Club de mathématiques : combinatoire

Jacques Darné

Séance du 15 février 2014

1 Ensembles finis

On s'intéresse à des ensembles finis, dont on veut compter les éléments. Le nombre d'éléments d'un ensemble fini E est noté $\#E = |E| = Card(E)$ et on l'appelle le *cardinal* de E.

On peut numéroter les éléments de E, c'est-à-dire désigner un premier, un deuxième, un troisième, etc. Par définition, dire que E est fini, c'est dire que cela s'arrête : il y a un dernier, le n-ième. Souvent, on notera alors $E = \{x_1, x_2, ..., x_n\}$, ou même $E = \{1, 2, ..., n\}$, c'est-à-dire que l'on désignera les éléments par leur numéro.

Notre premier exemple de dénombrement est le suivant : On veut compter les paires ordonnées d'éléments de E. Une *paire ordonnée* est formée de deux éléments a et b de E et est notée (a, b). *Ordonnée* signifie que $(a, b) \neq (b, a)$. Si $|E| = n$, il y a n possibilités pour le choix de a pour chacun de ces choix, n possibilités pour le choix de b. Ce qui fait n^2 paires possibles.

On peut généraliser un peu : prenons deux ensembles finis E et F, qui contiennent respectivement n et m éléments. On peut compter les paires formées d'un élément a de E et d'un élément b de F. Par le même raisonnement que ce qui précède, il y en a mn. Si l'on note $E \times F = \{\ (a, b) \mid a \in E \text{ et } b \in F\ \}$ l'ensemble des telles paires (remarquer la cohérence de la notation), on a montré :

$$|E \times F| = |E| \cdot |F|.$$

Exercice 1.1 *Que se passe-t-il si on considère les triplets (a, b, c) ? Et si l'on ne considère plus les paires ou les triplets ordonnées ? Si l'on impose $a \neq b$?*
On remarquera que la dernière question, avec les paires non ordonnées, revient à compter le nombre de sous-ensemble de E de cardinal 2.

Un autre calcul fondamental consiste à compter les parties (les sous-ensembles) d'un ensemble E de cardinal n. On remarque pour cela que choisir une partie de A de E revient à choisir pour chaque élément entre les deux possibilités : il appartient à A, ou pas. Ce qui fait deux possibilités pour le premier, deux pour le second, etc. Il y a donc $2 \times 2 \times ... \times 2 = 2^n$ parties de E. Si l'on note $\mathcal{P}(E) = \{A \mid A \subseteq E\}$ l'ensemble des parties de E, on a montré :

$$|\mathcal{P}(E)| = 2^n$$

Exercice 1.2 *Deux parties A et B de E sont disjointes si elles n'ont aucun élément en commun (on note $A \cap B = \varnothing$). Combien y a-t-il de paires ordonnées (= couples) (A, B) de parties disjointes dans un ensemble E à n éléments ?*

Exercice 1.3 *Combien y a-t-il de couples (x, A) tels que $x \in A$ et $A \subseteq E$? ($|E| = n$).*

Exercice 1.4 *Combien y a-t-il de couples (A, B) tels que $A \subseteq B \subseteq E$? ($|E| = n$).*

Si E et F sont deux ensembles, une application $f : E \longrightarrow F$ associe à tout élément x de E un unique élément de F, que l'on note $f(x)$. f est dite :
- *Injective* si : $\forall\ x,\ y \in E,\ x \neq y \Rightarrow f(x) \neq f(y)$,
- *surjective* si : $\forall\ y \in F, \exists\ x \in E,\ f(x) = y$,
- *bijective* si elle est injective et surjective.

Ces définitions formelles se traduise ainsi :
- f est injective si un élément y de F a au plus un antécédent par f, c'est-à-dire que s'il existe un x dans E tel que $f(x) = y$, cet élément est unique.
- f est surjective si un élément de F a au moins un antécédent par f, c'est-à-dire que f atteint tous les éléments de F.
- f est bijective si un élément y de F a un unique antécédent par f, c'est-à-dire qu'à tout élément y de F on peut associer un unique x dans E tel que $f(x) = y$.

On remarque que la bijectivité de f est équivalente à l'existence d'une fonction inverse $f^{-1} : F \longrightarrow E$.

Exercice 1.5 (manipulations) *Montrer les propriétés suivantes :*
- *Si $f : E \longrightarrow F$ et $g : F \longrightarrow G$ sont injectives (resp. surjectives, resp. bijectives), alors $f \circ g$ l'est.*
- *f est bijective si et seulement si elle admet un inverse ($g : F \longrightarrow E$ tel que $g \circ f = Id_E$ et $f \circ g = Id_F$).*
- *Si $g \circ f$ est injective, alors f l'est.*
- *Si $g \circ f$ est surjective, alors g l'est.*
- *Avec $f : E \longrightarrow F$, $g : F \longrightarrow E$ et $h : G \longrightarrow E$, si $g \circ f \circ h$ et $f \circ h \circ g$ sont surjectives, et $h \circ g \circ f$ est injective, alors f, g et h sont bijectives.*

La propriété suivante justifie l'intérêt de ceci dans un cours de combinatoire :

$$|E| \leq |F| \;\Leftrightarrow\; \exists f : E \longrightarrow F \text{ injective } \;\Leftrightarrow\; \exists g : F \longrightarrow E \text{ surjective}$$

et donc :

$$|E| = |F| \;\Leftrightarrow\; \exists f : E \longrightarrow F \text{ bijective }.$$

En fait, compter, c'est choisir une bijection entre l'ensemble des objets à compter et $[\![1, n]\!]$...

Exercice 1.6 (fondamental) $|E| = |F| = n$. *Combien y a-t-il de bijections de E dans F ?*

L'ensemble des bijections de $\{1, ..., \}$ dans lui-même est noté S_n et on l'appelle *le n-ième groupe symétrique*. Ceux qui savent ce que c'est pourront vérifier que c'est en effet un groupe pour la composition des fonctions.

D'après l'exercice précédent :

$$|S_n| = n \cdot (n-1) \cdots 2 \cdot 1 = n!$$

Il y a en effet n choix possibles pour l'image du premier élément, $n-1$ pour l'image du deuxième, etc.

2 Arrangements et coefficients du binôme

On considère un ensemble E ayant n éléments. Comme on l'a vu plus haut, on pourra identifier E et $\{1, ..., n\}$.

On rappelle : $n! = n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 3 \cdot 2 \cdot 1$ ("factoriel n"). Par convention, $0! = 1$.

Soit $p \leq n$. Un *arrangement* de p élément de E, est une suite finie ordonnée de p éléments distincts. On a vu en exercice le nombre d'arrangements de longueur 2. Le nombre d'arrangements de longueur p est :

$$A_n^p := n \cdot (n-1) \cdot (n-2) \cdot ... \cdot (n-p+1) = \frac{n!}{(n-p)!}$$

On trouve cette formule avec le raisonnement habituel : il y a n possibilités pour le premier élément, $n-1$ pour le second (distinct du premier), etc. jusqu'au p-ième, pour lequel il y a $n-p+1$ possibilités.

On définit aussi les coefficients du binôme :

$$\binom{n}{p} := |\mathcal{P}_k(E)|$$

est le nombre de parties de cardinal k dans E. Il est nul $p > n$. Par convention, on dira aussi qu'il est nul si $p < 0$.

Toutes les formules qui suivent se démontrent soit par le calcul à partir de la première formule, soit par un raisonnement combinatoire. La première formule est obtenue à partir du nombre d'arrangement : chaque arrangement de longueur p définit une partie de cardinal p, mais il y a $p!$ arrangements qui définissent cette même partie (en quelque sorte, une partie de cardinal k est un "arrangement à permutation près".

On a une formule explicite :

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

Le fameux binôme de Newton, qui donne leur nom aux coefficients :

$$(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}.$$

La formule de Pascal :

$$\binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}.$$

On construit alors le triangle de Pascal à partir de :

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Deux autres formules très utiles :

$$\binom{n}{n-p} = \binom{n}{p} \text{ et } p\binom{n}{p} = n\binom{n-1}{p-1}.$$

Exercice 2.1 *Calculer* $\sum\limits_{k=0}^{n} \binom{n}{k}$ *et* $\sum\limits_{k \text{ pair}} \binom{n}{k}$.

Exercice 2.2 *Prouver la propriété des hexagones :*

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

Pourquoi Pascal lui a-t-il donné ce nom ?

Exercice 2.3 (Partitions de N) *Une p-partition de* $N \in \mathbb{N}$ *est une suite finie de longueur p* $a_1, ..., a_p$ *d'entiers positifs dont la somme est* N. *Par exemple* $1+2+0+1=4$. *Combien y a-t-il de p-partitions de* N *? Que se passe-t-il si on remplace "positifs" par "strictement postif" ?*

Exercice 2.4 (fonctions croissantes, injections, surjections) E *et* F *désignent* $\{1, ..., p\}$ *et* $\{1, ..., n\}$. *Calculer en fonction de* n *et* p *:*

- *Le nombre d'injections de* E *dans* F,
- *Le nombre de fonctions strictement croissantes de* E *dans* F,
- *Le nombre de fonctions croissantes de* E *dans* F *(plus difficile - se ramener au précédent).*

3 Groupe symétrique

S_n est l'ensemble des bijections de $\{1, ..., n\}$ dans lui-même, appelées permutations.

La composée de deux permutations est encore une permutation. La permutation identité, notée Id (celle qui à k associe k), est un élément neutre pour la composition : si σ est une permutation, $\sigma \circ Id = Id \circ \sigma = \sigma$. De plus, toute permutaion admet un inverse, c'est-à-dire que si on se donne une permutation σ, il existe une permutation σ^{-1} (unique) telle que $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = Id$. On dit que S_n est un *groupe* pour la composition. On prendra garde que en général $\sigma \circ \tau \neq \tau \circ \sigma$. Le fait que ce soit un groupe est surtout utile parce que l'on sait dire plein de choses sur les groupes, mais on ne l'utilisera pas vraiment ici.

On a des permutations particulières : les cycles (p.e. $[1; 5; 2; 3]$ dans S_5, qui envoie 1 sur 5, 5 sur 2, 2 sur 3, et 3 sur 5, et laisse 4 fixe), et les transpositions (cycles de longueur 2, i.e. celles qui échangent deux éléments).

Le théorème suivant est souvent utile quand on recherche un invariant par permutation, ce qui arrive très souvent. Il suffit alors de montrer que la quantité ou la propriété ne change pas lorsqu'on échange deux éléments (elle est invariante par transposition), et alors elle ne change pas quel que soit l'ordre qu'on donne aux éléments, c'est-à-dire quelle que soit la permutation qu'on leur fait subir.

Théorème 1 *Les transpositions engendrent S_n, c'est-à-dire que toute permutation peut s'écrire (de manière non unique) comme une composée de transpositions.*

Cf. Wikipedia pour une démonstration formelle (article "Permutations", chapitre "Décomposition en produit de transpositions") pour une démonstration. Il est surtout important de bien comprendre comment ça marche sur des exemples.

Exercice 3.1 *Quel est le nombre minimal de transpositions qui engendrent S_n (au sens du théorème précédent) ?*

Le théorème suivant permet de bien comprendre comment se comporte une permutation.

Théorème 2 *Toute permutation peut s'écrire de manière unique comme une composée de cycles à supports disjoints (qui commutent).*

"A supports disjoints" signifie que deux de ces cycles ne bougent pas le mêmes éléments. Par exemple, $[2, 3, 5]$ et $[1, 6]$ sont à supports disjoints, mais pas $[2, 3, 5]$ et $[2, 6]$, qui bougent tous les deux l'élément 2). Ils commutent alors, c'est-à-dire que l'ordre de la composition n'a pas d'importance dans ce cas ($[2,3,5] \circ [1,6] = [1,6] \circ [2,3,5]$, par exemple, mais attention : $[2,3,5] \circ [2,6] \neq [2,6] \circ [2,3,5]$!). L'unicité est donc à permutation près des facteurs (on parle de produits et de facteurs, et souvent on oublie "$\circ$", parce qu'on est dans un groupe).

Pour trouver la décomposition, on part de 1, on prend son image a_1, puis l'image a_2 de a_1, etc, jusqu'à ce qu'on retombe sur 1 (si 1 est fixe, on l'oublie, ou on dit que c'est un cycle de longueur 1), ce qui donne un premier cycle $[1, a_1, a_2, ...]$, puis on recommence à partir d'un élément qui n'est pas dans le cycle, etc, jusqu'à ce qu'on ait mis tous les éléments dans un cycle (sauf éventuellement les points fixes).

Exercice 3.2 *Combien y a-t-il de k-cycles dans S_n ?*

Exercice 3.3 *Ecrire un algorithme efficace pour calculer l'ordre d'une permutation σ, c'est-à-dire le plus petit entier d tel que $\sigma^n = Id$.*
($\sigma^n = \sigma \circ \sigma \circ \cdots \circ \sigma$).

Exercice 3.4 (anagrammes) *Combien y a-t-il d'anagrammes du mot "Prisée" ? D'abord, tenir compte de l'accent. Et si l'on n'en tient pas compte ? Combien y en a-t-il qui commencent par une voyelle ? Qui commencent par une voyelle et finissent par une consonne ?*

Plus généralement, combien peut-on réaliser de mots de n lettre comportant k lettres se répétant $p_1, p_2, ..., p_k$ fois ?

Application : Quel est le nombre d'anagrammes du mot "anagramme" ?

4 Exercices divers

Exercice 4.1 *Calculer :*

$$\sum_{X \subseteq E} |X|, \quad \sum_{X,\ Y \subseteq E} |X \cap Y| \text{ et } \sum_{X,\ Y \subseteq E} |X \cup Y|.$$

Exercice 4.2 (Poker) *On dispose d'un jeu de 54 cartes. Une "main" est un ensemble de 5 cartes, choisie au hasard dans le paquet. Combien y a-t-il de mains possibles ?*

Calculer la probabilité de tirer :

- *Une paire*
- *Une double paire*
- *Un brelan*
- *Un full*
- *Un carré*
- *Une suite*
- *Une couleur (une seule couleur)*

- *Une quinte (suite de cartes de la même couleur)*

Exercice 4.3 (Convolution de Vandermonde) *Soit E un ensemble fini et A, B deux parties de E. On considère l'application*

$$f : \begin{array}{c} \mathcal{P}(E) \to \mathcal{P}(A) \times \mathcal{P}(B) \\ X \mapsto (A \cap X, B \cap X) \end{array}.$$

1. *À quelles conditions sur A et B a-t-on f surjective ? f injective ?*
2. *Lorsque f est bijective, déterminer f^{-1}.*
3. *En déduire la formule de convolution de Vandermonde ($n, p, q \in \mathbb{N}$) :*

$$\sum_{k=0}^{n} \binom{p}{k} \binom{q}{n-k} = \binom{p+q}{n}.$$

Exercice 4.4 *Trouver une formule le nombre de permutations de S_n ayant un cycle de longueur $> n/2$ (dans sa décomposition en cycles disjoints).*

Exercice 4.5 100 *prisoniers sont mis à l'épreuve par un geôlier sadique, qui leur promet de les libérer aux conditions suivante :*

Les prisoniers, qui portent un matricule de 1 *à* 100*, devront tour à tour passer dans une salle contenant un meuble avec* 100 *tiroirs étiquetés de* 1 *à* 100*. Dans chaque tiroir se trouve le numéro d'un prisonier (les numéros sont répartis au hasard). Le prisonier pourra ouvrir la moitié des* 100 *tiroirs. Si tous les prisoniers trouvent leur matricule, ils sont libres. Mais si un seul échoue, ils restent tous en prison.*

Montrer que les prisoniers (qui peuvent se mettre d'accord avant mais ne communiquent pas pendant l'épreuve) ont une stratégie qui leur assure environ 30% *de chances de succès.*

Expliquer comment vous pouvez les faire gagner à coup sûr si l'on vous propose d'échanger deux papiers avant le début.

Club de mathématiques : combinatoire - corrections des exercices

Jacques Darné

Séance du 15 février 2014

Exercice 1 *Deux parties A et B de E sont disjointes si elles n'ont aucun élément en commun (on note $A \cap B = \varnothing$). Combien y a-t-il de paires ordonnées (= couples) (A, B) de parties disjointes dans un ensemble E à n éléments ?*

Il y a trois choix pour chaque élément : il appartient à A ou à B, ou encore ni à l'un, ni à l'autre. Le nombre cherché est donc 3^n.

Exercice 2 *Combien y a-t-il de couples (x, A) tels que $x \in A$ et $A \subseteq E$? ($|E| = n$).*

Il y a n choix pour x et on choisit ensuite le reste de A parmi les parties de $E - x$. Donc il y a $n2^{n-1}$ tels couples.

Exercice 3 *Combien y a-t-il de couples (A, B) tels que $A \subseteq B \subseteq E$? ($|E| = n$).*

C'est le même exercice que le premier : il y a trois choix pour x donné : $x \in A$, $x \in B - A$ ou $x \notin B$. Il y a donc 3^n tels couples.

L'exercice qui suit est juste un petit exercice de manipulation qui demande d'avoir bien compris les notions de surjectivité, injectivité et bijectivité.

Exercice 4 (fondamental) $|E| = |F| = n$. *Combien y a-t-il de bijections de E dans F ?*

Il y a n bijections de $[\![1, n]\!]$ dans lui-même (cf. la remarque après l'exercice).

Exercice 5 *Calculer $\sum\limits_{k=0}^{n} \binom{n}{k}$ et $\sum\limits_{k \text{ pair}} \binom{n}{k}$.*

La première formule peut se voir avec le binôme de Newton pour $(1+1)^n$. Je préfère la démonstration combinatoire :

$$\sum_{k=0}^{n}\binom{n}{k}=\sum_{k=0}^{n}|\mathcal{P}_k([\![1,n]\!])|=|\mathcal{P}([\![1,n]\!])|=2^n.$$

(On compte les parties de $[\![1,n]\!]$ suivant leur cardinal.)

$$\sum_{k \text{ pair}}\binom{n}{k}=2^{n-1}$$

La démonstration que j'ai donnée en cours consiste à dire qu'il y a autant de parties de cardinal pair qu'impair dans $E=[\![1,n]\!]$, en associant à une partie paire une partie impaire de manière bijective. La somme donné compte alors la moitié des parties, donc vaut $\frac{2^n}{2}=2^{n-1}$.

On peut raisonner comme suit :

- Si n est impair, on associe à une partie son complémentaire, de parité différente. La bijection inverse est définie de même.
- Si n est pair, on se ramène au cas précédent, par exemple en discutant suivant suivant que la partie X contient n ou pas : si $n \in X$, on lui associe $E-X$ auquel on rajoute n (noté $(E-X)\cup\{n\}$), et si $n \notin X$, on lui associe $E-X$ auquel on retire n (noté $(E-X)-\{n\}$). La réciproque est définie de même.

En fait, il y a une démonstration plus élégante pour traiter les deux cas ensemble (comme souvent, quand on trouve une formule simple à la fin, c'est qu'on peut faire un raisonnement élégant...).

On raisonne comme suit : soit X une partie de $[\![1,n-1]\!]$. Si son cardinal est pair, on lui associe X comme partie de $[\![1,n]\!]$. Si son cardinal est impair, on lui rajoute n : on lui associe $X\cup\{n\}$. On a ainsi défini une application des parties de $[\![1,n-1]\!]$ vers les parties de cardinal pair de $[\![1,n]\!]$. C'est une bijection, d'inverse $X\mapsto X\cap[\![1,n-1]\!]$ (où $\cap$ désigne l'intersection, c'est-à-dire les éléments que les deux ensembles ont en commun). Donc les parties paires de $[\![1,n]\!]$ sont bien au nombre de 2^{n-1} (et les parties impaires aussi, avec le même raisonnement).

La propriété des hexagones se prouve par le calcul (en tout cas, je n'ai pas mieux à ce jour). Les facteurs forment un hexagone dans le triangle de Pascal.

Exercice 6 (Partitions de N) *Une p-partition de $N\in\mathbb{N}$ est une suite finie de longueur p $a_1,...,a_p$ d'entiers positifs dont la somme est N. Par exemple $1+2+0+1=4$. Combien y a-t-il de p-partitions de N ? Que se passe-t-il si on remplace "positifs" par "strictement postif" ?*

Je rappelle brièvement la méthode donnée en cours : on trace N croix sur une ligne, et on intercale $p-1$ bâtons, ce qui donne une suite de $N+p-1$

symboles. Les suites ainsi formées correspondent de manière bijective aux p-partitions positives (avec éventuellement des zéros, quand deux bâtons se suivent) de N (la correspondance est évidente). Or choisir une telle suite revient à choisir la partie des symboles qui seront des bâtons, il y en a donc $\binom{N+p-1}{p-1}$.

Pour les partitions strictement positives, il suffit de dire que les p-partitions de N strictement positives sont en bijection avec les p-partitions positives de $N-p$ (en retirant 1 à tous les termes - la bijection réciproque ajoute 1), donc il y en a $\binom{N-1}{p-1}$.

Exercice 7 (fonctions croissantes, injections, surjections) *E et F désignent $\{1, ..., p\}$ et $\{1, ..., n\}$. Calculer en fonction de n et p :*
- *Le nombre d'injections de E dans F,*
- *Le nombre de fonctions strictement croissantes de E dans F,*
- *Le nombre de fonctions croissantes de E dans F (plus difficile - se ramener au précédent).*

Les injections sont par définition les p-arrangements du second ensemble, donc au nombre de $\frac{n!}{n-p)!}$ (n choix pour le premier, $n-1$ pour le second, etc. jusqu'au p-ième)

Les applications strictements croissantes sont déterminées uniquement par leur image, car une fois l'image choisie, une telle application est obligée d'envoyer1 sur le plus petit élément de l'image, 2 sur le plus petit de ceux qui restent, etc. Cette image est de cardinal p (une application strictement croissante est en particulier injective). Le nombre de fonctions croissantes est donc $\binom{n}{p}$.

Les fonctions croissantes sont en bijection avec les fonctions strictement croissante de $[\![1, p]\!]$ vers $[\![1, n+p]\!]$. Elles sont donc au nombre de $\binom{n+p}{p}$. La bijection est donnée par $\phi \mapsto \tilde{\phi} : k \mapsto \phi(k) + k$ (la bijection inverse est évidemment $\psi \mapsto \bar{\psi} : k \mapsto \psi(k) - k$).

Exercice 8 *Quel est le nombre minimal de transpositions qui engendrent S_n (au sens du théorème précédent) ?*

La démonstration suivante comporte des petites imprécisions dûes au fait que je ne voulais pas faire de démonstration formelle du fait que les transpositions engendrent S_n. C'est un fait assez intuitif, et dans le cadre du club de maths, il suffit de s'en convaincre, c'est-à-dire de regarder sur des exemples. Un lecteur intéressé pourra essayer d'en écrire une démonstration formelle ou se référera par exemple à Wikipédia (chapitre "Algorithme de décomposition" de l'article "permutation" - voir aussi l'article "groupe symétrique"). Wikipédia est souvent une source intéressante pour les mathématiques élémentaires.

Cette correction utilise également un peu de théorie des graphes. Je conseille vivement à ceux qui ne sauraient pas de quoi l'on parle de lire au moins les premières pages du cours de Pierre Bornztein, que l'on trouvera sur le site d'Animath (http ://www.animath.fr/IMG/pdf/cours-graphes.pdf).

On se convaincra que les transpositions $(i, i+1)$, qui échangent deux éléments consécutifs, suffisent (cf. le chapitre "Générateurs du groupe symétrique" de l'article "groupe symétrique" de Wikipédia). On a donc un ensemble transositions cardinal $k-1$ qui engendrent le groupe. Peut-on faire mieux ? La réponse est non : $k-1$ est optimal. En fait, si on se donne un ensemble T de transpositions, on considère le graphe (non orienté) dont les sommets sont les entiers de 1 à n, et tel qu'une arête relie i et j si et seulement si $(i, j) \in T$. Une condition nécessaire pour que les transpositions de T engendrent S_n est que le graphe soit connexe (Sinon, on ne pourra jamais échanger deux éléments de deux composantes connexes différentes quel que soit le nombre de transpositions de T qu'on applique. En fait, on se convaincra que la condition est suffisante). Or un graphe connexe à n sommet possède au moins n arête (cf. le cours de P. Bornztein p. 6). donc $|T| \geqslant n-1$, ce qu'on voulait.

Exercice 9 *Combien y a-t-il de k-cycles dans S_n ?*

Le choix d'un k-cycle de S_n passe par le choix du support (les éléments de $[\![1, n]\!]$ que le cycle bouge), de cardinal k par définition d'un k-cycle. On le note ici $c_1, ..., c_k$. Il y a $\binom{n}{k}$ possbilités pour ce choix. Puis il faut choisir le cycle. On prend c_1. On choisit son image parmi les $k-1$ autres éléments. Puis on choisit l'image de cette image parmi les $k-2$ qui reste... etc, jusqu'au dernier qui est nécessairement envoyé sur c_1. Il y a donc $(k-1)!$ tels choix, ce qui fait un total de $(k-1)!\binom{n}{k}$ k-cycles dans S_n.

Exercice 10 *Ecrire un algorithme efficace pour calculer l'ordre d'une permutation σ, c'est-à-dire le plus petit entier d tel que $\sigma^n = Id$.*
($\sigma^n = \sigma \circ \sigma \circ \cdots \circ \sigma$).

Pour calculer l'ordre d'une permutation, on la décompose d'abord en cycles disjoints (i.e. qui ne bougent pas les mêmes éléments). Le ppcm de la longueur des cycles donne l'ordre de la permutation. On remarquera que c'est un calcul beaucoup plus efficace que de la composer avec elle-même suffisamment pour finir par retomber sur Id.

Exercice 11 (anagrammes) *Combien y a-t-il d'anagrammes du mot "Prisée" ? D'abord, tenir compte de l'accent. Et si l'on n'en tient pas compte ? Combien y en a-t-il qui commencent par une voyelle ? Qui commencent par une voyelle et finissent par une consonne ?*

Plus généralement, combien peut-on réaliser de mots de n lettre comportant k lettres se répétant $p_1, p_2, ..., p_k$ fois (avec bien sûr $\sum k_i = n$) ?

Application : Quel est le nombre d'anagrammes du mot "anagramme" ?

Avec l'accent, il y a $6! = 720$ anagrammes de "prisée" (ce sont les permutations des lettres).

Sans l'accent, il y en a deux fois moins, car on a compté deux fois chaque cas.

On traite les deux questions suivantes par exemple avec l'accent.

Choix de la voyelle : 3 possibilités. Puis $5! = 120$ possibilités pour le reste. Ce qui donne 360 qui commencent par une voyelle.

Choix de la voyelle : 3 possibilités. 3 pour la consonne finale, puis $4! = 24$ pour le reste. Ce qui fait 216 qui commencent par une voyelle et finissent par une consonne.

On a au total $n!$ permutations des lettres, mais un anagramme donné correspond à $p_1!p_2!\cdots p_k!$ permutations, car il ne change pas si on permute des lettres qui sont les même. Ceci donne $\frac{n!}{p_1!p_2!\cdots p_k!}$ anagrammes.

Application : il y a $\frac{9!}{3!2!}$ anagrammes du mot “anagramme”.

Exercice 12 *Calculer :*

$$\sum_{X\subseteq E} |X|, \quad \sum_{X,\ Y\subseteq E} |X\cap Y| \ \textit{et} \ \sum_{X,\ Y\subseteq E} |X\cup Y|.$$

Pour cet exercice, il est très intéressant d'introduire la notion de fonction caractéristique : si X est une partie de E, on notera $\mathbb{1}_X$ la fonction qui à $x\in E$ associe 1 si $x\in X$ et 0 sinon. On a la formule évidente suivante :

$$\sum_{x\in E} \mathbb{1}_X(x) = |X|.$$

Alors on peut calculer par exemple :

$$\sum_{X\subseteq E} |X| = \sum_{X\subseteq E}\sum_{x\in E} \mathbb{1}_X(x) = \sum_{x\in E}\sum_{X\subseteq E} \mathbb{1}_X(x)$$

Or $\sum\limits_{X\subseteq E} \mathbb{1}_X(x)$ compte le nombre de parties de E qui contiennent x donné, et le choix d'une telle partie revient à choisir une partie de $E-\{x\}$, donc il y en a 2^{n-1} (où $n = |E|$) :

$$\sum_{X\subseteq E} \mathbb{1}_X(x) = 2^{n-1}.$$

On obtient donc :
$\sum\limits_{X\subseteq E} \mathbb{1}_X(x) = n2^{n-1}$.

Le calcul des autres sommes se fait en remarquant que $\mathbb{1}_{X\cap Y} = \mathbb{1}_X \cdot \mathbb{1}_y$ et que $|X\cup Y| = |X| + |Y| - |X\cap Y|$.

Exercice 13 100 *prisoniers sont mis à l'épreuve par un geôlier sadique, qui leur promet de les libérer aux conditions suivante :*

Les prisoniers, qui portent un matricule de 1 *à* 100*, devront tour à tour passer dans une salle contenant un meuble avec* 100 *tiroirs étiquetés de* 1 *à* 100*. Dans chaque tiroir se trouve le numéro d'un prisonier (les numéros sont répartis au hasard). Le prisonier pourra ouvrir la moitié des* 100 *tiroirs. Si tous les prisoniers trouvent leur matricule, ils sont libres. Mais si un seul échoue, ils restent tous en prison.*

Montrer que les prisoniers (qui peuvent se mettre d'accord avant mais ne communiquent pas pendant l'épreuve) ont une stratégie qui leur assure plus de 30% *de chances de succès.*

Expliquer comment vous pouvez les faire gagner à coup sûr si l'on vous propose d'échanger deux papiers avant le début.

Chaque prisonier va ouvir le tiroir qui correspond à son numéro, puis le tiroir qui correspond au numéro qu'il aura trouvé dedans, etc. Il fait ainsi exactement ce qu'on fait quant on décompose une permutation en cyles disjoints (la permutation en question est celle qui au numéro de chaque tiroir associe le numéro qui est dedans). Arriver au bout du cycle signifie retomber sur son propre numéro. Cela arrivera pour tous les prisoniers si et seulement si tous les cycles sont de longueur $\leqslant 50$.Il faut donc compter le nombre de premutations ayant un cycle de longueur > 50 dans S_{100}. On va faire le calcul dans S_n, et on l'appliquera pour $n = 100$ ensuite.

On a un cycle de longeur strictement supérieure à $\frac{n}{2}$ avec une probabilité

$$p(n) = \sum_{k>\frac{n}{2}} (n-k)!(k-1)!\binom{n}{k}.$$

En effet, pour choisir une permutation ayant un tel cycle, on choisit le cycle suivant son cardinal k, supérieur à $\frac{n}{2}$ (Il y en a $(k-1)\binom{n}{k}$ par un exercice déjà vu) puis une permutation du reste $((n-k))$ (pas de risque de compter deux fois une même permutation, puisqu'il ne peut y avoir d'autre cycle de cette taille).

Puis l'on calcule :

$$p(n) = \frac{1}{n!}\sum_{k>\frac{n}{2}} (n-k)!(k-1)!\frac{n!}{(n-k)!k!} = \frac{1}{n!}\sum_{k>\frac{n}{2}} \frac{n!}{k} = \sum_{k>\frac{n}{2}} \frac{1}{k}.$$

On sait que :

$$\sum_{k=0}^{n} \frac{1}{k} \sim \ln(n)$$

.

Ici, "$\sim$" signifie "équivalent quand n tends vers $+\infty$", c'est-à-dire que le quotient des deux membres tend vers 1. Ceux qui ne le savent pas peuvent l'admettre, et de toute façon vous pouvez calculer la somme à la calculatrice pour $n = 100$ et voir que ça donne un résultat proche.

On a donc

$$p(n) = \sum_{k=1}^{n} \frac{1}{k} - \sum_{k=0}^{\frac{n}{2}} \frac{1}{k} \sim \ln(n) - \ln(n/2) = \ln(2).$$

La probabilité que les prisonniers gagnent avec cette stratégie tend donc vers $1 - \ln(2) \approx 0.3$ quand n devient grand. Et c'est déjà proche pour $n = 100$.

Si l'on vous propose d'échanger daus papiers au début, il suffit de "casser" le grand cycle s'il y en a un ...