Chapitre 1.
Arithmétique

1. Raisonnement par récurrence

1.1 Principe

Il s'agit d'un ***raisonnement inductif***, c'est-à-dire un raisonnement visant à produire des connaissances par des conclusions plus générales que les prémisses. A partir du constat de la validité d'une propriété dépendant d'un entier naturel n sur des cas particuliers, on la valide par une démonstration pour une situation générale. Cette démonstration est donc réalisée en enchaînant trois étapes :

- La phase 1 consiste à vérifier la propriété proposée sur un cas particulier. Elle correspondra à la plus petite valeur n_0 du naturel n à partir de laquelle la propriété proposée à la démonstration sera vraie (en général pour $n = 0$ ou $n = 1$). Cette phase est celle de l'*initialisation*, on contrôle qu'il existe bien une première valeur qui enclenche le processus
- La phase 2 consiste à démontrer que si la propriété est vraie pour une valeur p indéfinie supérieure ou égale à la valeur particulière n_0, elle est alors vraie pour la valeur suivante $p + 1$. Cette étape est celle de l'*hérédité*, tout successeur reçoit la propriété de son prédécesseur.
- La phase 3 consiste à formuler la procédure et sa conclusion : la propriété est vraie pour la valeur n_0. Si elle est vraie pour p, alors elle est vraie pour $p + 1$, on peut donc en conclure qu'elle s'étend à tout entier $n \geq n_0$. La propriété est vraie pour toute valeur de n supérieure ou égale à n_0. Cette dernière phase, en s'appuyant sur les phases 1 et 2, *valide à l'infini* la propriété énoncée et lui confère son caractère de généralité.

Cette procédure « démonstration par récurrence » approchée par divers mathématiciens anciens, al-Karaji (? - 1023), as-Samw'al (? - 1175), Pascal (1623 - 1662), a été théorisée définitivement au siècle dernier par Henri Poincaré (1854 - 1912). Il faut remarquer que cette méthode ne fait rien découvrir, elle permet seulement de valider des propriétés « inventées » par ailleurs. C'est dans l'élaboration de la formule de récurrence que réside la difficulté essentielle.

1.2 Exemples

Exemple 1 Examinons les sommes d'entiers successifs

1 + 2	3 + 0	3
(1 + 2) + 3	3 + 3	6
(1 + 2 + 3) + 4	6 + 4	10
(1 + 2 + 3 + 4) + 5	10 + 5	15
(1 + 2 + 3 + 4 + 5) + 6	15 + 6	21

Nous écartons ici la difficulté essentielle, à savoir, déterminer à partir de ces cas particuliers la formule de récurrence qui donne la somme des n premiers entiers. On suppose que pour $n \geq 2$, on a $1 + 2 + \ldots + n = \frac{n(n+1)}{2} = S_{1,n}$. Dans $S_{1,n}$ le 1 indique qu'il s'agit de nombres à la puissance 1 et le n indique qu'on somme depuis 1 jusqu'à la valeur indiquée par n.

Phase 1 : pour $n = 2$ (donc ici $n_0 = 2$) on a $S_{1,2} = 1 + 2 = 3$ et $\frac{2(2+1)}{2} = 3$. La propriété est donc vraie pour $n = 2$.

Phase 2 : on suppose que pour une valeur naturelle indéterminée p supérieure ou égale à 2 on a $S_{1,p} = 1 + 2 + ... + (p - 1) + p = \frac{p(p+1)}{2}$; c'est-à-dire que la somme des entiers naturels depuis 1 jusqu'au $p^{\text{ième}}$ terme est égale au demi produit du dernier terme de la somme (p) par son successeur (le dernier augmenté d'une unité : $p + 1$). On se propose alors de démontrer qu'il en est de même pour $1 + 2 + ... + p + (p + 1)$, somme des entiers naturels depuis 1 jusqu'à $p + 1$. Cette somme peut être écrite de façon à mettre en évidence ce qui a été supposé vrai $[1 + 2 + ... + p] + (p + 1) = \frac{p(p+1)}{2} + (p + 1) = \frac{p(p+1)}{2} + \frac{2(p+1)}{2} = \frac{(p+1)(p+2)}{2} = \frac{(p+1)[(p+1)+1]}{2}$. On constate que ce résultat est le demi produit du dernier terme de la somme $(p + 1)$ par $[(p + 1) + 1]$ son successeur. Il s'agit bien de la propriété proposée en remplaçant p par $p + 1$.

Phase 3 : nous avons vérifié que pour $n = 2$, $S_{1,n} = \frac{n(n+1)}{2}$ est vraie. Nous avons démontré que si $S_{1,p} = \frac{p(p+1)}{2}$ pour un naturel p indéterminé supérieur ou égal à 2 alors $S_{1,(p+1)} = \frac{(p+1)[(p+1)+1]}{2}$. On peut en conclure que pour tout naturel $n \geq 2$ on a l'égalité suivante $S_{1,n} = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Remarque Ce résultat est à retenir, la somme, de 1 à n, des n premiers entiers est :

$$\frac{n(n+1)}{2}.$$

Exemple 2 : « Tout nombre P_n qui s'écrit $7^{2n+1} + 1$ pour n entier naturel est divisible par 8 ».

Phase 1 : pour $n = 0$, on a $P_0 = 7^{2(0)+1} + 1 = 7 + 1 = 8$, la propriété est vraie.

Phase 2 : supposons la propriété vraie pour un naturel p indéterminé, $P_p = 7^{2p+1} + 1$ est divisible par 8, c'est-à-dire que $P_p = 7^{2p+1} + 1 = 8k$, le nombre k étant un naturel. On a par conséquent $P_{p+1} = 7^{2(p+1)+1} + 1 = 7^{(2p+1)+2} + 1 = 7^{2p+1} \times 7^2 + 1 = 49 \times 7^{2p+1} + 1 =$

$(48 + 1)\times 7^{2p+1} + 1 = 48\times 7^{2p+1} + (7^{2p+1} + 1) = 6\times 8\times 7^{2p+1} + 8k = 8(6\times 7^{2p+1} + k)$. Or comme le nombre $K = 6\times 7^{2p+1} + k$ est un entier car somme et produit d'entiers, $8(6\times 7^{2p+1} + k) = 8K$ est un multiple de 8. On en conclut que P_{p+1} est un multiple de 8.
Phase 3 : on a vérifié que pour $n = 0$, P_n est divisible par 8. On a démontré que si P_p est divisible par 8 pour une valeur p entière indéterminée alors P_{p+1} est divisible par 8. On peut en conclure que pour tout entier naturel n, P_n est divisible par 8.

Exemple 3 Proposition : « Pour tout n naturel supérieur ou égal à 1, $a_n = 7^n + 2$ est divisible par 3 ».
Phase 1 : pour $n = 1$, $a_1 = 7^1 + 2 = 9 = 3\times 3$, donc c'est vrai.
Phase 2 : supposons que, pour un entier p indéterminé supérieur ou égal à 1, on ait $a_p = 7^p + 2 = 3k$ avec k entier. On en déduit que $a_{p+1} = 7^{p+1} + 2 = 7 \times 7^p + 2 = 7(3k - 2) + 2$ car on a supposé que $7^p = 3k - 2$. On a alors $a_{p+1} = 21\ k + 12 = 3(7k + 4)$ donc que a_{p+1} est divisible par 3.
Phase 3 : on a vérifié que pour $n = 1$, a_n est divisible par 3. On a démontré que si a_p est divisible par 3 pour une valeur p entière indéterminée alors a_{p+1} est divisible par 3. On peut en conclure que pour tout entier naturel n, $a_n = 7^n + 2$ est divisible par 3.

Remarque La question de « l'invention » des propositions de récurrence a été évoquée précédemment. Examinons la situation simple suivante (dans d'autres situations autrement plus complexes la réponse peut s'avérer beaucoup moins évidente) : « Pour tout naturel $n \geq 100$, $11^n + 1$ est un multiple de 10 ». La vérification que c'est vrai pour $n =$ 100 n'étant pas immédiate par un simple calcul numérique, examinons d'abord la phase 2, c'est-à-dire qu'on suppose que pour un entier indéterminé p supérieur ou égal à 100, $11^p + 1 = 10k$. Examinons alors $11^{p+1} + 1 = 11\times 11^p + 1 = (10 + 1)\times 11^p + 1 = 10\times 11^p + (11^p + 1) = 10\times 11^p + 10k = 10(11^p + k)$, la propriété s'avère héréditaire. Reste donc la phase 1. En fait, toute puissance de 11, a une écriture se terminant par 1 (on peut le démontrer par récurrence !) et donc tout nombre $11^n + 1$ a une écriture se terminant par un 2. Il ne peut être divisible par 10 car un nombre doit se terminer par un 0 pour être divisible par 10. Sur ce cas on constate donc qu'on peut montrer qu'une propriété est héréditaire sans qu'elle soit vraie. La réalisation des phases 1 et 2 est donc essentielle.

■ **Exercice 1**
Démontrer par récurrence que la somme des carrés des n premiers entiers notée $S_{2,n}$ est :

$$\frac{n(n+1)(2n+1)}{6}.$$

Aide : contrôler par développement que $(n + 2)(2n + 3) = 2n^2 + 7n + 6$.

■ **Exercice 2**
1. Calculer $1^3 + 2^3$, puis $1^3 + 2^3 + 3^3$ et $1^3 + 2^3 + 3^3 + 4^3$.
2. Comparer ces résultats respectivement avec $S_{1,2}$, $S_{1,3}$ et $S_{1,4}$. Quelle généralisation ces résultats suggèrent-ils ?
3. Démontrer par récurrence ce résultat général.

■ **Exercice 3**
Démontrer par récurrence que pour tout n entier naturel, le nombre $P_n = n^3 - n$ est divisible par 3.
Aide : vérifier par développement que $(p + 1)^3 = p^3 + 3p^2 + 3p + 1$.

■ **Exercice 4**
Démontrer par récurrence que pour tout naturel n, $A_n = 3^{2n} - 2^n$ est divisible par 7.

2. Division euclidienne

2.1 Définition

Cette notion a déjà été abordée dans l'ouvrage consacré à la classe de première.
Effectuons la division avec reste de 8 532 par 13

8532	13
073	656
082	
04	

Cette opération donne pour résultat 8 532 = 13× 656 + 4. Dans cette écriture 8 532 est le dividende, 13 le diviseur, 656 le quotient et 4 le reste. Le reste a la particularité d'être strictement inférieur au diviseur.
Plus généralement la division euclidienne d'un entier naturel a par un entier naturel non nul b, consiste à déterminer les naturels q et r tels que l'on ait $a = bq + r$ et $0 \leq r < b$.

<u>Définition 1</u> Quels que soient les deux entiers naturels *a* et *b* tels que *b* soit non nul, il existe des entiers naturels *q* et *r* uniques tels que : $a = bq + r$ et $0 \leq r < b$.

Dans le cadre de ce programme, l'existence et l'unicité des entiers q et r pour tout couple $(a ; b) \in \mathbb{N} \times \mathbb{N}^*$ est admise. L'écriture $(a ; b) \in \mathbb{N} \times \mathbb{N}^*$ signifie que a est un entier naturel quelconque et que b est un entier naturel non nul.

2.2 Écriture d'un algorithme de division euclidienne

Un ***algorithme*** est un procédé de calcul. Il s'agit donc ici de mettre en évidence une méthode dont l'exécution pas à pas, appliquée à deux entiers naturels a et b, conduit à la connaissance des entiers q et r.

	A	B
1	Valeur de *a*	Valeur de *b*
2		
3	Quotient *q*	=ENT(A2/B2)
4	Reste *r*	=A2 – B2*B3

Un tableur ou une calculatrice réalisent une division décimale à l'aide de la commande « division » notée « / » ou « ÷ ». La valeur de a est entrée dans la cellule A2, celle de b dans la cellule B2. Ensuite la commande « A2/B2 » effectue le calcul du nombre a/b. La commande « ENT » donne la partie entière de cette expression (le nombre avant la virgule). On a $0 \leq r < b$ et, par addition de bq, on obtient

$bq + 0 \leq bq + r < bq + b$ soit $bq \leq a < b(q + 1)$ ou encore que $q \leq \frac{a}{b} < q + 1$. Ceci indique que le quotient $\frac{a}{b}$ est compris entre les nombres successifs q et $q + 1$, on peut conclure que la commande « = ENT(A2/B2) » donne pour résultat la valeur de q. Cette valeur est indiquée dans la cellule B3. La commande « B2*B3 » indique le produit du contenu de la cellule B2, la valeur b, par celui de la cellule B3, la valeur q. Il s'agit donc du calcul du produit bq. La commande « =A2 – B2*B3 » effectue la différence du contenu de la cellule A2 et de bq. Il s'agit donc du calcul de $a – bq$. Or, comme on sait que $a = bq + r$ et donc que $a – bq = r$, la cellule B4 contient donc la valeur de r.

■ **Exercice 5**
La division euclidienne de l'entier naturel a par l'entier naturel b donne pour quotient q et pour reste r. La division euclidienne de $(a + 15)$ par $(b + 5)$ donne q pour quotient et r pour reste. Déterminer la valeur de q.

■ **Exercice 6**
D'une part, la division euclidienne de l'entier naturel a par 7 donne pour reste 3 et, d'autre part, $100 \leq a \leq 120$. Déterminer les valeurs possibles de a.

3. Multiples dans Z

3.1 Multiples d'un entier naturel dans Z

Le programme de première a défini les multiples d'un entier naturel dans IN. Dire qu'un entier naturel a est multiple d'un entier naturel b non nul signifie qu'il existe un entier naturel k tel que $a = b \times k$ ou encore bk. On dit aussi que b est un diviseur de a. Ainsi a-t-on 28 multiple de 4 car $28 = 4 \times 7$ et 4 qui est diviseur de 28.
Dire que l'entier naturel a est divisible par l'entier naturel b est équivalent à dire que a est multiple de b. Les propositions « *a est multiple de b* » et « *b est diviseur de a* » signifient la même chose. L'extension à l'ensemble des entiers relatifs Z conduit à la définition qui suit.

Définition 2 Dire que l'entier relatif a est multiple de l'entier naturel b non nul signifie qu'il existe un entier relatif k tel que $a = b \times k$ ou encore bk. Cela consiste donc à compléter la liste des naturels multiples de b par leurs opposés (à chaque entier naturel k on associe son opposé $– k$).

Rappel : valeur absolue
Le nombre a étant un entier relatif, le nombre positif noté $|a|$ est égal à a si $a \geq 0$ et égal à $– a$ si $a \leq 0$.
Certaines propriétés établies pour les multiples dans IN sont vraies pour les multiples dans Z. On retiendra en particulier les théorèmes suivants :

Théorème 1 Si b est un entier strictement positif et si a est un multiple non nul de b, alors : $0 < b \leq |a|$.

Nous savons que si a est un naturel non nul multiple de l'entier naturel b, $0 < b \leq a$. Si a est négatif, on peut écrire cette relation pour $-a$ qui est positif $0 < b \leq -a$. La multiplication par -1 donne $a \leq -b < 0$ et comme $-b < b$ du fait que b est positif, on en conclut que $a \leq b \leq -a$ ce qui signifie $0 < b \leq |a|$ car $b \neq 0$.

Théorème 2 **Si a est multiple de b et si b est multiple de c, alors a est multiple de c.**
Le nombre a est multiple de b c'est-à-dire $a = kb$ avec k entier et b multiple de c donc $b = k'c$ avec k' entier. Finalement $a = k(k'c) = (kk')c = Kc$, donc a est multiple de c.

Théorème 3 **Si a et b sont des multiples de l'entier c, alors, pour tous les entiers relatifs m et n, le nombre $ma + nb$ est multiple de c.**
Si les nombres a et b sont des multiples de l'entier c, c'est que $a = kc$ et $b = k'c$ avec k et k' entiers, alors $ma + nb = m(kc) + n(k'c) = (mk + nk')c = Kc$ et donc $ma + nb$ est multiple de c.

Remarques ***Implication, condition nécessaire et condition suffisante, équivalence*** : nous avons démontré ici une implication. La propriété P_1 est « a et b sont des multiples de l'entier c », la propriété P_2 est « Pour tous entiers relatifs m et n, $ma + nb$ est multiple de c », elle s'exprime par « Si P_1 alors P_2 ».
La propriété P_1 vraie est une condition suffisante pour que la propriété P_2 soit vraie car P_2 est vraie lorsque P_1 est vraie. Ou encore, il est suffisant que la propriété P_1 soit vraie pour que la propriété P_2 soit vraie.
A-t-on « P_2 implique P_1 » ? Si « pour tous les entiers relatifs m et n on a $ma + nb$ multiple de c », alors « c'est en particulier vrai pour $m = 1$ et $n = 0$ et donc $1a + 0b = a$ est multiple de c. De même pour $m = 0$ et $n = 1$, b est multiple de c ». On a donc P_2 implique P_1, la condition P_2 vraie est suffisante pour que P_1 soit vraie.
En même temps on a démontré que P_1 vraie est une condition nécessaire pour que P_2 soit vraie car si a ou b n'étaient pas multiples de c nous n'aurions pas « $ma + nb$ multiple de c pour tous les entiers relatifs m et n ».
P_1 implique P_2 et P_2 implique P_1 peut se résumer en disant que P_1 et P_2 sont équivalentes. On peut dire que « P_1 est une condition nécessaire et suffisante de P_2 ».

Attention ! L'essentiel réside dans l'utilisation du quantificateur « Pour tous ». La propriété P' « $ma + nb$ est multiple de c » n'a pas le même sens. Ce n'est pas parce que a et b ne sont pas multiples de c qu'il n'existe pas de nombres entiers m et n tels que le nombre $ma + nb$ soit un multiple de c. Ici un exemple suffit pour le prouver : 7 n'est pas un multiple de 5, 8 n'est pas un multiple de 5 or $1 \times 7 + 1 \times 8 = 15$ est un multiple de 5. On peut donc dire que P_1 n'est pas une condition nécessaire de la propriété P'.

■ **Exercice 7**
1. Vérifier que l'entier 25 212 521 est multiple de 73 et de 137.
2. Donner un autre entier composé de deux fois la même série de 4 chiffres. Fait-on la même vérification ?
3. Effectuer le produit de 73 par 137 et expliquez le phénomène.

■ **Exercice 8**
Combien y a-t-il de multiples positifs de 17 inférieurs à 2000 ?

■ **Exercice 9**
Démontrer par ***disjonction des cas*** (nombre pair puis nombre impair) que tout nombre a et son carré, ont la même parité.

■ **Exercice 10**
Les nombres a et b sont des entiers relatifs. Montrer que si $a^2 + b^2$ est un multiple de 2 alors $(a + b)^2$ est multiple de 2. La réciproque est-elle vraie ?

■ **Exercice 11**
Le nombre a est un multiple du nombre c. Démontrer que si b multiple de a alors b est un multiple de c. La réciproque est-elle vraie ?

■ **Exercice 12**
Quel est l'ensemble des entiers relatifs n tels que 16 est multiple de $n + 7$?

■ **Exercice 13**
Déterminez tous les couples $(x ; y)$ d'entiers naturels tels que $(x + 2)(y - 1) = 10$.

■ **Exercice 14**
Déterminer le nombre a compris entre 1 et 9 tel que le nombre $\overline{3\,5a4}$ soit divisible par le nombre 9.

■ **Exercice 15**
Déterminer les nombres a et b compris entre 1 et 9 tels que l'entier $\overline{2\,a3b}$ soit divisible par 4 et par 3.

■ **Exercice 16**
On considère le nombre $A = n(n + 1)(2n + 1)$.
1. Démontrer que :
   a- A est un multiple de 2.
   b- A est un multiple de 3 (par disjonction des cas : on distinguera $n = 3k$, $n = 3k + 1$ et $n = 3k + 2$).
2. Le nombre A est-il divisible par 5 pour tout n pair ?

■ **Exercice 17**
1. Montrer qu'une condition nécessaire pour qu'un naturel a soit divisible par 4 est qu'il soit pair.
2. Est-ce une condition suffisante ?

3.2 Ensemble des multiples strictement positifs d'un entier naturel

On considère l'entier naturel non nul a. L'ensemble de ses multiples strictement positifs (dans $\mathbb{N}^*$) est $M_a = \{m = ka, k$ étant un entier naturel quelconque non nul$\}$. Cet ensemble a un nombre infini d'éléments, cela peut se démontrer en utilisant un ***raisonnement par l'absurde***. En effet si ce n'était pas le cas, cet ensemble admettrait un plus grand élément noté G_a. Ce naturel G_a étant élément de M_a c'est qu'il existe un entier naturel k tel que $G_a = ka$. Or si on considère le nombre $(k + 1)a$, ce nombre est un multiple de a et il est plus grand que G_a car $k + 1 > k$ et donc $(k + 1)a > ka$. On peut en conclure que G_a

n'est pas le plus grand élément de M_a ce qui est contraire à notre hypothèse de départ et nous permet de conclure que cette hypothèse est fausse et donc que M_a est infini.

Plus petit commun multiple : a et b étant deux naturels non nuls on désigne par M_a et M_b l'ensemble de leurs multiples respectifs. Les multiples communs à ces deux ensembles appartiennent à M_a **et** M_b c'est-à-dire à $M = M_a \cap M_b$. Cet ensemble M n'est pas vide car il contient au moins un élément : ab. Il ne contient que des éléments positifs car M_a et M_b ne contiennent que des éléments positifs. On peut donc en conclure que M contient un plus petit élément, il est appelé « plus petit commun multiple ».
Dans les cas simples on peut se contenter de dresser la liste des premiers multiples de a et de b jusqu'à parvenir à un premier élément commun qui sera le plus petit commun multiple.
Exemple La liste des premiers multiples de 24 est 24, 48, 72, 96, 120, 144, 168, 192, 216, 240, 264, 288, 312, 336, 360, 384. Pour 15, c'est : 15, 30, 45, 60, 75, 90, 105, 120. On peut donc en conclure que le plus petit commun multiple de 24 et 15 est 120.

4. Congruences

4.1 Définition et premières propriétés

Définition 3 : *n* étant un entier naturel supérieur ou égal à 2, on dira que deux nombres entiers *a* et *b* sont congrus modulo *n* si et seulement si leur différence est un multiple de *n*.

Le nombre n étant un entier naturel supérieur ou égal à 2, « $a \equiv b \bmod n$ » est équivalent à « Il existe un entier relatif k tel que $a - b = k \times n$ ».

Théorème 4 Deux nombres entiers *a* et *b* sont congrus modulo *n* si et seulement si ils ont même reste *r* par leur division euclidienne par *n*. Dans ce cas *a* et *b* sont congrus à ce reste *r*.
Supposons que $a \equiv b \bmod n$, c'est que $a - b = k \times n$. Effectuons la division euclidienne de a et b par n. On détermine les entiers q, r, q' et r' tels que $a = nq + r$ avec $0 \leq r < n$ et $b = nq' + r'$ avec $0 \leq r' < n$. Par différence on obtient $a - b = (nq + r) - (nq' + r') = (nq - nq') + (r - r') = n(q - q') + (r - r')$. L'hypothèse indique que ce nombre est multiple de n, c'est-à-dire $(nq - nq') + (r - r') = k \times n$ et alors $(r - r') = n[k - (q - q')]$. Le nombre $(r - r')$ est un multiple de n. On a $0 \leq r < n$ et $0 \leq r' < n$, cela donne $0 \leq r < n$ et $-n < -r' \leq 0$. Par addition, on obtient : $-n < r - r' < n$. Or le seul multiple de n compris strictement entre $-n$ et n est 0 donc $r - r' = 0$ ou encore $r = r'$.
Réciproquement, effectuons la division euclidienne de a et b par n. Si le reste est le même, c'est que $a = nq + r$ et $b = nq' + r$ avec $0 \leq r < n$. Par différence on obtient alors $a - b = (nq + r) + (nq' + r) = nq - nq' = n(q - q')$. La différence est un multiple de n, donc $a \equiv b$ modulo n.

Exemple 1
Posons $n = 5$ et soient $a = 237$ et $b = 122$. On a alors $237 - 122 = 115 = 23 \times 5$ et donc $237 \equiv 122 \bmod 5$.