Chapitre C3 : Arithmétique et dénombrement

1 Divisibilité

Théorème 1.1 (*Division euclidienne dans* $\mathbb{Z}$)

Soit $(a,b) \in \mathbb{Z}^2$ avec $b \neq 0$. Alors il existe un unique couple d'entiers $(q,r) \in \mathbb{Z}^2$ tel que :

i) $a = bq + r$;

ii) $0 \leqslant r < |b|$.

On dit alors que q est le quotient et r le reste de la division euclidienne de a par b.

Exemple 1.2
Déterminer le reste de la division euclidienne de -1086 par 12.

Définition 1.3

Soit $(a,b) \in \mathbb{Z}^2$.

*i) On dit que a **divise** b, et on note $a|b$ s'il existe un entier $k \in \mathbb{Z}$ tel que $b = ka$:*

$$a|b \iff \exists k \in \mathbb{Z},\ b = ka.$$

*ii) Dans ce cas, on dit que b est un **multiple** de a, ou encore que a est un **diviseur** de b.*

Notation 1.4
La négation de la relation de divisibilité sera notée $\nmid$.

Exemples 1.5
On a notamment 2 divise $n \in \mathbb{Z}$ si et seulement si n est pair et $\forall n \in \mathbb{Z},\ n|0, 1|n$.

Proposition 1.6

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

Remarque 1.7
La relation de divisibilité peut aussi s'exprimer en termes de congruence. En effet :

$$a|b \iff \exists k \in \mathbb{Z},\ b = ka \iff b \equiv 0\,[a]\,.$$

Proposition 1.8

i) $\forall a, b \in \mathbb{Z},\ (a|b \ \text{ et } \ b|a) \Rightarrow (a = b \ \text{ ou } \ a = -b)$

ii) $\forall a, b, c \in \mathbb{Z},\ (a|b \ \text{ et } \ b|c) \Rightarrow a|c$

Exemple 1.9

1. Montrer que pour tout $n \in \mathbb{N}$, 9 divise $10^n - 1$.
2. Montrer qu'un nombre est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

2 Nombres premiers

Définition 2.1

*Un **nombre premier** est un nombre entier $p \geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.*

Lemme 2.2

Tout entier $n \geqslant 2$ est divisible par au moins un nombre premier.

Théorème 2.3

Il existe une infinité de nombres premiers.

Exemple 2.4
Déterminer tous les nombres premiers inférieurs ou égaux à 50.

Lemme 2.5 (*Lemme de Gauss*)

Soit p un nombre premier et $(a,b) \in \mathbb{Z}^2$. Si $p|ab$, alors $p|a$ ou $p|b$.

Théorème 2.6 (*Décomposition d'un nombre en produit de facteurs premiers*)

Soit $n \in \mathbb{N}^*$. Alors n s'écrit de manière unique $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_k^{\nu_k}$, avec $k \in \mathbb{N}$, $p_1 < p_2 \cdots < p_k$ des nombres premiers et $\forall i \in [\![1,k]\!]$, $\nu_i \in \mathbb{N}^*$.

Exemple 2.7
Déterminer la décomposition en facteurs premiers de 801. En déduire tous les diviseurs de 801.

3 PGCD, PPCM

Définition 3.1

Soit $(a,b) \in \mathbb{Z}^2$, $(a,b) \neq (0,0)$.

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

$$PGCD(a,b) = \max\{n \in \mathbb{N}^* \mid n|a \text{ et } n|b\}.$$

*ii) On dit que a et b sont **premiers entre eux** si $PGCD(a,b) = 1$.*

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

$$PPCM(a,b) = \min\{n \in \mathbb{N}^* \mid a|n \text{ et } b|n\}.$$

Le lemme suivant est la base de l'algorithme d'Euclide.

Lemme 3.2

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

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

Méthode 3.3 (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 $(u_n)_{n\in\mathbb{N}}$ 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 la suite $(u_n)_{n\in\mathbb{N}}$ est décroissante et positive à partir du rang 2. Elle converge donc. Comme de plus, c'est une suite d'entiers, elle est stationnaire. Mais, par définition de la suite $(u_n)_{n\in\mathbb{N}}$, pour tout $n \in \mathbb{N}^*$, si $u_n \neq 0$, alors $u_{n+1} < u_n$. Cela montre qu'elle stationne à 0, à partir d'un rang N. Soit $d = u_{N-1}$, la dernière valeur non nulle de cette suite. On montre alors que d est le PGCD de a et b. En effet, on montre par récurrence, en utilisant le lemme précédent, que $\forall n \in [\![1, N-1]\!]$, $\text{PGCD}(a,b) = \text{PGCD}(u_{n-1}, u_n) = \text{PGCD}(u_n, u_{n+1})$. En prenant $n = N-1$, il vient $\text{PGCD}(a,b) = \text{PGCD}(d,0) = d$.

Exemple 3.4
Déterminer le PGCD de 1176 et 924.

4 Cardinal d'un ensemble fini

4 a) Définition et premiers résultats

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. Cette approche intuitive sera suffisante dans le cadre de ce cours mais on donne néanmoins les définitions précises d'ensemble fini.

Théorème et définition 4.1

*On dit qu'un ensemble E est **fini** s'il existe un entier n et une bijection $\phi : [\![1, n]\!] \to E$. Lorsqu'il existe, l'entier n est unique ; il est appelé le **cardinal** de E et sera noté* $\text{Card}\, E$, $|E|$ *ou* $\#E$. *Par convention, l'ensemble $\varnothing$ est fini, et son cardinal est* 0.

Remarque 4.2
On admettra le théorème précédent. La bijection ϕ peut être considérée comme une numérotation des éléments de E et comme n est unique ce qui permet de parler **du** cardinal d'un ensemble.

Deux ensembles E et F sont dit **équipotents**, ce qui sera noté $E \simeq F$, s'il existe une bijection entre eux. Ainsi, deux ensembles finis ont le même cardinal si et seulement si ils sont équipotents.

Exemple 4.3
Déterminer dans chaque cas si l'ensemble proposé est fini ou infini :

1. l'ensemble des entiers pairs de 0 à n où $n \in \mathbb{N}^*$;
2. l'ensemble des nombres complexes de module 1 ;
3. l'ensemble des solutions d'un système linéaire ;
4. $\mathbb{R}^3$;
5. l'ensemble des matrices à 2 lignes et 2 colonnes inversibles.

Théorème 4.4

Soient E, F deux ensembles.

i) Si F est fini, alors il existe une injection $f : E \to F$ si et seulement si E est fini et qu'on a $\text{Card}\, E \leqslant \text{Card}\, F$.

ii) Si E est fini, alors il existe une surjection $g : E \to F$ si et seulement si F est fini et $\text{Card}\, E \geqslant \text{Card}\, F$.

iii) Si E ou F est fini, alors il existe une bijection de $h : E \to F$ si et seulement si E et F sont finis et $\text{Card}\, E = \text{Card}\, F$.

4 b) Cardinaux et opérations ensemblistes

Théorème 4.5

Soit A et B deux parties d'un ensemble fini E. On a les résultats suivants :

i) *Si $A \cap B = \varnothing$, alors* $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B$.

ii) *Si $\overline{A}$ dénote le complémentaire de A dans E, alors* $\operatorname{Card} A + \operatorname{Card} \overline{A} = \operatorname{Card} E$.

iii) *Dans tous les cas on a* $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A \cap B)$.

Théorème 4.6

Soient $(A_i)_{1 \leqslant i \leqslant n}$ une famille d'ensembles finis deux à deux disjoints. On a alors :

$$\operatorname{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \operatorname{Card} A_i.$$

Théorème 4.7

Soit E un ensemble fini, et A une partie de E. L'ensemble A est fini, et $\operatorname{Card} A \leqslant \operatorname{Card} E$ *et* $A = E$ *si et seulement si* $\operatorname{Card} A = \operatorname{Card} E$.

Théorème 4.8

Soient E et F deux ensembles finis de même cardinal et $f : E \to F$ une application. Les assertions suivantes sont équivalentes :

i) *f est injective.* *ii)* *f est surjective.* *iii)* *f est bijective.*

Théorème 4.9

Soient n, p des entiers non nuls, et $E, E_1, \ldots, E_n$ des ensembles finis. On a alors les résultats suivants :

i) $\operatorname{Card}(E_1 \times E_2) = \operatorname{Card} E_1 \times \operatorname{Card} E_2$.

ii) $\operatorname{Card}(E_1 \times \cdots \times E_n) = \operatorname{Card}(E_1) \times \cdots \times \operatorname{Card}(E_n)$.

iii) $\operatorname{Card}(E^p) = (\operatorname{Card} E)^p$.

Théorème 4.10

Soient E et F deux ensembles finis. Alors $\operatorname{Card}\left(F^E\right) = (\operatorname{Card} F)^{\operatorname{Card} E}$.

Théorème 4.11

Soit E un ensemble fini de cardinal n. L'ensemble des parties des E, noté $\mathcal{P}(E)$, est également fini, de cardinal 2^n.

5 p-listes ou tirages avec remise

Définition 5.1

Soit E un ensemble, et p un entier. On appelle ***p-liste*** *d'éléments de E tout p-uplet $(e_1, \ldots, e_p)$ d'éléments (non nécessairement distincts...) de E.*

Théorème 5.2

Soit E est un ensemble fini de cardinal n et $p \in \mathbb{N}$. Le nombre de p-listes d'éléments de E est n^p.

Exemple 5.3

1. Les plaques d'immatriculation sont de la forme $AA-555-AA$. Combien y a-t-il de plaques d'immatriculation différentes au total ?
2. Une urne contient k boules numérotées de 1 à k. On effectue 5 tirages avec remise. Combien y a-t-il de tirages différentes en tenant compte de l'ordre ?

6 Arrangements ou tirage sans remise

6 a) Définitions et premiers résultats

Définition 6.1

Soit E un ensemble fini de cardinal n, et $0 \leqslant p \leqslant n$ un entier. On appelle ***arrangement*** *de p éléments de E tout p-uplet $(e_1, \dots, e_p)$ d'éléments deux à deux distincts de E et on note A_n^p le nombre d'arrangements de p éléments d'un ensemble à n éléments.*

Exemple 6.2

1. Une urne contient k boules numérotées de 1 à k. On effectue 5 tirages sans remise. Combien y a-t-il de tirages différentes en tenant compte de l'ordre ?
2. Quelle est la probabilité pour qu ?au moins deux personnes parmi 30 aient la même date anniversaire ? On supposera que les dates anniversaires sont équiréparties parmi 365 dates possibles.

Théorème 6.3

Soient $0 \leqslant p \leqslant n$. On a : $A_n^p = \dfrac{n!}{(n-p)!}$.

Exemple 6.4
Soit a, b, c des réels distincts. Déterminer toutes les injections de $\{1,2,3\}$ dans $\{a,b,c\}$.

Corollaire 6.5

Soient E et F deux ensembles finis tels que $\operatorname{Card} E = p$ et $\operatorname{Card} F = n$. Alors le nombre d'applications injectives $f : E \to F$ est égal à $A_n^p = \dfrac{n!}{(n-p)!}$.

6 b) Application des arrangements aux permutations d'un ensemble

Définition 6.6

Soit E un ensemble fini. On appelle ***permutation*** *de E toute bijection de E dans E. On note encore $\mathfrak{S}(E)$ l'ensemble des permutations de E et $\mathfrak{S}_n$ l'ensemble des permutations de $[\![1, n]\!]$.*

Théorème 6.7

Soit E un ensemble fini de cardinal n. Alors $\operatorname{Card} \mathfrak{S}(E) = n!$.

Exemple 6.8
Soit a, b, c des réels distincts. Déterminer toutes les bijections de $\{1,2,3\}$ dans $\{a,b,c\}$.

Corollaire 6.9

Soient E et F deux ensembles finis tels que $\operatorname{Card} E = \operatorname{Card} F = n$. Alors le nombre de bijections $f : E \to F$ est égal à $n!$.

7 Combinaisons ou tirages simultanés

Définition 7.1

Soit E un ensemble fini de cardinal n, et $0 \leqslant p \leqslant n$ un entier. On appelle ***combinaison*** *de p éléments parmi E tout sous-ensemble de E de cardinal p. On notera $\mathcal{P}_p(E)$ l'ensemble des parties de E, de cardinal p.*

Exemple 7.2

Soit a, b, c des réels distincts. Déterminer toutes les p-combinaisons de $\{a, b, c\}$ pour $p = 0, 1, 2, 3$. Déterminer le nombre de 2-combinaisons.

Théorème 7.3

Soient $0 \leqslant p \leqslant n$ des entiers. Le nombre de parties à p éléments d'un ensemble E de cardinal n vaut

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

Remarque 7.4

On aurait pu donc définir directement $\binom{n}{p} = \operatorname{Card} \mathcal{P}_p(E)$.

Proposition 7.5

Soient $0 \leqslant p \leqslant n$ deux entiers. On a

i) $\binom{n}{0} = 1$, $\binom{n}{n} = 1$, $\binom{n}{1} = n$ *et* $\binom{n}{p} = \binom{n}{n-p}$;

ii) si $0 < p < n$, alors $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$ *(relation de Pascal).*

Remarque 7.6

On rappelle que, par convention, on a également posé : $\binom{n}{p} = 0$ pour $p > n$ ou $p < 0$.

Exemple 7.7

Soit $n \in \mathbb{N}^*$.

1. Déterminer $\displaystyle\sum_{0 \leqslant 2k \leqslant n} \binom{n}{2k}$ et $\displaystyle\sum_{0 \leqslant 2k+1 \leqslant n} \binom{n}{2k+1}$.
2. Soit E un ensemble à n éléments, déterminer le nombre de couples (A, B) de parties distinctes telles que $A \cap B = \emptyset$.

Exemple 7.8

Soit $0 \leqslant p \leqslant n$ deux entiers. Déterminer le cardinal de l'ensemble des applications strictement croissantes de $[\![1, p]\!]$ dans $[\![1, n]\!]$ est de cardinal $\binom{n}{p}$.