}$$

$$2^{16} \equiv (-17)^2 = 289 \equiv 16 \pmod{91}$$

$$2^{32} \equiv 16^2 \equiv -17 \pmod{91}$$

$$2^{64} \equiv (-17)^2 \equiv 16 \pmod{91}$$

Or, $91 = 64 + 16 + 8 + 2 + 1$

Donc :

$$\begin{aligned} 2^{91} &= 2^{64} * 2^{16} * 2^8 * 2^2 * 2^1 \\ &\equiv 16 * 16 * (-17) * 4 * 2 \pmod{91} \\ &\equiv 37 \pmod{91} \end{aligned}$$

Total : 6 élévations au carré et 4 produits pour prouver que :

$$\begin{aligned} 2^{91} &\equiv 37 \pmod{91} \\ &\not\equiv 2 \pmod{91} \end{aligned}$$

On peut donc conclure que 91 n'est pas premier, sans en connaître de facteur non trivial.

2) $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$ est-il premier ?

Choisissons $a = 2$.

$$2^{F_5} \equiv 2 \pmod{F_5}$$

\Rightarrow On ne peut pas conclure.

Essayons $a = 3$.

$$2^{F_5} \equiv 497143883 \not\equiv 3 \pmod{F_5}$$

$\Rightarrow F_5$ n'est pas premier.

7.2 Remarque :

La réciproque du petit théorème de Fermat est fausse.

$$\boxed{a^n \equiv a \pmod{n}, \forall a \in \mathbb{N} \not\Rightarrow n \text{ premier}, n > 1}$$

Le plus petit contre-exemple est $n = 561 = 3 * 11 * 17$ (pas premier)

Mais on a $a^{561} \equiv a \pmod{561}, \forall a \in \mathbb{N}$

Démonstration :

Il suffit de démontrer que

$$561 \mid \underbrace{a^{561} - a}_{=a(a^{560}-1)} \quad \forall a \in \mathbb{N}$$

Ceci revient à montrer que :

$$1) 3|a(a^{560} - 1) \quad \forall a$$

$$2) 7|a(a^{560} - 1) \quad \forall a$$

$$3) 11|a(a^{560} - 1) \quad \forall a$$

1) Montrons que $3|a(a^{560} - 1) \quad \forall a$

$$3|a \Rightarrow 3|a.(a^{560} - 1) \Rightarrow \text{OK}$$

ou

$$3 \nmid a \stackrel{\text{Fermat}}{\Rightarrow} a^2 \equiv 1(3) \Rightarrow (a^2)^{280} \equiv 1^{280}(3)$$

$$\Rightarrow a^{560} \equiv 1(3)$$

$$\Rightarrow 3|a^{560} - 1$$

$$\Rightarrow 3|a(a^{560} - 1), \forall a \Rightarrow \text{OK}$$

2) Démonstration semblable.

3) Démonstration semblable.

On sait depuis 1992 qu'il existe une infinité d'entiers n non premiers, mais tels que

$$a^n \equiv a \pmod{n} \quad \forall a \in \mathbb{N}$$

Remarque :

En perfectionnant ce test, trois mathématiciens indiens (Agrawal, Kayal et Saxena) ont prouvé qu'on peut tester la primalité d'un entier $n > 0$ donné, en un temps polynomial (algorithme en $O((\log n)^{12})$).

8. Congruences linéaires

Les congruences du type

$$a.x \equiv b \pmod{m}$$

sont appelées congruences linéaires ($x \in \mathbb{Z}_m$ est l'inconnue) et sont utilisées dans beaucoup d'applications concrètes.

On a vu que : $x \equiv y \pmod{m} \Rightarrow a.x \equiv a.y \pmod{m}, \forall a \in \mathbb{Z}$

Attention : La réciproque n'est pas vraie (même si $a \not\equiv 0 \pmod{m}$).

$$\left. \begin{array}{l} a.x \equiv a.y \pmod{m} \\ a \not\equiv 0 \pmod{m} \end{array} \right\} \not\Rightarrow x \equiv y \pmod{m}$$

8.1 Théorème

$$\boxed{a.x \equiv a.y \pmod{m} \Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}}$$

Remarque :

C'est vrai même si $a = 0$ car :

$$(a, m) = (0, m) = m$$

donc :

$$\frac{m}{(a, m)} = \frac{m}{m} = 1$$

et on a bien :

$$x \equiv y \pmod{1}$$

$$a.x \equiv a.y \pmod{m}$$

$$\Rightarrow m \mid a.x - a.y$$

$$\Rightarrow m \mid a(x - y)$$

Posons $(a, m) = d$

$$\Rightarrow \left(\frac{a}{d}\right) \text{ et } \left(\frac{m}{d}\right) \text{ sont des entiers et } \left(\frac{a}{d}, \frac{m}{d}\right) = 1$$

De plus, $m \mid a(x-y)$

$$\Rightarrow \frac{m}{d} \mid \frac{a}{d}(x-y)$$

$$\text{On a donc : } \left. \begin{array}{l} \frac{m}{d} \mid \frac{a}{d}(x-y) \\ \left(\frac{a}{d}, \frac{m}{d}\right) = 1 \end{array} \right\} \begin{array}{l} \text{corollaire 2} \\ \Rightarrow \frac{m}{d} \mid (x-y) \Rightarrow x \equiv y \pmod{\frac{m}{d}} \end{array}$$

$$\Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$$

8.2 Corollaire

$$\left. \begin{array}{l} a.x \equiv a.y \pmod{m} \\ \text{et} \\ (a, m) = 1 \end{array} \right\} \Rightarrow x \equiv y \pmod{m}$$

8.3 Exemple

$$12x \equiv 16 \pmod{80}$$

On cherche tous les $x \in \mathbb{Z}_{80} = \{0, 1, 2, \dots, 79\}$ vérifiant la congruence $\underline{4}.3x \equiv \underline{4}.4 \pmod{80}$.

$$\text{On a } (4, 80) = 4$$

$$\Rightarrow 3x \equiv 4 \pmod{\frac{80}{4}}$$

$$\Rightarrow 3x \equiv 4 \pmod{20}$$

$$\Rightarrow 3x \equiv 24 \pmod{20}$$

$$\Rightarrow \underline{3}x \equiv \underline{3}.8 \pmod{20}$$

$$\text{On a } (3, 20) = 1$$

$$\text{Donc } \boxed{x \equiv 8 \pmod{20}}$$

$$\Rightarrow x \equiv 8, 28, 48, 68 \pmod{80}$$

Conclusion : La congruence $12x \equiv 16 \pmod{80}$ possède 4 solutions $\pmod{80}$.

9. Théorème de Gauss (1801)

La congruence linéaire

$$a.x \equiv b \pmod{m}$$

possède une solution si et seulement si $(a, m) \mid b$.

Si cette condition est satisfaite, il y a exactement (a, m) solutions distinctes \pmod{m}

Exemples

1) $36x \equiv 8 \pmod{102}$
 $(36, 102) = 6 \nmid 8 \Rightarrow$ pas de solution.

2) $141x \equiv 438 \pmod{1200}$
 $(141, 1200) = 3 \mid 438$
 \Rightarrow Il y a exactement 3 solutions $\pmod{1200}$.
 $\Rightarrow 3 * 47x \equiv 3 * 146 \pmod{1200}$
 $\Rightarrow 47x \equiv 146 \pmod{400}$

Et on a $(47, 400) = 1$
 \Rightarrow Il y a une seule solution $\pmod{400}$

Algorithme de résolution :

$$(47, 400) = 1 \stackrel{\text{Bézout}}{\Rightarrow} \exists x, y \in \mathbb{Z} : 47x + 400y = 1$$

Si on arrive à trouver un tel x et un tel y , alors en réduisant $\pmod{400}$, on a :

$$47x \equiv 1 \pmod{400}$$

$$47 * (146x) \equiv 146 \pmod{400}$$

Cherchons x et y tels que $47x + 400y = 1$.

Astuce :

$$47 * 0 + 400 * 1 = 400 \quad L_1$$

$$47 * 1 + 400 * 0 = 47 \quad L_2$$

x	y	$47x + 400y$	
0	1	400	L_1
1	0	47	L_2
-8	1	24	$L_3 = L_1 - 8L_2$
-17	2	1	$L_4 = 2L_3 - L_2$

$$\Rightarrow 47 * (-17) + 400 * 2 = 1$$

$$\downarrow \times (\text{mod } 400)$$

$$\Rightarrow 47 * (-17) \equiv 1 (\text{mod } 400)$$

$$\Rightarrow 47 * \underbrace{(-17) * 146}_{=x} \equiv 146 (\text{mod } 400)$$

$$\Rightarrow x \equiv -17 * 146 (\text{mod } 400)$$

$$\equiv -2482 (\text{mod } 400)$$

$$\equiv -82 (\text{mod } 400)$$

$$\Rightarrow x \equiv 318 (\text{mod } 400)$$

$$\Rightarrow x \equiv 318, 718, 1118 (\text{mod } 1200)$$

Table des matières.

CHAPITRE I : PROBLÈMES DE DÉNOMBREMENT	3
1. COEFFICIENTS BINOMIAUX	3
1.1 Définition:	3
1.2 Cas limites:	3
1.3 Propriétés:	3
1.4 Quelques exemples :	5
1.5 Récurrence additive et triangle de Pascal :	9
1.6 Problème de Roméo et Juliette	13
1.7 Formule dite « du binôme de Newton »	15
2. FORMULE D'INCLUSION – EXCLUSION	17
2.1 Introduction.	17
2.2 Théorème.	17
2.3 Démonstration.....	18
2.4 Applications.....	18
2.4.1 Dérangement de n objets.	18
2.4.2 Fonction φ d'Euler.....	20
2.4.3 Applications, injections et surjection.....	21
2.4.4 Partitions d'un ensemble.....	23
2.4.4.1 Les nombres de Stirling de 2 ^{ème} espèce.....	24
2.4.5 Permutation de n objets en k cycles.....	25
2.4.5.1 Les nombres de Stirling de 1 ^{ère} espèce :	25
3. FONCTIONS GÉNÉRATRICES, NOMBRES DE FIBONACCI, ET NOMBRES DE CATALAN	28
3.1 Nombres de Fibonacci	28
3.2 Nombres de Catalan.....	31
3.3 En résumé	36
3.4 Nombres de Fibonacci et nombre d'or.....	37
CHAPITRE II : RELATIONS DE RÉCURRENCE	41
1. RÉCURRENCES LINÉAIRES HOMOGÈNES À COEFFICIENTS CONSTANTS	41
1.1 Définition :	41
1.2 Théorème :	41
2. RÉCURRENCES LINÉAIRES NON-HOMOGÈNES À COEFFICIENTS CONSTANTS	49
3. COMPLÉMENTS SUR LES NOMBRES DE CATALAN	52
3.1 Problème d'André sur les chemins minimaux.....	52
3.2 Triangulations d'un n-gone convexe	55
3.3 Arbre binaire de n sommets.....	56
CHAPITRE III : COMPORTEMENTS ASYMPTOTIQUES	58
1. NOMBRES DE FIBONACCI	59
2. COEFFICIENTS BINOMIAUX $\binom{2n}{n}$ ET NOMBRES DE CATALAN	60
3. NOMBRES HARMONIQUES	62
4. COMPORTEMENT ASYMPTOTIQUE DE $n!$ ET FORMULE DE STIRLING	66
5. NOMBRES PREMIERS ET FONCTION $\pi(N)$	68
Loi de raréfaction des nombres premiers.....	70
CHAPITRE IV : ARITHMÉTIQUE ET CODAGE MODULAIRE	72
1. DÉFINITION (GAUSS, 1801) :	72
2. PROPRIÉTÉS ÉLÉMENTAIRES	72
3. APPLICATIONS	73
4. RAPPELS SUR LE PGCD	75

5.	THÉORÈME DE BÉZOUT.....	75
6.	LE PETIT THÉORÈME DE FERMAT.....	76
7.	TESTS DE PRIMALITÉ.....	78
7.1	<i>Démonstration</i>	78
7.2	<i>Remarque</i> :.....	79
8.	CONGRUENCES LINÉAIRES.....	81
8.1	<i>Théorème</i>	81
8.2	<i>Corollaire</i>	82
8.3	<i>Exemple</i>	82
9.	THÉORÈME DE GAUSS (1801).....	83