Al 5 - Entiers naturels - Dénombrements

1 Rudiments d'arithmétique dans $\mathbb{N}$

1.1 Divisibilité

Définition 1
Soit $(a, b) \in \mathbb{N}^2$.

1. On dit que b divise a, et on note $b|a$, s'il existe un entier $k \in \mathbb{N}$ tel que $a = kb$.
En d'autres termes :

$$b|a \iff \exists k \in \mathbb{N},\ a = kb$$

2. On dit aussi que a est un multiple de b, ou que b est un diviseur de a.

Notation :
La négation de la relation de divisibilité est notée $\nmid$.

Exemple 1

1. 2 divise $n \in \mathbb{N}$ si, et seulement si, n est pair.

2. $\forall n \in \mathbb{N},\ n|0$ et $\forall n \in \mathbb{N},\ 1|n$.

Remarque 1

1. Soit $(a, b) \in \mathbb{N}^2$. Si $a|b$ et $b \neq 0$ alors $a \leq b$.

2. On en déduit que l'ensemble des diviseurs de $n \in \mathbb{N}^*$ est inclus dans $[\![1, n]\!]$ et contient au moins 1 et n.

Proposition 1
Soit $(a, b, c) \in \mathbb{N}^2$.

1. $a|a$

2. $(a|b \text{ et } b|a) \implies a = b$

3. $(a|b \text{ et } b|c) \implies a|c$

Théorème-Définition 1
Soit $(a, b) \in \mathbb{N}^2$ avec $b \neq 0$. Alors :

1. il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que :

$$a = bq + r \quad \text{et} \quad 0 \leq r < b$$

2. on dit que q est le **quotient** et r le **reste** de la division euclidienne de a par b.

Remarque 2
En Python :

1. $a//b$ renvoie le quotient de la division euclidienne de a par b

2. $a\%b$ renvoie le reste de la division euclidienne de a par b

Théorème 1
Soit $(a,b) \in \mathbb{N}^2$ avec $b \neq 0$. Alors $b|a$ si, et seulement si, le reste de la division euclidienne de a par b est nul.

Remarque 3
On a les équivalences suivantes dans $\mathbb{N}$:

$$b|a \iff \exists k \in \mathbb{N},\ a = kb \iff a \equiv 0\,[b]$$

1.2 Nombres premiers

Définition 2
Un nombre premier est un entier $p \geq 2$ qui n'est divisible que par 1 et par p.

Théorème 2
Tout entier $n \geq 2$ admet au moins un diviseur premier.

Théorème 3
Il existe une infinité de nombres premiers.

Le crible d'Eratosthène
Pour déterminer tous les nombres premiers compris entre 2 et N, on peut procéder comme suit. On commence par écrire les nombres de 2 à N, et on éliminera ensuite pas à pas ceux qui ne sont pas premiers en procédant comme suit :

1. 2 est un nombre premier. Par contre, tous les multiples stricts de 2 n'en sont pas. On élimine donc tous les nombres pairs différents de 2.
2. 3 est un nombre premier. De, même on élimine tous les multiples de 3 différents de 3.
3. 4 n'est pas premier (et a donc déjà été éliminé), mais 5 est premier. On barre donc tous les multiples de 5 différents de 5.
4. On continue ainsi jusqu'à avoir épuisé tous les nombres, en considérant à chaque étape le plus petit nombre qui n'a pas été éliminé ou sélectionné ; c'est nécessairement un nombre premier, et on élimine ensuite tous ses multiples stricts.

Théorème 4
Soient $n \in \mathbb{N}$ et $n \geq 2$. Alors n s'écrit de manière unique, à l'ordre près des facteurs :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

avec :

$$k \in \mathbb{N}^*,\ p_1 < p_2 < \dots < p_k \text{ des nombres premiers et } \forall i \in [\![1,k]\!],\ \alpha_i \in \mathbb{N}^*$$

1.3 PGCD, PPCM

Définition 3
Soit $(a,b) \in \mathbb{N}^2$.

1. Le plus grand commun diviseur de a et b est le nombre entier noté $PGCD(a,b)$, et défini par :

$$PGCD(a,b) = a \wedge b = \max\{n \in \mathbb{N}, n|a \text{ et } n|b\}$$

2. On dit que a, b sont premiers entre eux si :

$$a \wedge b = 1$$

3. Le plus petit commun multiple de a et b est le nombre entier noté $PPCM(a,b)$, défini par :

$$PPCM(a,b) = a \vee b = \min\{n \in \mathbb{N}, a|n \text{ et } b|n\}$$

Remarque 4
Pour tout $a \in \mathbb{N}$, on a :

$$a \wedge 0 = a$$

Proposition 2
Soient $(a,b) \in \mathbb{N}^2$, avec $b \neq 0$ et r le reste de la division euclidienne de a par b. Alors :

$$PGCD(a,b) = PGCD(b,r)$$

L'algorithme d'Euclide
L'algorithme d'Euclide est un algorithme permettant de calculer le PGCD de deux nombres entiers a et b.
On définit pour cela une suite d'entiers (u_n) telle que $u_0 = a$, $u_1 = b$, et pour tout entier $n \in \mathbb{N}^*$, u_{n+1} est le reste de la division euclidienne de u_{n-1} par u_n si $u_n \neq 0$ et $u_{n+1} = 0$ dans le cas contraire.
On peut alors montrer que (u_n) est une suite nulle à partir d'un certain rang.

1. En effet, pour tout $n \in \mathbb{N}^*$, si $u_n \neq 0$, alors $u_{n+1} < u_n$.
Cela montre que (u_n) stationne à 0 à partir d'un rang N.

2. Soit $d = u_{N-1}$, la dernière valeur non nulle de cette suite. Par récurrence, en utilisant le proposition précédente, on obtient :

$$PGCD\,(a,b) = PGCD\,(u_{n-1},u_n) = PGCD\,(u_n,u_{n+1})$$

3. En prenant $n = N-1$, il vient :

$$PGCD(a,b) = PGCD(d,0) = d$$

2 Dénombrement

2.1 Notion de cardinal d'un ensemble fini

Remarque 5
Intuitivement, on dit qu'un ensemble est fini s'il possède un nombre fini d'éléments, et son cardinal est alors le nombre de ses éléments. Formellement, cela donne la définition suivante (hors-programme).

Définition 4

1. On dit qu'un ensemble non vide E est fini s'il existe un entier naturel non nul n et une bijection $\varphi : [\![1,n]\!] \to E$.

2. Lorsqu'il existe, l'entier n est unique ; il est appelé le cardinal de E et est noté $\text{card}(E)$, $|E|$ ou encore $\#E$.

3. Par convention, l'ensemble $\varnothing$ est fini, et son cardinal est 0.

4. Un ensemble est dit infini s'il n'est pas fini.

Remarque 6
Intuitivement, φ peut être considérée comme une numérotation des éléments de E.
Si $E = \{e_1, e_2, \ldots, e_n\}$ alors :

$$\varphi : \begin{array}{ccc} [\![1,n]\!] & \to & E \\ i & \mapsto & e_i \end{array}$$

Exemple 2

1. Pour $n \in \mathbb{N}^*$, l'ensemble $[\![1,n]\!]$ est de cardinal n.

2. Soient $p, n \in \mathbb{N}^*$ tels que $p \leq n$. Alors $[\![p, n]\!]$ est de cardinal $n - p + 1$.

Théorème 5
Deux ensembles finis ont le même cardinal si, et seulement si, ils sont en bijection.

Théorème 6
Soient E, F deux ensembles, et $f \in \mathcal{F}(E, F)$.

1. Si f est injective et F est fini alors E est fini et :

$$\text{card}(E) \leq \text{card}(F)$$

2. Si f est surjective et E est fini alors F est fini et :

$$\text{card}(F) \leq \text{card}(E)$$

Remarque 7 Principe des tiroirs

1. Une application de E dans F avec $\text{card}(E) > \text{card}(F)$ ne peut donc pas être injective : il existe alors deux éléments distincts de E qui ont la même image.

2. C'est le principe des tiroirs : si on range $n + 1$ paires de chaussettes dans n tiroirs, alors il existe un tiroir contenant au moins deux paires.

Théorème 7
Soient E un ensemble fini, et A une partie de E. Alors A est fini, et :

1.

$$\text{card}(A) \leq \text{card}(E)$$

2.

$$A = E \iff \text{card}(A) = \text{card}(E)$$

Théorème 8
Soient E et F deux ensembles finis de même cardinal. Alors pour toute application $f : E \to F$, on a :

$$f \text{ injective} \iff f \text{ surjective} \iff f \text{ bijective}$$

Théorème 9
Soient E, F deux ensembles finis, et $A \subset E$. On a les résultats suivants :

1. Si $E \cap F = \varnothing$, alors

$$\text{card}(E \cup F) = \text{card}(E) + \text{card}(F)$$

2. Si $\overline{A}$ est le complémentaire de A dans E, alors

$$\text{card}\left(\overline{A}\right) = \text{card}(E) - \text{card}(A)$$

3. Dans tous les cas, on a

$$\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F)$$

Théorème 10
Soit $(A_i)_{1 \leq i \leq n}$ une familles d'ensembles finis deux à deux disjoints. On a :

$$\text{card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \text{card} A_i$$

Théorème 11
Soient n un entier naturel non nul, E , F et E_1, ..., E_n des ensembles finis. On a alors les résultats suivants :

1.
$$\text{card}(E \times F) = \text{card}(E)\text{card}(F)$$

2.
$$\text{card}(E_1 \times E_2 \times \ldots \times E_n) = \text{card}(E_1)\text{card}(E_2)\ldots\text{card}(E_n)$$

3.
$$\text{card}(E^n) = \text{card}(E)^n$$

2.2 p-listes ou tirages avec remise

Définition 5
Soient E un ensemble fini non vide, et $p \in \mathbb{N}^*$. On appelle p-liste d'éléments de E tout p-uplet $(e_1, \ldots, e_p)$ d'éléments de E.

Remarque 8

1. C'est aussi une famille d'éléments de E indexée par $I = [\![1, p]\!]$.

2. L'ordre compte.

3. Les répétitions sont autorisées.

Exemple 3

1. Une 4-liste de $[\![1, 10]\!]$ est, par exemple $(1, 1, 3, 2)$.

2. Un digicode d'un immeuble est composé de 5 symboles parmi les chiffres de 0 à 9 et les lettres A et B : c'est donc une 5-liste de $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B\}$.

Modèle : tirages successifs avec remise
Soit E un ensemble à n éléments. Il y a autant de manières de construire une p-liste d'éléments de E que de prélever (les unes après les autres et) avec remise p boules dans une urne en contenant n.

Théorème 12
Il y a n^p manières de tirer avec remise p boules dans une urne en contenant n.

Théorème 13
Soient E et F deux ensembles finis. Alors :
$$\text{card}(F^E) = \text{card}(F)^{\text{card}(E)}$$

2.3 Arrangements ou tirages sans remise

Définition 6
Soient E un ensemble fini non vide, et $p \in \mathbb{N}^*$. On appelle p-arrangement ou arrangement de p éléments de E tout p-uplet $(e_1, \ldots, e_p)$ d'éléments distincts de E.

Remarque 9

1. L'ordre compte.

2. Les répétitions ne sont pas autorisées ; c'est ce qui différencie les p-arrangements des p-listes.

Exemple 4

1. Un 4-arrangement de $[\![1, 10]\!]$ est, par exemple $(2, 6, 1, 8)$.

2. Une course hippique met en jeu 20 chevaux. Un quinté est un 5-arrangement.

Modèle : tirages successifs sans remise
Soit E un ensemble à n éléments. Il y a autant de manières de construire un arrangement de $p \leq n$ éléments de E que de prélever (les unes après les autres et) sans remise p boules dans une urne en contenant n.

Notation :
Soient $n \geq p$ des entiers naturels. On note A_n^p le nombre d'arrangements de p éléments d'un ensemble à n éléments.

Théorème 14
Soient $n \geq p$ des entiers naturels. On a :

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

Théorème 15
Soient E et F deux ensembles finis non vides tels que $\text{card}(E) = p$ et $\text{card}(F) = n$ avec $p \leq n$.
Alors le nombre d'injections $f : E \to F$ est égal à A_n^p.

Définition 7
Soit E un ensemble fini de cardinal n. On appelle permutation de E tout n-arrangement de E.

Théorème 16
Soit E un ensemble fini de cardinal n. Alors il y a $n!$ permutations de E.

Théorème 17
Soient E et F deux ensembles finis tels que $\text{card}(E) = \text{card}(F) = n$.
Alors le nombre de bijections $f : E \to F$ est égal à $n!$

2.4 Combinaisons ou tirages simultanés

Définition 8
Soient E un ensemble fini, et $p \in \mathbb{N}$. On appelle p-combinaison ou combinaison de p éléments parmi E toute partie de E de cardinal p.

Remarque 10

1. L'ordre ne compte pas.

2. Les répétitions ne sont pas autorisées.

Exemple 5
Les 2-combinaisons de $[\![1, 3]\!]$ sont $(1, 2), (1, 3)$ et $(2, 3)$.

Modèle : tirages simultanés
Soient E un ensemble à n éléments, et p un entier inférieur à n. Il y a autant de manières de construire une partie à p éléments de E que de prélever simultanément p boules dans une urne en contenant n.

Théorème 18
Soient $p \leq n$ des entiers naturels. Le nombre de parties à p éléments d'un ensemble à n éléments est :

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

Remarque 11

1. On a $\binom{n}{0} = \binom{n}{n} = 1$. En effet, si l'on souhaite prélever d'un seul coup toutes les boules d'une urne, ou au contraire aucune, il n'y a qu'une seule possibilité.
2. En outre, on a $\binom{n}{1} = \binom{n}{n-1} = n$. En effet, si l'on souhaite prélever une boule parmi n, il y a n possibilités. Et de manière duale, si on souhaite prélever une poignée de $n-1$ boules, il y a encore n possibilités, puisqu'il suffit en fait de choisir celle que l'on ne prélèvera pas.

Théorème 19
Soit E un ensemble fini de cardinal n. Alors l'ensemble $\mathcal{P}(E)$ des parties de E est également fini, et son cardinal est 2^n.