FRANCQUEVILLE Martin

190 : Méthodes combinatoires, problèmes de dénombrement

Réf : De Biasi, Mathématiques pour le CAPES et l'agrégation tome I et III
Risler-Boyer, Algèbre pour la L3
Calder Germoni tome 1 (DVLP 1)
Bernis (DVLP 2)

I Quelques outils de dénombrement

1) Définitions et propriétés de base

prop 1 : (formule du crible) : $E_1, \dots, E_n$ n ensembles finis ; alors on a $\#\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} \sum_{(a_1,\dots,a_k)\in[1,n]} (-1)^{k+1} \bigcap_{i=1}^{k} E_i$

prop : $\# S_n = n!$

prop 2 : Soient E, F deux ensembles finis, $\#E = n$, $\#F = p$ alors $\#\{f : E \to F\} = p^n$

ex : nombre de parties d'un ensemble à n éléments est 2^n.

déf 3 : Soit E ensemble à n éléments, $1 \le p \le n$ un arrangement de p éléments de E est un p-uplet $(e_1, \dots, e_p) \in E^p$, $\forall i,j \in [1,p]$, $e_i \neq e_j$ si $i \neq j$.

prop 4 : Le nombre d'arrangements à p éléments d'un ensemble E, $\#E = n$, est $\frac{n!}{(n-p)!}$

ex 5 tirage de p boules dans une urne contenant n boules numérotées de 1 à n, où l'ordre de tirage a une importance.

2) Coefficients binomiaux

déf 6 : On appelle coefficients binomiaux les nombres de parties à k éléments d'un ensemble à n éléments, et on les note $\binom{n}{k}$, pour tout $n, k \in \mathbb{N}$.

prop 7 : $\forall n, k \in \mathbb{N}$, $k \le n$, on a $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
$k > n$, $\binom{n}{k} = 0$

prop : On a $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

prop 7 : Soient $n, k \in \mathbb{N}$, $n \ge k$:
* $\binom{n}{k} = \binom{n}{n-k}$; * $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ pour $k \ge 1$
* $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$; * $\binom{n}{k} = \frac{n}{n-k}\binom{n-1}{k}$
$k \ge 1$

cor 8 : Soient $n \in \mathbb{N}$, p premier, $p > n$, alors : p divise $\binom{p}{n}$.

prop : formule du binôme : $\forall a, b \in A$ anneau tel que $ab = ba$: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

application 9 : $\mathbb{F}_q$ corps de caractéristique $p > 0$, alors $\mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^p$ est un morphisme de corps.

application 10 : Soit $P = \left(\binom{i-1}{j-1}\right)_{1 \le i,j \le n}$ la matrice de Pascal son inverse est donnée par : $P^{-1} = \left((-1)^{i-j}\binom{i-1}{j-1}\right)_{1 \le i,j \le n}$

application 11 : Le nombre de permutations sans points fixes est $d_n = n! \sum_{0 \le k \le n} \frac{(-1)^k}{k!}$

prop 12 $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2 = \left(\sum_{k=1}^{n} k\right)^2$ (cf annexe schéma 1)

II Liens avec la théorie des groupes et des corps finis

1) Actions de groupe

~~[illegible]~~

déf 13 : Soient G un groupe, X un ensemble ; une action de G sur X est une application $G \times X \to X$, $(g, x) \mapsto g \cdot x$

telle que 1) $\forall g, g' \in G, \forall x \in X,\ g\cdot(g'\cdot x) = gg'\cdot x$

2) $\forall x \in X,\ 1\cdot x = x$

déf 14: G opère transitivement sur X si
$\forall x \in X, \forall y \in X, \exists g \in G,\ g\cdot x = y$

G opère fidèlement si ~~$\forall x$~~ pour $g \in G$, $\forall x \in X,\ g\cdot x = x$ implique $g = 1$.

déf 15: Si G opère sur X, pour $x \in Hx$, on définit le stabilisateur de x comme le sous-groupe de G H_x tel que ~~$\forall x \in X$~~ $\forall g \in H_x,\ g\cdot x = x$. On définit aussi l'orbite de x notée $\omega(x)$ l'ensemble $\{g\cdot x \mid g \in G\}$

prop 16: Pour $x \in X$, en notant G/H_x l'ensemble des classes à gauche, on a que $G/H_x \to \omega(x)$, $\bar{g} \mapsto g\cdot x$ est une bijection,
d'où $\#\omega(x) = \frac{\#G}{\#H_x}$ si G est fini

prop 17 (équation aux classes) Soit G un groupe fini, alors: $\#G = \#Z(G) + \sum_{i=1}^{n} \#\omega_i$ où les ω_i sont les orbites non triviales des éléments de G sous l'action de G par ~~automorphisme~~ conjugaison

application 18: Soit p un nombre premier, si G est un p-groupe, alors son centre est non trivial
Si $\#G = p^2$, alors G est abélien

2) Corps finis (p nombre premier, $n \in \mathbb{N}^*$, $q = p^n$)

prop 19: Pour p premier et $q = p^n$, alors $\#GL_n(\mathbb{F}_q) = \prod_{i=0}^{n-1}(q^n - q^i)$

prop 20: Si φ est l'indicatrice d'Euler, alors $\forall n \in \mathbb{N}$, on a: $n = \sum_{d \mid n} \varphi(d)$

application 21: Pour p premier et $q = p^n$, $\mathbb{F}_q^*$ est cyclique.

prop: Pour $p > 2$, $\#\mathbb{F}_q^{*2} = \{x^2 \mid x \in \mathbb{F}_q^*\}$ est de cardinal ~~$\frac{p-1}{2}$~~ $\frac{q-1}{2}$

prop 22: Soient $a, b \in \mathbb{F}_q^*$, alors l'équation $ax^2 + by^2 = 1$ admet au moins une solution (x, y)

application 23: Toute matrice de forme quadratique non dégénérée sur $\mathbb{F}_q^n$ ~~est~~ est congruente à l'une de ces deux matrices: I_n ou $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$ où $a \notin \mathbb{F}_q^{*2}$

déf 24: On appelle groupe projectif linéaire d'un module $PGL_n(\mathbb{F}_q)$ le groupe $\frac{GL_n(\mathbb{F}_q)}{Z(GL_n(\mathbb{F}_q))}$

prop 25: $Z(GL_n(\mathbb{F}_q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q\}$

prop 26: $\#PGL_n(\mathbb{F}_q) = \prod_{i=1}^{n}(q^n - q^i)$

3) La loi de réciprocité quadratique (p et q premiers)

prop 27: Si $p > 2$, alors: $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$

définition 28: On appelle symbole de Legendre ~~d'un~~ de $x \in \mathbb{F}_p^*$
~~noté $\left(\frac{x}{p}\right)$, pour $x \in \mathbb{F}_p^*$, $x^{\frac{p-1}{2}}$ la fonction~~
$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$

DVLP 1

Lemme 29 : Soit $a \in \mathbb{F}_p^*$, alors on a $\#\{x \in \mathbb{F}_p \mid ax^2 = 1\} = 1 + \left(\frac{a}{p}\right)$

Théorème 30 : (loi de réciprocité quadratique) On a la relation
$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ si $p > 2$ et $q > 2$

Remarque 31 : Etant donné que le symbole de Legendre est multiplicatif avec la proposition suivante, on peut toujours vérifier si un entier k est un carré ou non modulo p :

Prop 32 : Si $p > 2$, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

III Séries génératrices

Déf 33 : Soit $(a_n)_{n \in \mathbb{N}}$ une suite de complexes. On appelle série génératrice exponentielle la série entière :
$S = \sum_{n \geq 0} \frac{a_n}{n!} z^n$ pour $z \in \mathbb{C}$

Remarque : Trouver une autre expression en série entière de S permet de donner les coefficients a_n

Prop 34 : Une autre manière de calculer le nombre de permutations sans point fixe en posant $S(z) = \sum \frac{d_n}{n!} z^n$

DVLP 2

Th 35 : (nombres de Bell) On note, pour $n \in \mathbb{N}$, B_n le nombre de partitions de l'ensemble $\{1, \dots, n\}$. On a :
$B_n = \frac{1}{e} \sum_{k=0}^{+\infty} \frac{k^n}{k!}$

Déf 36 : (nombres de Catalan) On note, pour $n \in \mathbb{N}$, C_n le nombre de chemin possible du point $(0,0)$ au point (n,n) sans passer sous la diagonale $[(0,0),(n,n)]$ (schéma 2), avec par convention $C_0 = 1$, en se déplaçant soit d'une case vers le haut, soit d'une case vers la droite. On calcule C_n de deux manières différentes :

* En remarquant que $\forall n \in \mathbb{N}^*$, $C_n = \sum_{k=1}^{n} C_{k-1} C_{n-k}$ (schéma 3) et en étudiant la série entière $f(x) = \sum_{n=0}^{+\infty} C_n x^n$

* En remarquant qu'un chemin passant sous la diagonale correspond à un unique chemin de $(0,0)$ à $(n+1, n-1)$, et réciproquement. Ainsi, le nombre C_n correspond à la différence entre le nombre de chemins de $(0,0)$ à (n,n) et le nombre de chemins de $(0,0)$ à $(n+1, n-1)$, d'où $C_n = \binom{2n}{n} - \binom{2n}{n+1}$

* en ~~appliquant~~ symétrisant la "suite" du chemin par rapport à la sous diagonale $[(1,0),(n,n-1)]$ (schéma 4)

(4)

Schéma 1 :

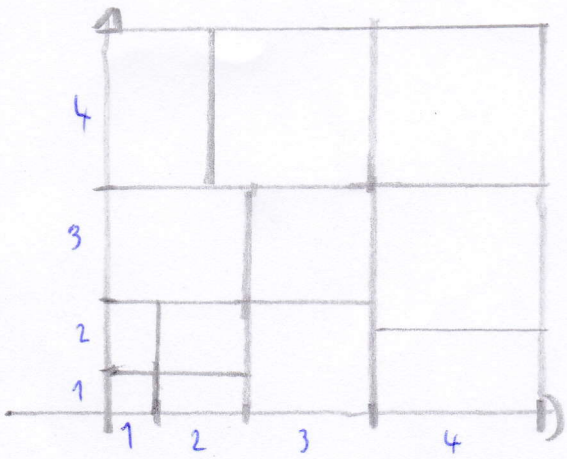


Illustration de l'égalité

$$\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$$

Schéma 2 :

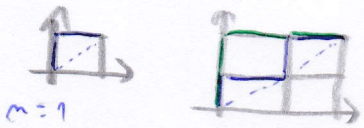
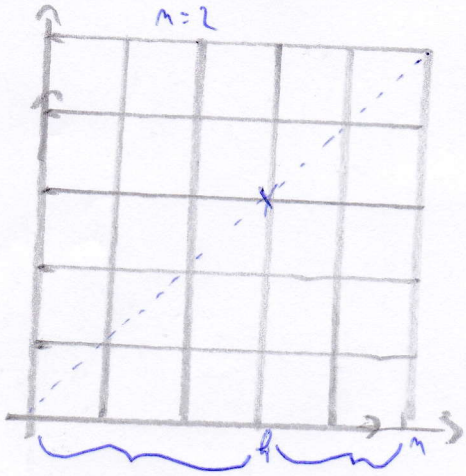


Schéma 3 :

γ un chemin valide



C_{k-1} possibles $\quad C_{n-k}$ possibles

où $k = \inf\{i \geq 0 \mid (i,i) \in \gamma\}$

Schéma 4 :

γ un mauvais chemin