Chapitre 2 : Entiers naturels

Programme officiel PCSI

c) Ensembles de nombres usuels

Entiers naturels, entiers relatifs, divisibilité dans $\mathbb{Z}$, diviseurs, multiples. Théorème de la division euclidienne.	
PGCD de deux entiers relatifs dont l'un au moins est non nul.	Le PGCD de a et b est défini comme étant le plus grand élément (pour l'ordre naturel dans $\mathbb{Z}$) de l'ensemble des diviseurs communs à a et b.
PPCM. Algorithme d'Euclide. Nombre premier. L'ensemble des nombres premiers est infini.	
Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.	La démonstration est hors programme. Application au calcul du PGCD et du PPCM.

a) Cardinal d'un ensemble fini

Cardinal d'un ensemble fini.	Notations $\|A\|$, $\mathrm{Card}(A)$. Tout fondement théorique des notions d'entier naturel et de cardinal est hors programme.
Cardinal d'une partie d'un ensemble fini, cas d'égalité. Une application entre deux ensembles finis de même cardinal est bijective si et seulement si elle est injective, si et seulement si elle est surjective.	
Opérations sur les cardinaux : union disjointe ou quelconque, complémentaire, différence, produit cartésien. Cardinal de l'ensemble des applications d'un ensemble fini dans un autre. Cardinal de l'ensemble des parties d'un ensemble fini.	La formule du crible est hors programme.

b) Listes et combinaisons

Nombre de p-listes (ou p-uplets) d'éléments distincts d'un ensemble de cardinal n, nombre de permutations d'un ensemble de cardinal n.	Nombre d'applications injectives d'un ensemble de cardinal p dans un ensemble de cardinal n.
Nombre de parties à p éléments (ou p-combinaisons) d'un ensemble de cardinal n.	Démonstration combinatoire des formules de Pascal et du binôme.

Plan du résumé

I – Nombres entiers naturels

1. Définition
2. Propriétés

II – Ensembles finis

1. Définition
2. Propriétés
   - a. Ensembles finis et inclusion
   - b. Ensembles finis et applications

III – Dénombrement

1. Cardinal et opérations
2. Cardinal et applications
   - a. Cardinal de $\mathscr{F}(E,F)$
   - b. Permutations
   - c. Combinaisons, arrangements, p-listes

IV – Arithmétique dans $\mathbb{N}$

1. Multiples et diviseurs d'un entier
   - a. Définitions
   - b. Division euclidienne
   - c. Algorithme d'Euclide
2. Nombres premiers
   - a. Généralités
   - b. Théorème fondamental de l'arithmétique

Résumé

I – Nombres entiers naturels

1. Définition

Définition :

On appelle $\mathbb{N}$ l'ensemble des entiers naturels.

2. Propriétés

Propriété :

Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

Corollaires :

- Toute partie majorée non vide de $\mathbb{N}$ a un plus grand élément.
- Toute suite d'entiers décroissante est stationnaire.

II – Ensembles finis

1. Définition

Rappel : Pour tout couple entiers (n, m) tels que $n \leq m$, on note $[\![n\,;m]\!]$ l'ensemble des entiers compris entre n et m (au sens large). Cela fonctionne aussi avec les entiers négatifs.

Définitions :

Soit E un ensemble non vide. On dit que E est fini s'il existe une bijection entre E et $[\![1;n]\!]$ avec $n \in \mathbb{N}^*$. Dans ce cas, l'entier n est le nombre d'éléments de E ou cardinal de E, noté $\operatorname{Card} E$.

Propriétés :

- Toute partie de $[\![1;n]\!]$ est finie de cardinal inférieur ou égal à n et est égale à $[\![1;n]\!]$ si elle est de cardinal n.
- Soient n et p deux entiers. S'il existe une bijection de $[\![1;p]\!]$ sur $[\![1;n]\!]$, alors $p = n$.
- Une partie non vide P de $\mathbb{N}$ est finie si et seulement si elle est majorée.
- Si P est une partie de $\mathbb{N}$, non vide et finie de cardinal n, il existe une unique bijection strictement croissante de l'intervalle $[\![1;n]\!]$ sur P.

2. Propriétés

a. Ensembles finis et inclusion :

Propriété :

Toute partie E' d'un ensemble fini E est finie et $\operatorname{Card} E' \leq \operatorname{Card} E$, avec égalité si et seulement si $E' = E$.

b. Ensembles finis et applications :

Propriété :

Soient E et F deux ensembles finis.

- Il existe une injection de E dans F si et seulement si $\mathrm{Card}\,E \leq \mathrm{Card}\,F$.
- Il existe une surjection de E dans F si et seulement si $\mathrm{Card}\,E \geq \mathrm{Card}\,F$.
- Il existe une bijection de E dans F si et seulement si $\mathrm{Card}\,E = \mathrm{Card}\,F$.

Corollaire :

Soient E et F deux ensembles finis de même cardinal et f une application de E dans F.

f est bijective $\Leftrightarrow$ f est surjective $\Leftrightarrow$ f est injective.

III – Dénombrement

1. Cardinal et opérations

Propriété :

Si A et B sont des ensembles finis et disjoints (c'est-à-dire tels que $A \cap B = \varnothing$) alors $A \cup B$ est fini et $\mathrm{Card}(A \cup B) = \mathrm{Card}\,B + \mathrm{Card}\,A$.

Corollaires :

- Si A et B sont des ensembles finis alors $A \setminus B$ est fini et $\mathrm{Card}(A \setminus B) = \mathrm{Card}\,A - \mathrm{Card}(A \cap B)$.
- Si A et B sont des ensembles finis alors $A \cap B$ et $A \cup B$ sont finis et :

$$\mathrm{Card}(A \cup B) = \mathrm{Card}\,B + \mathrm{Card}\,A - \mathrm{Card}(A \cap B).$$

- Si $A_1, A_2, ..., A_n$ sont n ensembles finis et disjoints deux à deux (c'est-à-dire tels que pour tous i et j tels que $i \neq j$, on a $A_i \cap A_j = \varnothing$), alors $A_1 \cup A_2 \cup ... \cup A_n$ est fini et :

$$\mathrm{Card}(A_1 \cup A_2 \cup ... \cup A_n) = \mathrm{Card}\,A_1 + \mathrm{Card}\,A_2 + ... + \mathrm{Card}\,A_n$$

Propriété :

Si E et F sont des ensembles finis, $E \times F$ l'est aussi et $\mathrm{Card}(E \times F) = (\mathrm{Card}\ E) \times (\mathrm{Card}\ F)$.

Propriété :

Si E est un ensemble fini, $\mathscr{P}(E)$ l'est aussi et $\mathrm{Card}\,\mathscr{P}(E) = 2^{\mathrm{Card}\ E}$.

2. Cardinal et applications

a. Cardinal de $\mathscr{F}(E,F)$:

Propriété :

Si E et F sont deux ensembles finis non vides, alors $\mathscr{F}(E,F)$ l'est aussi et $\mathrm{Card}\,\mathscr{F}(E,F) = (\mathrm{Card}\ F)^{\mathrm{Card}\ E}$.

b. Permutations :

Définition :

Soit E un ensemble fini. On appelle permutation de E une bijection de E dans lui-même.

Propriété :

Soit E un ensemble fini de cardinal $n \geq 1$. Le nombre de permutations de E est n!

Corollaire :

Soient E et F deux ensembles finis de même cardinal $n \geq 1$. Le nombre de bijections de E dans F est n!.

c. Combinaisons, arrangements, p-listes :

Définitions :

Soit E un ensemble fini de cardinal n.

On appelle combinaison de p éléments de E (avec $0 \leq p \leq n$) toute partie à p éléments de E.

On appelle p-liste de p éléments de E tout p-uplet de E^p.

On appelle arrangement de p éléments de E (avec $0 \leq p \leq n$) une p-liste de p éléments de E deux à deux distincts.

Propriétés :

Soit E un ensemble fini de cardinal n.

- $\forall\, p \in \mathbb{N}$, le nombre de p-listes de E^p est n^p.
- $\forall\, p \in [\![0, n]\!]$, le nombre d'arrangements de p éléments de E est $\dfrac{n!}{(n-p)!}$, noté A_n^p.
- $\forall\, p \in [\![0, n]\!]$, le nombre de combinaisons de p éléments de E est le coefficient binomial $\dbinom{n}{p}$.

Corollaire :

Soit E et F deux ensembles finis de cardinaux respectifs p et n avec $1 \leq p \leq n$. Le nombre d'injections de E dans F est A_n^p.

IV – Arithmétique dans $\mathbb{N}$

1. Multiples et diviseurs d'un entier

a. Définitions :

Définitions :

Un entier relatif d non nul est un diviseur d'un entier relatif n s'il existe un entier k tel que $n = kd$.

On dit aussi que d divise n, que n est un multiple de d. On note $d \mid n$.

Le PGCD de deux entiers relatifs n et n' est le plus grand diviseur commun à ces deux entiers.

On le note $\mathrm{PGCD}(n, n')$ ou $n \wedge n'$.

Le PPCM de deux entiers relatifs n et n' est le plus petit multiple positif commun de ces deux entiers.

On le note $\mathrm{PPCM}(n, n')$ ou $n \vee n'$.

b. Division euclidienne :

Théorème et définitions :

Soient n et m sont deux entiers relatifs avec $m \neq 0$. Il existe un unique couple (q, r) d'entiers tels que :

$$n = qm + r \quad \text{et} \quad 0 \leq r < m.$$

L'écriture $n = qm + r$ est appelée la division euclidienne de n par m, l'entier q est le quotient et l'entier r est le reste de la division euclidienne.

c. Algorithme d'Euclide :

Propriété (*lemme d'Euclide*) :

Si a et b sont deux entiers avec b non nul et r est le reste de la division euclidienne de a par b, alors :

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r).$$

Algorithme d'Euclide :

Si $a \geq b > 0$ alors le PGCD de a et b, noté d, est le dernier reste non nul dans le tableau suivant :

		Reste	*Quotient*	*Division euclidienne de A par B*
a	b	r_1	q_1	$a = q_1 b + r_1$
b	r_1	r_2	q_2	$b = q_2 r_1 + r_2$
r_1	r_2	r_3	q_3	$r_1 = q_3 r_2 + r_3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_k	r_{k+1}	r_{k+2}	q_{k+2}	$r_k = q_{k+2} r_{k+1} + r_{k+2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r_{\alpha-2}$	$r_{\alpha-1}$	$r_\alpha = d$	q_α	$r_{\alpha-2} = q_\alpha r_{\alpha-1} + r_\alpha$
$r_{\alpha-1}$	r_α	0		

Théorème de Bézout : (*malheureusement hors programme*)

Soient n et m sont deux entiers de PGCD d. Il existe une infinité de couples $(u, v) \in \mathbb{Z}^2$ tels que :

$$u \times n + v \times m = d.$$

Propriété :

Tout diviseur commun de deux entiers divise leur PGCD.

2. Nombres premiers

a. Généralités :

Définition :

Un entier naturel est premier s'il possède exactement deux diviseurs positif : 1 et lui-même.

Propriété :

Tout entier naturel supérieur à 2 possède un diviseur premier.

Propriété :

Il y a une infinité de nombres premiers.

Théorème de Gauss : (*malheureusement hors programme*)

> Soient a, b et c sont trois entiers non nuls tels que $\text{PGCD}(a,b)=1$. Si a $a \mid bc$ alors $a \mid c$.

Corollaires :

- Soient b et c deux entiers et p un nombre premier qui ne divise pas b. Si $p \mid bc$, alors $p \mid c$.
- Soient a, b et c trois entiers. Si $\text{PGCD}(a,b)=1$ et a et b divisent c, alors $ab \mid c$.

Propriété :

> Tout entier naturel $n \geq 2$ non premier possède un diviseur premier inférieur ou égal à $\sqrt{n}$.

b. Théorème fondamental de l'arithmétique :

Théorème (fondamental de l'arithmétique) :

Tout nombre entier $N \geq 2$ se décompose de façon unique (à l'ordre près) en produit de nombres premiers. Autrement dit : $\forall N \in \mathbb{N} \setminus \{0;1\}$, il existe un unique entier $r \in \mathbb{N}^*$, un unique r-uplet $(p_1, p_2, ..., p_r)$ de nombres premiers tel que $p_1 < p_2 < ... < p_r$ et un unique r-uplet $(n_1, n_2, ..., n_r)$ d'entiers strictement positifs tels que :

$$N = p_1^{n_1} p_2^{n_2} ... p_r^{n_r}.$$

Les p_i pour $i \in [\![1, r]\!]$ sont appelés facteurs ou diviseurs premiers de N.

Corollaire :

Soient a et b deux entiers naturels de décompositions $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ et $b = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$, les α_i et β_i pouvant être nuls. Alors :

$$\text{PGCD}(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} ... p_r^{\min(\alpha_r,\beta_r)}$$
$$\text{PPCM}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} ... p_r^{\max(\alpha_r,\beta_r)}$$
$$\text{PGCD}(a,b) \times \text{PPCM}(a,b) = ab$$