Combinatoire

Yes, counting is hard. We may as well get that out and understood right at the top. « Counting » is short for « enumerative combinatorics », which certainly doesn't sound easy.

George E. Martin, *Counting : the art of enumerative combinatorics.*

1. Dénombrements « élémentaires »

Les premiers résultats de cette section se trouvent par exemple dans le chapitre *Probabilités discrètes et dénombrements* de [FF] (voir aussi [Mar] pour varier les exemples).

— Si $X = \{x_1, \dots, x_m\}$ est un ensemble fini à m éléments et $Y = \{y_1, \dots, y_n\}$ un ensemble fini à n éléments, il y a n^m applications $f\colon X \to Y$. En effet, il y a n choix possibles pour $f(x_i)$ pour chaque $i \in \{1, \dots, m\}$.
Parmi celles-ci, seules $\frac{n!}{(n-m)!}$ sont injectives (n choix possibles pour $f(x_1)$, puis $n-1$ choix possibles pour $f(x_2)$ car on ne peut pas prendre la même image si l'on veut que f soit injective, et ainsi de suite).

— Nombre de parties d'un ensemble fini : avec les notations ci-dessus, $\mathscr{P}(X)$ (l'ensemble des parties de X) est de cardinal $2^{|X|} = 2^m$. En effet, $\mathscr{P}(X)$ est en bijection avec l'ensemble des fonctions de X vers $\{0,1\}$ (en associant à une partie sa fonction indicatrice).

— Le nombre de parties à k éléments d'un ensemble à n éléments est noté $\binom{n}{k}$ et il est égal à $\frac{n!}{k!(n-k)!}$. En effet, soit X un ensemble à n éléments et soit E un ensemble à k éléments. Notons $\mathscr{P}_k(X)$ l'ensemble des parties de X à k éléments. On a une surjection

$$\begin{array}{ccc} \{f\colon E \to X \text{ telle que } f \text{ est injective}\} & \to & \mathscr{P}_k(X) \\ f & \mapsto & f(E) \end{array}$$

et chaque partie à l'arrivée possède $k!$ antécédents (car une fois que l'on fixe l'image de f, on est juste en train de compter les bijections d'un ensemble à k éléments dans un ensemble à k éléments). Donc $\frac{n!}{(n-k)!} = k!|\mathscr{P}_k(X)|$.

— Lemme des tiroirs et applications :

▷ L'agglomération rennaise compte 360 000 habitants, et personne n'a plus de 200 000 cheveux sur la tête. Ainsi, vous croiserez peut-être à Rennes une personne ayant exactement le même nombre de cheveux que vous !

▷ En fait, si l'on suppose qu'il y a en France 68 millions d'habitants, une des variantes du lemme des tiroirs nous dit qu'il y a au moins 340 personnes en France qui ont le même nombre de cheveux. Précisément : *si n objets sont répartis dans m récipients, l'un des récipients continent au moins n/m objets.*

▷ Démonstration du théorème de Bolzano-Weierstrass réel par dichotomie

▷ Théorème d'approximation de Dirichlet : si $\alpha \in \mathbf{R}$ et $N \in \mathbf{N}^*$, il existe $(p,q) \in \mathbf{Z}^2$ avec $1 \leqslant q \leqslant N$ et tels que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN}$. Un corollaire est que la *mesure d'irrationalité* d'un irrationnel est au moins égale à 2 (voir exercice 5.1).

▷ Pour celles et ceux qui ont fait un peu d'informatique : le *pumping lemma* en théorie des langages est une jolie application du lemme des tiroirs.

▷ Pour encore plus d'applications combinatoires : [Mar].

— Formule du crible [CP] : Si $A_1, \dots, A_n$ sont des parties finies d'un ensemble E, on a

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\emptyset \neq J \subseteq \{1,\dots,n\}} (-1)^{|J|-1} \left|\bigcap_{j \in J} A_j\right|$$

Une démonstration sympa : soit $A := \bigcup_{i=1}^{n} A_i$. La fonction

$$\prod_{i=1}^{n}(1 - \mathbb{1}_{A_i})$$

est nulle sur A, mais en développant le produit, elle est égale à

$$1 + \sum_{\emptyset \neq J \subseteq \{1,\dots,n\}} (-1)^{|J|} \prod_{j \in J} \mathbb{1}_{A_j} = 1 + \sum_{\emptyset \neq J \subseteq \{1,\dots,n\}} (-1)^{|J|} \mathbb{1}_{\bigcap_{j \in J} A_j}$$

Donc pour tout $x \in A$,

$$0 = 1 + \sum_{\emptyset \neq J \subseteq \{1,\dots,n\}} (-1)^{|J|} \mathbb{1}_{\bigcap_{j \in J} A_j}(x)$$

c'est-à-dire

$$1 = \sum_{\emptyset \neq J \subseteq \{1,\dots,n\}} (-1)^{|J|-1} \mathbb{1}_{\bigcap_{j \in J} A_j}(x).$$

On obtient la conclusion en sommant sur $x \in A$. □

Applications :

- ▷ Si $\alpha, \beta \in \mathbf{F}_q^\times$ la forme quadratique

$$\begin{array}{ccc} \mathbf{F}_q^2 & \to & \mathbf{F}_q \\ (x,y) & \mapsto & \alpha x^2 + \beta y^2 \end{array}$$

  représente 1. C'est une étape clef de la réduction des formes quadratiques dans le cas où le corps de base est fini. Voir [Goz, CG] entre autres.

- ▷ Nombre de surjections $f : X \to Y$. Le nombre de surjections d'un ensemble fini à m éléments vers un ensemble fini à n éléments est

$$\sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} i^m.$$

  voir [CP, Chap. IV].

- ▷ Nombre de permutations sans point fixe [CP, Chap. IV]. Nous le verrons par une autre méthode dans la section 3.

- ▷ Première étape du développement sur la proportion de couples d'entiers premiers entre eux (voir la section suivante).

2. Formule d'inversion de Möbius

- — Produit de convolution des suites et définition de la fonction μ : [Goz]
- — Formule d'inversion : [Goz]
- — Séries de Dirichlet et convolution : [Ten, Apo]
- — Applications :
  - ▷ Indicatrice d'Euler
  - ▷ Proportion de couples d'entiers premiers entre eux : [FGNa]
  - ▷ Nombre d'irréductibles de $\mathbf{F}_q[X]$: [Goz]

3. Utilisation de séries génératrices

3.1. Prérequis sur les séries formelles

[Ber] : étant donné un anneau commutatif A, définition de l'anneau $A[[X]]$ qui n'est rien de plus que l'ensemble des suites à valeurs dans A muni d'opérations compatibles avec la notation sous forme de séries. Éléments inversibles de cet anneau.

3.2. Mise en jambe

— [Mar] : on dispose de 5 balles rouges, 6 balles vertes et 7 balles bleues. Combien y-a-t'il de façons de donner 9 balles à Alice et 9 balles à Bob de sorte qu'ils aient chacun au moins une balle de chaque couleur ?
▷ Il s'agit du coefficient de X^9 lorsqu'on développe le polynôme

$$(X+X^2+X^3+X^4)(X+X^2+X^3+X^4+X^5)(X+X^2+X^3+X^4+X^5+X^6).$$

— On note $a(n)$ le nombre de manières de payer n euros avec des pièces de 1 et 2 euros. Montrer que dans $\mathbf{Q}[[X]]$ on a l'égalité suivante :

$$\sum_{n=0}^{+\infty} a(n)X^n = \frac{1}{(1-X^2)(1-X)}.$$

Voir l'exercice 5.4 pour la conclusion.

3.3. Nombre de partitions d'un entier

— Définition d'une composition de n et d'une partition de n.
— Théorème d'Euler sur les partitions en parts distinctes : [CG] dans l'annexe concernant les partitions à la fin du chapitre sur la réduction.
— Diagrammes de Young et lien avec la réduction de Jordan des endomorphismes nilpotents : [MM]. Voir l'exercice 5.7.

3.4. Suites satisfaisant une relation de récurrence

— La grande idée : une relation de récurrence sur la suite se traduit en une équation satisfaite par sa série génératrice.
— L'exemple du dénombrement des permutations sans points fixes [Ber] (aussi appelées dérangements)
— D'autres idées : la suite de Fibonacci (exercice 5.5), les nombres de Bell [FGNa] (B_n est le nombre de partitions de l'ensemble $\{1,\dots,n\}$), les nombres de Catalan (exercice 5.6).

4. Utilisation d'actions de groupes

4.1. Prérequis

Si un groupe fini G agit sur un ensemble fini X et si $(g,x) \in G \times X$, on note :
— $Gx := \{g.x,\ g \in G\}$ l'orbite du point x sous l'action de G.
— $\mathrm{Stab}_G(x) := \{g \in G \mid g.x = x\}$ le stabilisateur de x dans G.
— $X^g := \{x \in X \mid g.x = x\}$ l'ensemble des points de X fixés par g.

Pour nos questions de dénombrement, nous aurons besoin des deux faits suivants :
— **Relation orbite-stabilisateur** : pour un $x \in X$ fixé, la considération de l'application

$$\begin{array}{ccc} G & \to & Gx \\ g & \mapsto & g.x \end{array}$$

permet de montrer que $|G| = |Gx|.|\mathrm{Stab}_G(x)|$.
— **Formule de Burnside** : si on note Ω l'ensemble des orbites pour l'action de G sur X, on a

$$|\Omega| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

« le nombre d'orbites est la moyenne du nombre de points fixés par chaque élément du groupe ». Cette formule se démontre en partant de l'égalité

$$\sum_{x\in X}\sum_{g\in G}\mathbb{1}_{g.x=x} = \sum_{g\in G}\sum_{x\in X}\mathbb{1}_{g.x=x},$$

c'est-à-dire en comptant de deux manières différentes le nombre de couples (g,x) qui satisfont l'équation $g.x = x$.

4.2. Dénombrement sur les corps finis

— Le dénombrement des matrices diagonalisables dans $\mathrm{M}_n(\mathbf{F}_q)$, qui utilise l'action de $\mathrm{GL}_n(\mathbf{F}_q)$ (voir le complément sur les corps finis).

— Le nombre de points de $\mathbf{P}^2(\mathbf{F}_q)$ et le jeu Dobble, qui utilise l'action de $\mathbf{F}_q^\times$ sur $\mathbf{F}_q^3 \setminus \{0\}$.

4.3. Dénombrement de coloriages

— Nombre de façons réellement différentes de colorier les arêtes d'un octogone avec 4 arêtes d'une couleur et 4 arêtes d'une autre couleur. Le groupe qui agit est le groupe diédral D_8.

— Un développement classique : coloriages du cube. Le groupe qui agit est le groupe des isométries positives du cube, qui est isomorphe au groupe symétrique $\mathfrak{S}_4$ via l'action sur les 4 grandes diagonales.

5. Exercices

Exercice 5.1. *Mesure d'irrationalité*

On appelle mesure d'irrationalité d'un réel α la borne supérieure de l'ensemble des réels μ tels qu'il existe une infinité de couples $(p,q) \in \mathbf{Z} \times \mathbf{N}^*$ tels que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\mu}$.
Soit $\alpha \in \mathbf{R} \setminus \mathbf{Q}$. On introduit

$$C := \left\{(p,q) \in \mathbf{Z} \times \mathbf{N}^* \text{ tels que } \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}\right\} \text{ et } F := \left\{\frac{p}{q},\ (p,q) \in C\right\}.$$

1. Déduire du théorème d'approximation de Dirichlet que $d(\alpha, F) = 0$.
2. En déduire que F est infini.
3. Conclure que la mesure d'irrationalité de α est au moins égale à 2.

Solution. https://fr.wikiversity.org/wiki/Introduction_%C3%A0_la_th%C3%A9orie_des_nombres/Exercices/Approximation_diophantienne_et_fractions_continues □

Remarque : cette définition peut sembler contre-intuitive, car la mesure d'irrationalité est d'autant plus grande que α est bien approché par des rationnels. On pourrait s'attendre à ce qu'un nombre bien approché soit « proche d'être rationnel » et donc ait une petite mesure d'irrationalité. Mais en fait ce n'est pas le cas, les nombres algébriques sont d'autant moins bien approchés qu'ils ont un petit degré sur $\mathbf{Q}$. Autrement dit, plus ils sont « proches d'être rationnels » dans le sens « avoir un polynôme minimal sur $\mathbf{Q}$ de petit degré », moins ils sont bien approchés par des rationnels. Plus précisément, on a le théorème suivant, dû à Liouville :

Théorème 5.2. *Si α est un réel algébrique de degré $d > 1$, alors il existe une constante $A > 0$ telle que pour tout rationnel p/q avec $q > 0$,*

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{A}{q^d}.$$

Démonstration. La preuve de ce résultat est largement accessible au niveau de l'agrégation, c'est une jolie application de l'inégalité des accroissements finis ! Voir par exemple https://fr.wikiversity.org/wiki/Introduction_%C3%A0_la_th%C3%A9orie_des_nombres/Approximation_diophantienne_et_fractions_continues ou [FGNb, Nombres de Liouville] : dans cet exercice, on construit des nombres réels approchés si rapidement par des rationnels qu'ils ne satisfont l'inégalité du théorème 5.2 pour aucun d, ce qui implique qu'ils sont transcendants. □

Exercice 5.3. *Fonctions arithmétiques multiplicatives*

Une fontion $f\colon \mathbf{N}^* \to \mathbf{C}$ est dite multiplicative si $f(1) = 1$ et pour tout couple $(m,n) \in (\mathbf{N}^*)^2$ d'entiers premiers entre eux, $f(mn) = f(m)f(n)$.

1. Montrer que si f et g sont deux fonctions multiplicatives, alors $f \star g$ l'est aussi.
2. Application : en déduire que si $k \geqslant 1$ est un entier fixé, alors la fonction

$$\begin{array}{ccc} \mathbf{N}^* & \to & \mathbf{C} \\ n & \mapsto & \sum_{d|n} d^k \end{array}$$

est multiplicative.

3. Montrer que l'inverse (pour le produit de convolution) d'une fonction multiplicative est une fonction multiplicative.
4. En déduire une preuve alternative de l'expression explicite de la fonction de Möbius.

Solution. voir https://www.mathraining.be/chapters/70?type=10 □

Exercice 5.4. *Série génératrice et décomposition en éléments simples*

Le but de cet exercice est de démontrer de deux façons différentes une formule close pour le nombre $a(n)$ de façons de payer n euros en pièces de 1 et 2 euros.

1. Montrer « à la main » que $a(n) = \lfloor \frac{n}{2} \rfloor + 1$.
2. On se propose maintenant de redémontrer la formule de la question précédente à l'aide de la série génératrice associée à ce problème de dénombrement.
   (a) Montrer que
   $$\sum_{n=0}^{+\infty} a(n)X^n = \left(\frac{1}{1-X^2}\right)\left(\frac{1}{1-X}\right) \quad \text{dans } \mathbf{Q}[[X]].$$
   (b) Trouver des rationnels a, b, c tels que
   $$\sum_{n=0}^{+\infty} a(n)X^n = \frac{a}{1+X} + \frac{b}{1-X} + \frac{c}{(1-X)^2}.$$
   On pourra faire appel à des raisonnements analytiques pour trouver a, b, c, mais il est ensuite bon de se convaincre que l'égalité est vraie dans $\mathbf{Q}[[X]]$.
   (c) Retrouver le résultat de la question 1.

Solution. voir [Bil] □

Exercice 5.5. *Série génératrice de la suite de Fibonacci*

On rappelle la définition de la suite de Fibonacci : $F_0 = 0$, $F_1 = 1$ puis $F_{n+2} = F_{n+1} + F_n$. On note
$$f(X) := \sum_{n=0}^{+\infty} F_n X^n$$
la série génératrice de la suite de Fibonacci.

1. Montrer que $f(X) = \frac{X}{1-X-X^2}$ dans $\mathbf{Q}[[X]]$
2. En déduire que si l'on note $\alpha := \frac{1+\sqrt{5}}{2}$ et $\beta := \frac{1-\sqrt{5}}{2}$, on a
   $$f(X) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha X} - \frac{1}{1-\beta X}\right) \quad \text{dans } \mathbf{R}[[X]]$$
3. Conclure en retrouvant l'expression de F_n comme une fonction de n uniquement.

Solution. voir [Bil] □

Exercice 5.6. *Nombres de Catalan, séries entières, loi du temps de retour en 0 de la marche aléatoire symétrique sur* $\mathbf{Z}$.

On note $\mathcal{C}_n$ l'ensemble des $(u_0, \ldots, u_{2n})$ dans $\mathbf{N}^{2n+1}$ tels que
$$\begin{cases} u_0 = u_{2n} = 0 \\ |u_{i+1} - u_i| = 1 \text{ pour tout } i \in \{0, \ldots, 2n-1\} \end{cases}$$
On note c_n le cardinal de $\mathcal{C}_n$. On l'appelle le n^{e} nombre de Catalan.

1. En notant $\mathcal{C}_n^+$ le sous-ensemble de $\mathcal{C}_n$ formé des $(u_i)_{0 \leqslant i \leqslant 2n}$ ne s'annulant qu'en 0 et en $2n$, montrer que $|\mathcal{C}_n^+| = |\mathcal{C}_{n-1}|$.

2. Montrer que pour tout $n \geqslant 1$,
$$c_n = \sum_{k=0}^{n-1} c_k c_{n-1-k}$$
3. Montrer que $c_n \leqslant 4^n$ et en déduire que la série entière $\sum_{n\geqslant 0} c_n x^n$ a un rayon de convergence supérieur ou égal à $1/4$.
4. Pour $x \in]-\frac{1}{4}, \frac{1}{4}[$, on définit $f(x) := \sum_{n=0}^{+\infty} c_n x^n$. Montrer que pour tout $x \in]-\frac{1}{4}, \frac{1}{4}[$,
$$xf(x)^2 - f(x) + 1 = 0$$
5. En déduire que pour tout $x \in]-\frac{1}{4}, \frac{1}{4}[\setminus\{0\}$,
$$f(x) = \frac{1-\sqrt{1-4x}}{2x}.$$
6. Montrer que pour tout $n \geqslant 0$
$$c_n = \frac{1}{n+1}\binom{2n}{n}.$$
7. Soit $(X_i)_{i\geqslant 1}$ des variables aléatoires iid suivant la loi de Rademacher (c'est-à-dire qu'elles prennent les valeurs -1 ou 1 avec probabilité $\frac{1}{2}$). Pour tout $n \geqslant 1$, on note
$$S_n := \sum_{i=1}^{n} X_i$$
et on introduit le temps de premier retour en 0 :
$$T := \inf\{n \geqslant 1 \mid S_n = 0\}.$$
Montrer que pour tout $n \geqslant 1$, $\mathbb{P}(T = 2n) = \frac{c_{n-1}}{2^{2n-1}}$. On a ainsi déterminé la loi du temps de premier retour en 0 de la marche aléatoire symétrique sur $\mathbf{Z}$.
8. En déduire que $\mathbb{P}(T < +\infty) = 1$ et que $\mathbb{E}(T) = +\infty$.

Remarque : il est aussi possible d'obtenir le résultat de la question 6 sans passer par les séries entières : voir la page Wikipédia des nombres de Catalan, dans la section sur les mots de Dyck.

Solution. Les questions 1 à 6 sont traitées par une méthode analogue dans [FGNa] à partir de la deuxième édition. □

Exercice 5.7. *Utilisation des diagrammes de Young*

Soit k un corps et n un entier inférieur ou égal à 6. Montrer que deux matrices nilpotentes de $\mathrm{M}_n(k)$ sont semblables si et seulement si elles ont même rang et même polynôme minimal. Donner un contre-exemple dans $\mathrm{M}_7(k)$.

Solution. *cf.* [MM], dans les exercices du chapitre sur la réduction de Jordan. □

Références

[Apo] Tom M. Apostol. *Introduction to analytic number theory.* Springer.

[Ber] Grégory Berhuy. *Algèbre : le grand combat.* Calvage et Mounet.

[Bil] Margaret Bilu. *Séries génératrices.* notes de cours : https://www.math.u-bordeaux.fr/~mbilu/seriesgen.pdf.

[CG] Philippe Caldero and Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries, Tome I.* Calvage et Mounet.

[CP] Philippe Caldero and Marie Peronnier. *Carnet de voyage en Algébrie.* Calvage et Mounet.

[FF] Dominque Foata and Aimé Fuchs. *Calcul des probabilités.* Dunod.

[FGNa] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X-ENS Algèbre 1.* Cassini.

[FGNb] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X-ENS Analyse 1.* Cassini.

[Goz] Ivan Gozard. *Théorie de Galois.* Ellipses.

[Mar] George E. Martin. *Counting : The art of enumerative combinatorics.* Springer.

[MM] Roger Mansuy and Rached Mneimné. *Algèbre linéaire. Réduction des endomorphismes.* Vuibert.

[Ten] Gerald Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres.* Dunod.