Table des matières

0- Préliminaire

L'arithmétique concerne les entiers.

Avant de commencer, rappelons quelques notions simples sur les entiers naturels.

L'ensemble des entiers naturels est noté $\mathbb{N}$ et une construction usuelle de $\mathbb{N}$ est faite à partir des axiomes de Peano (voir aussi Dedekind):

1. l'élément appelé zéro et noté: 0, est un entier naturel.
2. Tout entier naturel n a un unique successeur, noté $s(n)$
3. Aucun entier naturel n'a 0 pour successeur.
4. Deux entiers naturels ayant même successeur sont égaux.
5. Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est égal à $\mathbb{N}$.

Le premier axiome permet de poser que l'ensemble des entiers naturels n'est pas l'ensemble vide,

le troisième qu'il possède un premier élément

et le cinquième est celui qui justifie le raisonnement par récurrence.

Une autre conséquence de cette construction est que tout sous-ensemble **non vide** $\mathcal{E}$ de $\mathbb{N}$ **a un plus petit élément** (c'est-à-dire, un élément qui est **dans** $\mathcal{E}$ et qui est inférieur à tous les autres éléments de $\mathcal{E}$.)
et tout sous-ensemble **fini** $\mathcal{F}$ de $\mathbb{N}$ **a un plus grand élément** (c'est-à-dire, un élément qui est **dans** $\mathcal{F}$ et qui est supérieur à tous les autres éléments de $\mathcal{F}$).
Ces résultats sont faux dans les autres ensembles numériques.
Dans $\mathbb{R}$, par exemple, l'intervalle]0;1[est borné, mais, ne possède ni plus petit élément, ni plus grand élément.

L'ensemble $\mathbb{Z}$ (ensemble des entiers relatifs) s'obtient en symétrisant l'ensemble $\mathbb{N}$ des entiers naturels.
(Autrement dit : Dans $\mathbb{N}$, l'équation $2 + x = 0$ n'a aucune solution.
on crée un nouvel ensemble tel que $2 + x = 0$ a une et une seule solution).
Dans notre système de numération décimale: $\mathbb{N} = \{0; 1; 2; 3; ... \}$
$\mathbb{Z} = \{...; -4; -3; -2; 0; 1; 2; 3; ...\}$
L'astérisque (*) est le symbole utilisé pour noter un ensemble sans l'élément 0. $\mathbb{N}^* = \mathbb{N} - \{0\}$ et $\mathbb{Z}^* = \mathbb{Z} - \{0\}$

I- Divisibilité dans $\mathbb{Z}$

I-1- Multiples d'un entier relatif

I-1-1- Définition:

Soit m un entier ($m \in \mathbb{Z}$)

m est un multiple de l'entier b signifie qu'il existe un entier c tel que $m = bc$.

I-1-2- Exemples:

* 15 est un multiple de 3 car, $15 = 3\times5$ et $5 \in \mathbb{Z}$.
** -12 est un multiple de 3 car, $-12 = 3\times(-4)$ et $-4 \in \mathbb{Z}$.
*** L'ensemble des multiples de 3 est noté $3\mathbb{Z}$. $3\mathbb{Z} = \{... ; -15 ; -12 ; -9 ; -6 ; -3 ; 0 ; 3 ; 6 ; 9 ; ...\}$
**** Quel est l'ensemble des multiples de 2 ? de1 ? de 0 ?

I-1-3- Un raisonnement par l'absurde:

Montrer que 15 n'est pas un multiple de 2.

Démonstration

I-2- Divisibilité dans $\mathbb{Z}$.

I-2-1- Définition:

Dire que l'entier b divise l'entier a signifie qu'il existe un entier c tel que $a = bc$.

b est un diviseur de a
a est divisible par b Notation: $b \mid a$ (b divise a)
(Nécessairement, un diviseur est un entier non nul : voir remarque ci-dessous)

I-2-2-Remarques:

* 0 ne divise aucun entier non nul, car, si $a \neq 0$, $a \neq 0\times c$.
** 0 est divisible par tout nombre entier, car, $0 = b\times0$
*** 1 divise tout nombre entier, car, $a = 1\times a$
**** -1 divise tout nombre entier, car, $a = (-1)\times(-a)$
***** tout entier a divise a, car, $a = a\times1$

I- 3- Propriétés

I- 3- 1: propriété 1

Énoncé : Si b divise a alors $-b$ divise a

Preuve:

I- 3- 2: propriété2

Énoncé : Si b divise a et si $a \neq 0$ alors $|b| \leqslant |a|$

Preuve:

Cas particulier: $b \in \mathbb{N}$ et $a \in \mathbb{N}^*$ et $b \mid a$ implique $b \leqslant a$
Conséquence : Tout entier a non nul possède un nombre fini de diviseurs puisqu'un diviseur b de a vérifie : $-a \leqslant b \leqslant a$.

I- 3- 3: propriété 3

Énoncé : Si b divise a et si a divise b alors $a = b$ ou $a = -b$

***Preuve*:**

I- 3- 4: *Transitivité de la relation de divisibilité*

Énoncé : Si a divise b et si b divise c alors a divise c
(Si $a \mid b$ et $b \mid c$ alors $a \mid c$)

***Preuve*:**

I- 3- 5: *Divisibilité d'une combinaison linéaire d'entiers à coefficients entiers*

Énoncé : Si a divise b et c alors a divise $b + c$, $b - c$, $bx + cy$ où $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$
(x et y étant des entiers, si $a \mid b$ et $a \mid c$ alors $a \mid bx + cy$)

***Preuve*:**

I- 3- 6: Divisibilité et produit

Énoncé : Si a divise b alors a divise bc quel que soit l'entier c
(c étant un entier, si $a \mid b$ alors $a \mid bc$)

***Preuve*:**

Exercice*:*

Trouver tous les diviseurs communs positifs à $9k + 2$ et $12k + 1$ où $k \in \mathbb{N}$
Remarque: *il existe au moins un diviseur positif commun: l'entier naturel 1*
Rédaction: Soit d un diviseur commun à $9k + 2$ et $12k + 1$.
alors d divise toute combinaison linéaire d'entiers $x(9k + 2) + y(12k + 1)$ (x, y, k sont des entiers)
(On choisit alors x et y de façon à "éliminer" k)
d divise donc $4(9k + 2) - 3(12k + 1) = 5$
(On a montré: Si d existe alors (nécessairement) d est un diviseur de 5)
Conclusion: Puisque d est positif, les seules valeurs possibles de d sont 1 et 5.
Attention: k étant choisi, 5 n'est pas nécessairement un diviseur de $9k + 2$ et $12k + 1$
Exemple: $k = 2$ $9 \times 2 + 2 = 20$ et $12 \times 2 + 1 = 25$ $5 \mid 20$ et $5 \mid 25$
$k = 3$ $9 \times 3 + 2 = 29$ et $12 \times 3 + 1 = 37$ 5 ne divise ni 29, ni 37
On étudiera la réciproque plus tard.

I-4- Deux définitions : nombres premiers entre eux et nombres premiers

1) (Dans $\mathbb{Z}$). Deux **nombres** entiers sont **premiers entre eux** si et seulement si leurs seuls diviseurs communs sont -1 et 1.

2) (Dans $\mathbb{N}$). Un entier naturel p est un **nombre premier** si et seulement si il possède exactement deux diviseurs 1 et p lui-même.

(Le premier nombre premier est 2).

Ces notions seront exploitées plus loin dans le cours.

II- Division euclidienne

II- 1- Division euclidienne dans $\mathbb{N}$.

(Axiome d'Archimède :

Soit b un entier naturel non nul.

Pour tout entier naturel a, il existe un entier naturel n tel que a < nb)

Théorème :
a et b étant deux entiers positifs, et, b étant non nul ($a \in \mathbb{N}$ et $b \in \mathbb{N}^*$)
il existe un couple unique (q, r) d'entiers positifs tel que $a = bq + r$ et $0 \leqslant r < b$

Démonstration:

II- 2- Définition

Effectuer la division euclidienne dans $\mathbb{N}$ de a par b ($b \neq 0$), c'est déterminer le couple (q, r) d'entiers naturels tel que $a = bq + r$ et $0 \leqslant r < b$

q est le quotient, r est le reste, a est le dividende et b est le diviseur.

Conséquence: b divise a équivaut à $r = 0$ dans la division euclidienne de a par b.

Remarques :

* Ne pas confondre : le diviseur dans la division euclidienne et " b est un diviseur de a "

** dans la division euclidienne de a par b, il y a b restes possibles ($r \in \{0 ; 1 ; 2 ; ... ; b-1\}$).

II- 3- Division euclidienne dans $\mathbb{Z}$

La division euclidienne se généralise dans $\mathbb{Z}$ avec $a = b\,q + r$ et $0 \leqslant r < |b|$

Important: Le **reste** r est toujours **positif.**

Exemple:

a	b	$a = bq + r$ avec $0 \leqslant r < \lvert b\rvert$	q	r
37	11	$37 = 11\times 3 + 4$	3	4
37	–11	$37=(-11)\times(-3)+4$	–3	4
–37	11	$-37=11\times(-4)+7$	–4	7
–37	–11	$-37=(-11)\times 4+7$	4	7

***Exercices*:**

* Quand on veut étudier une propriété sur un entier quelconque a, il est utile de remarquer que $a = bq + r$ avec $0 \leqslant r < |b|$.

Le nombre de possibilités d'écrire a est donc fini ($a = bq$ ou $a = bq + 1$ ou .... ou $a = bq + (b - 1)$) et tous ces cas sont disjoints deux-à-deux.

** b étant un entier naturel, une liste de b entiers consécutifs contient un multiple de b.

Exemple : L'un des entiers $n - 1$; n ; $n + 1$ est un multiple de 3.

1) Disjonction des cas

Il est important de remarquer qu'on peut toujours écrire $a = bq + r$ avec $0 \leqslant r < |b|$
Quand b est connu, on peut écrire tous les cas possibles pour r.

Énoncé : Démontrer que, pour tout entier naturel n, $a = n(n + 1)(2n + 1)$ est divisible par 3.

Démonstration :

On peut considérer trois cas: (q étant un entier)

$n = 3q$	$a = 3q(n + 1)(2n + 1)$	est divisible par 3
$n = 3q + 1$	$a = n(n + 1)[2(3q+1) + 1] = 3n(n + 1)(2q + 1)$	est divisible par 3
$n = 3q + 2$	$a = n(3q + 2 + 1)(2n + 1) = 3n(q + 1)(2n + 1)$	est divisible par 3

On a ainsi prouvé: Pour tout entier naturel n, $a = n(n + 1)(2n + 1)$ est divisible par 3.

Complément :

L'un des entiers n ou n + 1 est pair. Le produit n(n + 1)(2n + 1) est divisible par 2 et par 3.
2 et 3 sont premiers entre eux. Le produit n(n + 1)(2n + 1) est divisible par 6.

2) Un système en arithmétique

Résoudre dans $\mathbb{N}^3$ le système suivant: $\begin{cases} ab+bc+ca=abc \quad (1) \\ 0<a<b<c \quad (2) \end{cases}$

Remarques: Lorsqu'on a une suite d'inégalités: $x_1 < x_2 < \ldots < x_n$ (n termes), on en déduit un encadrement de la somme des x_i

Puisque pour $1 \leqslant i \leqslant n$, on a: $x_1 < x_i < x_n$, alors $nx_1 < x_1 + x_2 + \ldots + x_n < nx_n$

Par exemple dans cet énoncé: $3a < a + b + c < 3c$

Une méthode: à partir de l'inégalité (2), on cherche les encadrements des termes de la somme de (1)

Puisque a, b et c sont des entiers **strictement positifs** en multipliant chaque membre de (2) successivement par a, b et c, on a:
$0 < b < c$ implique $0 < ab < ac$ (3)
$0 < a < c$ implique $0 < ab < bc$ (4)
$0 < a < b$ implique $0 < ac < bc$ (5)
De (3) et (5), il vient: $ab < ac < bc$ (6) et (voir remarque): $3ab < ab + ac + bc < 3bc$ (7)
D'après (1), les solutions du système doivent vérifier: $3ab < abc < 3bc$ (8)
Puisque $ab \neq 0$, on obtient de (8): $3 < c$ et puisque $bc \neq 0$, $a < 3$.
Les valeurs possibles pour a sont: 1 et 2
Si $a = 1$, on a dans (1): $b + bc + c = bc$, soit $b + c = 0$ ce qui est impossible dans $\mathbb{N}$.
Si a = 2, on a dans (1): $2b + bc + 2c = 2bc$, soit $2(b + c) = bc$ (9)
Or, $b < c$, d'où, (voir remarque) $2b < b + c < 2c$ (10)
D'après (9) et (10), $4b < bc < 4c$ (11)
De (11), il vient: $4 < c$ et $b < 4$.
Or, $a = 2$ et $a < b$. La seule valeur possible pour b est 3.
En faisant $b = 3$ dans (9): $6 + 2c = 3c$. On en déduit: $c = 6$
On a montré: s'il existe un triplet (a,b,c) solution du système, le seul triplet possible est (2;3;6)
La réciproque est obligatoire: $2\times3 + 3\times6 + 6\times2 = 36$ et $2\times3\times6 = 36$
$0 < 2 < 3 < 6$
Le système est vérifié.
Conclusion: Il existe un et un seul triplet de $\mathbb{N}^3$ solution du système: le triplet (2; 3; 6)

3) Factorisation
n étant un entier supérieur ou égal à 5, montrer que les entiers $a = n^3 - n^2 - 12n$ et $b = 2n^2 - 7n - 4$ sont divisibles par $(n - 4)$
Une méthode: on commence par diviser le terme de plus haut degré par $(n - 4)$ en ligne et ainsi de suite c'est-à-dire: $n^3 = n^2(n-4) + 4n^2$ ...
Ce qui donne: $a = n^3 - n^2 - 12n = n^2(n-4) + 4n^2 - n^2 - 12n$
$= n^2(n-4) + 3n^2 - 12n$
$= n^2(n-4) + 3n(n-4) + 12n - 12n$
$= (n^2 + 3n)(n-4)$

$b = 2n^2 - 7n - 4 = 2n(n-4) + 8n - 7n - 4$
$= 2n(n-4) + n - 4$
$= (2n+1)(n-4)$

Une dernière remarque : soustractions successives

Soit b un entier naturel non nul et a un entier naturel.

On ôte b autant de fois qu'il faut (c'est le quotient q) à a … jusqu'à ce qu'il reste un nombre d'éléments strictement inférieur à b, (c'est le reste r).

Illustration : division euclidienne de 154 par 37

154 – 37 = 117 ; 117 – 37 = 80 ; 80 – 37 = 43 ; 43 – 37 = 6

On a donc : $154 = 4\times37 + 6$

III- Congruences

On a utilisé plusieurs fois depuis le début de ce chapitre le fait que pour étudier l'ensemble des entiers, on étudiait par exemple les trois cas:

le sous-ensemble E_0 est l'ensemble des multiples de 3, $n = 3k$ avec k entier.

le sous-ensemble E_1 est l'ensemble des multiples de 3 plus 1, $n = 3k + 1$ avec k entier

le sous-ensemble E_2 est l'ensemble des multiples de 3 plus 2, $n = 3k + 2$ avec k entier.

On a alors trois sous-ensembles de $\mathbb{Z}$ et **chacun d'eux peut être caractérisé** par le fait que tous ses éléments donnent **le même reste** dans la division par 3.

$E_0 = \{..., -9; -6; -3; 0; 3; 6; 9; 12; ....\}$

$E_0 = \{n/\ n = 3k \text{ et } k \in \mathbb{Z}\}$. Un élément quelconque de E_0 est divisible par 3, le reste est 0

$E_1 = = \{..., -8; -5; -2; 1; 4; 7; 10; 13; ....\}$

$E_1 = \{n/\ n = 3k + 1 \text{ et } k \in \mathbb{Z}\}$. Le reste d'un élément quelconque de E_1 dans la division par 3 est 1.

$E_2 = = \{..., -7; -4; -1; 2; 5; 8; 11; 14; ....\}$

$E_2 = \{n/\ n = 3k + 2 \text{ et } k \in \mathbb{Z}\}$. Le reste d'un élément quelconque de E_2 dans la division par 3 est 2.

Pour simplifier, **on va choisir un représentant de l'ensemble** pour travailler sur cet ensemble, et, n'importe quel représentant fera l'affaire.

III- 1 Propriété et définition

Énoncé :

Soit c un entier relatif non nul.

Deux entiers a et b ont le même reste dans la division par c si et seulement si $a - b$ est un multiple de c.

Dans ce cas, on dit que a et b sont congrus modulo c, et, on écrit: $a \equiv b \bmod(c)$ ou $a \equiv b\ (c)$

Preuve:

III- 2- Transitivité de la congruence

Énoncé :

c étant un entier non nul, si $a \equiv a' \bmod(c)$ et $a' \equiv a'' \bmod(c)$ alors $a \equiv a'' \bmod(c)$

Preuve: évident d'après la définition

III-3- Congruence et opérations : compatibilité des opérations et congruences.

Énoncé :

c étant un entier non nul, si $a \equiv a' \bmod(c)$ et $b \equiv b' \bmod(c)$

alors $a + b \equiv a' + b' \bmod(c)$

alors $a - b \equiv a' - b' \bmod(c)$

alors $a.b \equiv a'.b' \bmod(c)$

alors $a^n \equiv a'^n \bmod(c)$

Preuve :

IV- Nombres premiers

IV-1- Définition

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

Conséquences: 0 et 1 ne sont pas premiers.

2 est premier et est le seul entier pair premier.

IV-2- Théorème

Soit n un entier naturel supérieur ou égal à 2, alors

* n admet au moins un diviseur premier

** Si n n'est pas premier, il admet au moins un diviseur premier p tel que $p \leqslant \sqrt{n}$

Preuve:

IV-2-1- Conséquence: critère pour déterminer un nombre premier (crible d'Ératosthène)

Soit n un entier $\geqslant 2$.

Si n n'est divisible par aucun des nombres premiers inférieurs ou égal à $\sqrt{n}$ alors n est premier.

Crible d'Érathostène

On écrit tous les entiers de 1 à 100 (ou une autre valeur) dans un tableau.

Le premier nombre premier est 2, on le sélectionne et on raye tous ses multiples.

Le premier entier non rayé 3 est donc premier, on le sélectionne et on raye tous ses multiples. (À partir de 9)

Le premier entier non rayé est premier, on le sélectionne et on raye tous ses multiples. (À partir de son carré)

X	2	3	X	5	X	7	X	X	X
11	X	13	X	X	X	17	X	19	X
X	X	23	X	X	X	X	X	29	X
31	X	X	X	X	X	37	X	X	X
41	X	43	X	X	X	47	X	X	X
X	X	53	X	X	X	X	X	59	X
61	X	X	X	X	X	67	X	X	X
71	X	73	X	X	X	X	X	79	X
X	X	83	X	X	X	X	X	89	X
X	X	X	X	X	X	97	X	X	X
101	X	103	X	X	X	107	X	109	X
X	X	113	X	X	X	X	X	X	X
X	X	X	X	X	X	127	X	X	X
131	X	X	X	X	X	137	X	139	X
X	X	X	X	X	X	X	X	149	X

IV-3- Propriété (Infinité de nombres premiers

Il existe une infinité de nombres premiers

Preuve: (démonstration d'Euclide)

IV-4- Décomposition en produit de facteurs premiers

IV-4-1- Théorème

Soit n un entier supérieur ou égal à 2, alors n se décompose en un produit de facteurs premiers et cette décomposition est unique à l'ordre près des facteurs.

Exemple: $360 = 2\times180 = 2\times2\times90 = 2\times2\times2\times45 = 2\times2\times2\times3\times15 = 2\times2\times2\times3\times3\times5 = 2^3\times3^2\times5$

$2^3\times3^2\times5$ est la décomposition de 360 en un produit de facteurs premiers.

Démonstration :

Existence d'une décomposition en facteurs premiers:

Un exemple: 28 n'est pas premier car 28 est divisible par 4 ; il s'écrit donc 4×7.

4 et 7 sont inférieurs à 28, on cherche à décomposer 4 et 7.

7 est premier et 4 s'écrit 2×2.

Comme 2 est premier : $28 = 2^2\times7$

Raisonnement par récurrence :

Initialisation: il est évident que 2 ; 3 ; 4; ... se décomposent un un produit de facteurs premiers.
Hérédité: Supposons que tout entier inférieur ou égal à un entier n est produit d'une famille de nombres premiers.
L'entier suivant $n + 1$ est:
- soit un nombre premier et la propriété est vérifiée.
- soit $n + 1$ est le produit d'un nombre premier p par un entier q.
q, étant un entier inférieur ou égal à n, est le produit de facteurs premiers et par le fait même $p\times q$ est le produit de facteurs premiers.
Conclusion: Par application du principe de récurrence, tous les entiers naturels peuvent s'écrire comme produit de nombres premiers.

Unicité d'une décomposition en facteurs premiers: :

Elle peut se démontrer à l'aide du théorème de Gauss qui sera vu dans le prochain §, mais, cela ne doit pas nous empêcher de réfléchir sur les méthodes :.

Principe à retenir pour démontrer l'unicité :

Pour montrer l'unicité d'une propriété (P) .... on suppose deux façons d'appliquer (P) et on montre qu'elles sont égales (façon directe)

ou on les suppose différentes, et, on montre qu'on a une contradiction (par l'absurde).

Ici : (P) : un entier n se décompose en un produit de facteurs premiers.

On suppose deux décompositions de n en un produit de facteurs premiers et on montre qu'on a nécessairement les mêmes facteurs.

Quand le théorème aura été démontré :

Théorème de Gauss: si un nombre p divise un produit ab et si p est premier avec a, alors il divise b

Application au nombre premier: si un nombre premier p divise un produit ab, alors il divise a ou il divise b

Soit deux produits de nombres premiers qui sont égaux. Prenons n'importe quel nombre premier p du premier produit.

Il divise le premier produit, et donc, le second.

p doit alors diviser au moins un facteur dans le second produit. Mais les facteurs sont tous des nombres premiers eux-mêmes, donc p doit être égal à un des facteurs du second produit.

On peut alors diviser par p les deux produits.

Ainsi de suite avec tous les facteurs premiers des deux produits.

Conséquence: les facteurs premiers des deux produits sont égaux.

IV-4-2- application à la recherche des diviseurs

Soit $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$ la décomposition en produit de facteurs premiers

Un diviseur de N est de la forme $p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}$ où pour tout $1 \leqslant i \leqslant k$, on a: $0 \leqslant \beta_i \leqslant \alpha_i$

Preuve:

Sens direct: Soit $d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}$. d divise N car $p_1^{\beta_1}$ divise $p_1^{\alpha_1}$ et de m^me pour les autres facteurs.

Sens réciproque: Soit d un diviseur de N alors il existe un entier q tel que $d \times q = N$.

Les entiers d et q s'écrivent chacun comme produit de facteurs premiers et le produit de ces deux décompositions est celle de N d'après l'unicité de la décomposition en un produit de facteurs premiers.

Par conséquent, les facteurs premiers de d sont ceux de N et ils ne peuvent intervenir qu'avec un exposant inférieur ou égal à α_i

IV-4-3- Nombre de diviseurs

Les exposants β_i peuvent prendre $\alpha_i + 1$ valeurs.

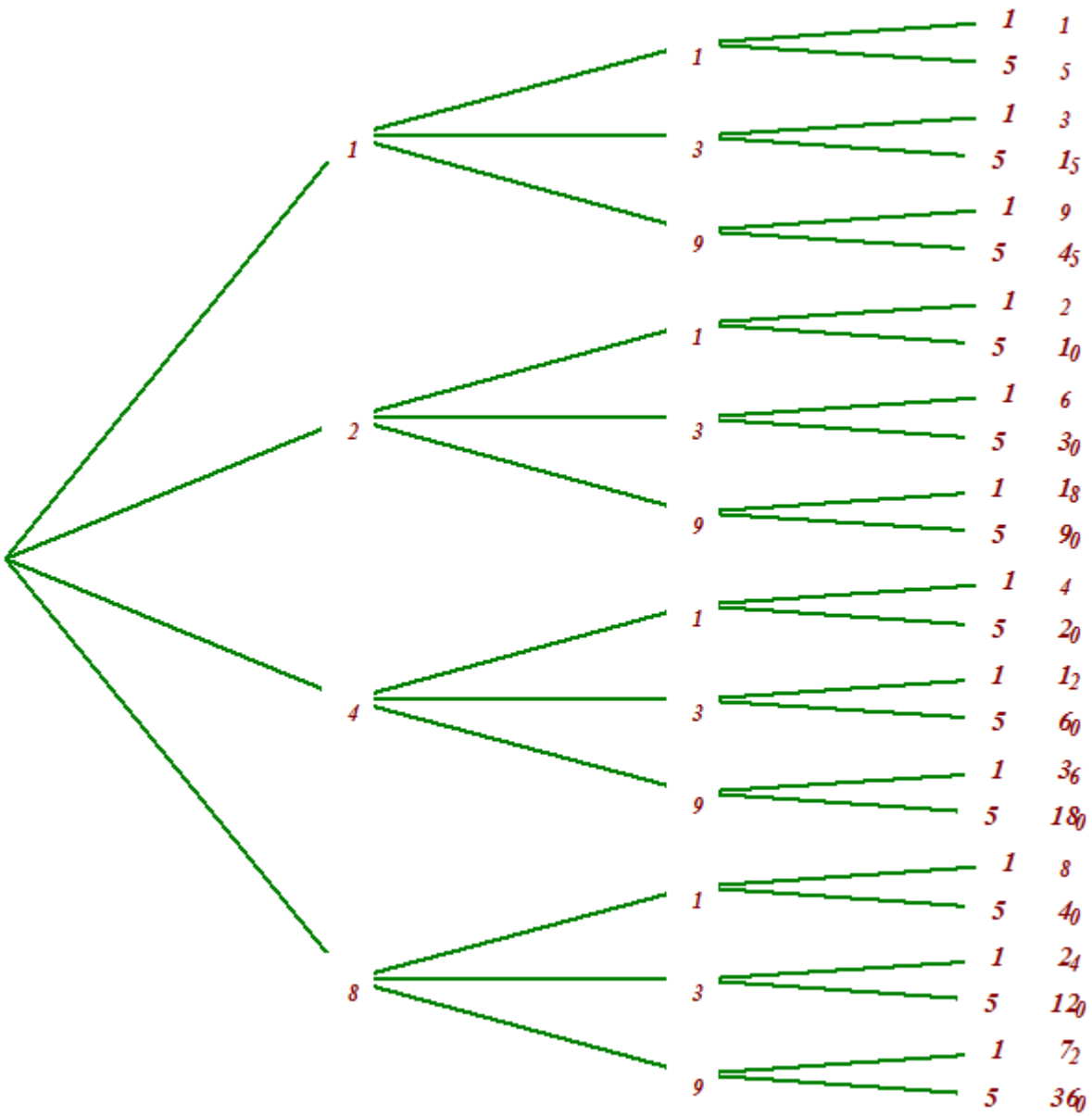
Soit le choix d'un facteur premier (par exemple: p_1).

Pour chaque choix de β_1, on peut choisir $\alpha_2 + 1$ facteurs p_2 et ainsi de suite.

Le nombre de diviseurs de N est: $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \ldots \times (\alpha_k + 1)$

Exemple: $360 = 2^3 \times 3^2 \times 5$ a $4 \times 3 \times 2 = 24$ diviseurs

Choix du nombre de facteurs				Diviseurs
facteurs	2	3	5	



V- PGCD - PPCM

V-1- Plus grand commun diviseur (pgcd)

V-1- 1- Recherche:

On cherche les diviseurs positifs communs à deux entiers positifs a et b.
Dans la suite, on note $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a
et $\mathscr{D}(a; b) = \mathscr{D}(a) \cap \mathscr{D}(b)$ l'ensemble des **diviseurs** positifs **communs** à a et b.

Un exemple: Soit $\mathscr{D}(6)$ l'ensemble des diviseurs de 6 et $\mathscr{D}(15)$ celui des diviseurs de 15
$\mathscr{D}(6) = \{1; 2; 3; 6\}$ et $\mathscr{D}(15) = \{1; 3; 5; 15\}$ $\mathscr{D}(6; 15) = \mathscr{D}(6) \cap \mathscr{D}(15) = \{1; 3\}$

Pour tout a et tout b, $\mathscr{D}(a, b)$ est un ensemble non vide, car, il contient l'entier 1.
$\mathscr{D}(a, b)$ est un **ensemble fini** car les éléments sont inférieurs ou égaux au plus petit des deux entiers a et b si a et b non nuls ou inférieurs ou égaux à a si $b = 0$.
Or, tout sous-ensemble (ou partie) de $\mathbb{N}$ non vide et fini contient un plus grand élément.

***Petit rappel de vocabulaire*:**
Dans l'ensemble des réels, on peut avoir des parties bornées sans avoir de plus petit ou de plus grand élément.
Dans $\mathbb{R}$,]0 ; 1[est une partie bornée.
Un majorant M (respectivement un minorant m) d'un sous-ensemble E est un réel tel que pour tout $x \in E$, on a : $x \leqslant M$ (resp. $x \geqslant m$) 1 ; $\sqrt{2}$; 2 ; 100 ... sont des majorants de]0 ; 1[
-10 ; $-\frac{1}{2}$; 0 … sont des minorants de]0 ; 1[.
Une borne supérieure (resp. inférieure) d'un sous-ensemble E est le plus petit des majorants (resp. le plus grand des minorants). 1 est la borne supérieure de]0 ; 1[
0 est la borne supérieure de]0 ; 1[
]0 ; 1[n'a ni minimum, ni maximum.

V-1- 2- Définition:
Par conséquent: $\mathscr{D}(a, b)$ contient un plus grand élément qui est appelé le plus grand commun diviseur à a et à b et noté PGCD(a; b) ou pgcd(a; b)

V- 2- Propriétés (conséquences immédiates de la définition)

V- 2- 1-
pgcd(a; 0) = a car tous les diviseurs de a sont des diviseurs de 0.

V- 2- 2-
pgcd(a; a) = a (évident)

V- 2- 3-
pgcd(1; a) = 1 (évident)

V- 2- 4-
si $a \mid b$ alors pgcd(a; b) = a (évident).

Exercice: Méthode par soustractions successives
Soit $a \geqslant b$, prouver que $\mathscr{D}(a; b) = \mathscr{D}(b; a - b)$
Application: en déduire le pgcd(168; 264)
Point méthode: Pour démontrer l'égalité de deux ensembles E et F, on montre $E \subset F$ et $F \subset E$.
Démonstration:
Montrons: $\mathscr{D}(a; b) \subset \mathscr{D}(b; a - b)$
Soit $d \in \mathscr{D}(a; b)$
On a: $d \mid a$ et $d \mid b$ donc $d \mid a - b$ (propriété I- 3- 5)
d est donc un diviseur de b et de $a - b$, soit $d \in \mathscr{D}(b; a - b)$
on a montré: $\mathscr{D}(a; b) \subset \mathscr{D}(b; a - b)$ (i)
Montrons: $\mathscr{D}(b; a - b) \subset \mathscr{D}(a; b)$
Soit $d \in \mathscr{D}(b; a - b)$
On a: $d \mid b$ et $d \mid a - b$ donc $d \mid (a - b) + b = a$ (propriété I- 3- 5)
d est donc un diviseur de b et de a , soit $d \in \mathscr{D}(a; b)$
on a montré: $\mathscr{D}(b; a - b) \subset \mathscr{D}(a; b)$ (ii)
Conclusion: D'après (i) et (ii), $\mathscr{D}(a; b) = \mathscr{D}(b; a - b)$

Application: ***Méthode par soustractions successives***
$\mathscr{D}(168; 264) = \mathscr{D}(168; 96) = \mathscr{D}(96; 72) = \mathscr{D}(72; 24) = \mathscr{D}(24; 48) = \mathscr{D}(24; 24) = \mathscr{D}(24)$
Les diviseurs communs à 168 et 264 sont ceux de 24,
par conséquent: pgcd(168; 264) = 24

V- 3- Algorithme d'Euclide

V- 3- 1: Résultat préliminaire

Soit a et b deux entiers positifs. On prend $0 < b < a$)

$a = b\,q + r$ avec $0 \leqslant r < b$.

Les diviseurs communs de a et b sont les diviseurs communs de b et r, c'est-à-dire: $\mathscr{D}(a; b) = \mathscr{D}(b; r)$

Démonstration:

Montrons: $\mathscr{D}(a; b) \subset \mathscr{D}(b; r)$

Soit $d \in \mathscr{D}(a; b)$

On a: $d \mid a$ et $d \mid b$ donc $d \mid a - bq = r$ (propriété I- 3- 5)

d est donc un diviseur de b et de r, soit $d \in \mathscr{D}(b; r)$

on a montré: $\mathscr{D}(a; b) \subset \mathscr{D}(b; r)$ (i)

Montrons: $\mathscr{D}(b; r) \subset \mathscr{D}(a; b)$

Soit $d \in \mathscr{D}(b; r)$

On a: $d \mid b$ et $d \mid r$ donc $d \mid bq + r = a$ (propriété I- 3- 5)

d est donc un diviseur de b et de a , soit $d \in \mathscr{D}(a; b)$

on a montré: $\mathscr{D}(b; r) \subset \mathscr{D}(a; b)$ (ii)

Conclusion: D'après (i) et (ii), $\mathscr{D}(a; b) = \mathscr{D}(b; r)$

V- 3- 2: Algorithme d'Euclide

D'après le résultat précédent, lorsque b ne divise pas a, on ramène la recherche de $\mathscr{D}(a; b)$ à celle de $\mathscr{D}(b; r)$ jusqu'au dernier reste non nul.

La succession des restes est une suite strictement décroissante, car, on a: $b < a$ et $r < b$.

Le pgcd(a; b) est alors le dernier reste non nul puisque pgcd(r; 0) = r.

Un exemple: $a = 138\,807$ $b = 52\,089$

$$138\,807 = 2 \times 52\,089 + 34\,629 \qquad a = bq_1 + r_1$$
$$52\,089 = 1 \times 34\,629 + 17\,460 \qquad b = r_1 q_2 + r_2$$
$$34\,629 = 1 \times 17\,460 + 17\,169 \qquad r_1 = r_2 q_3 + r_3$$
$$17\,460 = 1 \times 17\,169 + 291 \qquad r_2 = r_3 q_4 + r_4$$
$$17\,169 = 59 \times 291 + 0 \qquad r_3 = r_4 q_5 + r_5$$

pgcd(138 807; 52 089) = 291

On peut disposer ainsi

quotients		2 q_1	1 q_2	1 q_3	1 q_4	59 q_5
dividendes-diviseurs	138 807 a	52 089 b	34 629 r_1	17 460 r_2	17 169 r_3	291 r_4
restes	34 629 r_1	17 460 r_2	17 169 r_3	291 r_4	0 r_5	

Un exercice:

a et b sont deux entiers tels que $a = 630$ et $600 < b < 1\,100$ et pgcd(a; b) = 105

Déterminer b.

Rédaction: puisque pgcd(a; b) = 105, b est un multiple de 105 et comme $600 < b < 1\,100$, on a:

il existe un entier k tel que $b = 105 \times k$ et $600 < 105 \times k < 1\,100$. Soit $k \in \mathbb{N}$ et $k \in [6; 10]$

(On a montré: si b existe alors $b \in \{630; 735; 840; 945; 1\,050\}$. Il faut faire la réciproque, c'est-à-dire contrôler que ces nombres vérifient les données)

a	b	pgcd(a; b)	Conclusion

$630 = 6 \times 105$	$630 = 6 \times 105$	630	Non
$630 = 6 \times 105$	$735 = 7 \times 105$	105	Oui
$630 = 6 \times 105$	$840 = 8 \times 105$	$2 \times 105 = 210$	Non
$630 = 6 \times 105$	$945 = 9 \times 105$	$3 \times 105 = 315$	Non
$630 = 6 \times 105$	$1\,050 = 10 \times 105$	$2 \times 105 = 210$	Non

Conclusion: $b = 735$

V- 4 Nombres premiers entre eux- Théorème de Bezout

V- 4- 1- Définition

Deux entiers naturels sont dits premiers entre eux lorsque leur pgcd est égal à 1

La définition s'étend aux entiers relatifs.
Deux entiers relatifs sont dits premiers entre eux lorsqu'ils ont exactement deux diviseurs communs –1 et 1.

Exemple: –12 et 25 sont premiers entre eux.
$\mathscr{D}(-12) = \{-12; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12\}$
$\mathscr{D}(25) = \{-25; -5; -1; 1; 5; 25\}$
$\mathscr{D}(-12) \cap \mathscr{D}(25) = \{-1; 1\}$

V- 4- 2- Théorème de Bézout. Caractérisation des nombres premiers entre eux.

Bézout : mathématicien français (1730 - 1783).

a et b sont deux entiers naturels
"a et b sont premiers entre eux" si et seulement si "il existe deux entiers relatifs u et v tels que $au + bv = 1$"

Démonstration:

Une application:
Deux entiers consécutifs sont premiers entre eux.

En effet: $(n+1) + (-1)n = 1$

Exemple:
$2n + 1$ et $3n + 2$ sont premiers entre eux. car $2\times(3n+2)-3\times(2n+1)=1$

V- 4- 3 Propriété

Si a est premier avec b et premier avec c alors a est premier avec bc.
Puis, montrer: Si a est premier avec b alors a^n et b^p sont premiers entre eux.

Démonstration:

Recherche des coefficients u et v

On "remonte" l'algorithme d'Euclide:
Exemple: 47 et 35 sont premiers entre eux. On veut: $47u + 35v = 1$
Algorithme d'Euclide:
$47 = 35 \times 1 + 12$ (1)
$35 = 12 \times 2 + 11$ (2)
$12 = 11 \times 1 + 1$ (3)
De (3), on tire: (4) $1 = 12 - 11 \times 1$ et de (2), on tire : (5) $11 = 35 - 12 \times 2$
En substituant (5) dans (4), il vient: (6) $1 = 12 - (35 - 12 \times 2) = 12 \times 3 - 35$

Or, de (1), on a: (7) $12 = 47 - 35 \times 1$, ce qui donne: $1 = (47 - 35 \times 1) \times 3 - 35 = 47 \times 3 - 35 \times 4$
Conclusion: $u = 3$ et $v = -4$

Remarque: Si on établit la liste des multiples de 47 et 35, on trouve des entiers consécutifs...

k	$47 \times k$	$35 \times k$
1	47	35
2	94	70
3	**141**	105
4	188	**140**
5	235	175
6	282	210
7	329	245
8	376	280
9	423	315
...	...	...
38	**1786**	
...	...	
51		**1785**
...	...	...
73	**3431**	
...	...	...
98		**3430**

$47 \times 3 + 35 \times (-4) = 47 \times 38 + 35 \times (-51) = 47 \times 73 + 35 \times (-98) = 1$

V-5- Caractérisation du PGCD

V-5-1- Théorème

a, b, g sont des entiers strictement positifs
Les 3 propositions suivantes sont équivalentes:
(i) g est le pgcd de a et b

(ii) g est un diviseur de a et de b et les entiers $a' = \frac{a}{g}$ et $b' = \frac{b}{g}$ sont premiers entre eux.

(iii) g est un diviseur de a et de b et il existe deux entiers u et v tels que $au + bv = g$.

Démonstration:

V-5-2- Conséquences

* Si g est le pgcd de a et b alors, pour tout entier $c > 0$, gc est le pgcd de ac et bc

** Si g est le pgcd de a et b et si c divise a et b alors $\frac{g}{c}$ est le pgcd de $\frac{a}{c}$ et $\frac{b}{c}$.

Preuve: Par exemple en utilisant (iii)

g est un diviseur de a et de b et il existe deux entiers u et v tels que $au + bv = g$,
d'où, gc est un diviseur de ac et de bc et il existe deux entiers u et v tels que $(ac)u + (bc)v = gc$.

et, de plus, si c divise a et b alors $\frac{g}{c}$ est un diviseur de $\frac{a}{c}$ et de $\frac{b}{c}$ et il existe deux entiers u et v tels que $\left(\frac{a}{c}\right)u + \left(\frac{b}{c}\right)v = \frac{g}{c}$

V-5-3- Fraction irréductible

V-5-3-1- Définitions:

Une fraction est un quotient de deux entiers $\frac{a}{b}$ avec $b \neq 0$

Une fraction $\frac{a}{b}$ est irréductible lorsque a et b sont premiers entre eux.

V-5-3-2- Propriété

Toute fraction est égale à une fraction irréductible

En effet, soit $g = \text{pgcd}(a,b)$, on a: $\frac{a}{b} = \frac{ga'}{gb'} = \frac{a'}{b'}$ avec a' et b' sont premiers entre eux.

V-5-4- Théorème de Gauss

(Gauss : mathématicien allemand né en 1777, mort en 1855)

Théorème:

Si a, b, c sont des entiers strictement positifs tels que a divise bc et a est premier avec b alors a divise c.

Preuve:

a est premier avec b donc il existe deux entiers u et v tels que $au + bv = 1$

d'où, $(ac)u + (bc)v = c$

Comme a divise ac et bc alors a divise la combinaison linéaire $(ac)u + (bc)v$, donc, a divise c.

V-5-5- Divisibilité par un produit

Propriété:

Si un entier n est divisible par deux entiers a et b premiers entre eux alors il est divisible par leur produit ab

Preuve:

$n = ap$ et $n = bq$ donc $ap = bq$.

On en déduit que b divise ap, donc, puisque a et b premiers entre eux, d'après le théorème de Gauss, b divise p

On a alors: $p = bp'$, soit, $abp' = n$

Conclusion: ab divise n.

V-5-6- Exercices sur le PGCD

a) ***Énoncé :*** Trouver deux entiers naturels a et b tels que $a + b = 112$ et $\text{pgcd}(a, b) = 14$

Résolution : On peut remarquer que a et b sont interchangeables.

On peut supposer $a \leqslant b$ lors de la recherche et conclure en donnant les couples symétriques.

$a = 14a'$ et $b = 14b'$ avec a' et b' premiers entre eux

On a alors: $a' + b' = 8$ (car, $8 \times 14 = 112$)

Les couples $(a' ; b')$ possibles (1; 7), (3; 5)

Les couples $(a; b)$ sont: (14; 98), (42; 70); (70; 42) et (98; 14)

b) ***Énoncé :*** p et n sont deux entiers supérieurs ou égaux à 2.

Déterminer le pgcd de $a = pn$ et $b = p(n - 1)$

Résolution : p divise a et p divise b, et $a - b = p$, donc, p est le pgcd de a et b.

c) ***Énoncé :*** c et un entier premier avec b et g = pgcd(a, b)

Déterminer le pgcd de ac et b.

Résolution : g divise a et b, donc, g divise ac et b.

$a' = \frac{a}{g}$ et $b' = \frac{b}{g}$ sont premiers entre eux et c est premier avec b, donc, $a'c = \frac{ac}{g}$ et $b' = \frac{b}{g}$ sont premiers entre eux. (Un diviseur commun d de $a'c$ et b' est un diviseur commun de c et $b' = \frac{b}{g}$)

donc, pgcd(ac, b) = g

ou encore: $au + bv = g$ et $bu' + cv' = 1$

En multipliant membre à membre: $(ac)(uv') + b(auu' + bu'v + cvv') = g$, et g divise ac et b.

d) ***Énoncé :*** Déterminer quatre entiers strictement positifs a, b, c et d formant une suite arithmétique dans cet ordre dont la raison est un nombre premier avec a et $10a^2 = d - b$.

Résolution : Soit r la raison

$b = a + r$, $c = a + 2r$, $d = a + 3r$, d'où, $10a^2 = d - b = 2r$, soit: $5a^2 = r$ et r premier avec a
Par conséquent : r divise 5
$r = 1$ (impossible) ou $r = 5$
$a^2 = 1$
La suite est (1; 6; 11; 16)

e) ***Énoncé :*** Montrer que pour tout entier naturel n, $A = n(5n^2+1)$ est divisible par 6
Résolution : 2 et 3 étant premiers entre eux, on montre que A est divisible par 2 et par 3.
divisibilité par 2: $n = 2p$ ou $n = 2p + 1$
Si n est pair alors A est pair
Si n est impair alors $5n^2$ est impair et $5n^2 + 1$ est pair, donc, A est pair
divisibilité par 3: $n = 3k$ ou $n = 3k + 1$ ou $n = 3k + 2$
Si $n = 3k$ alors A est un multiple de 3
Si $n = 3k + 1$ alors $5n^2 + 1 = 5(9k^2+6k+1) + 1 = 3(15k^2+10k+2)$ est un multiple de 3
Si $n = 3k + 2$ alors $5n^2 + 1 = 5(9k^2+12k+4) + 1 = 3(15k^2+20k+7)$ est un multiple de 3
Conclusion: A étant un multiple de 2 et de 3, et, ***2 et 3 étant premiers entre eux***, A est un multiple de 6

V-6- Plus Petit Commun Multiple (PPCM)

V-6-1 Définition

a et b sont deux entiers strictement positifs.
Ils ont au moins un multiple commun strictement positif, d'où,
l'ensemble des multiples communs à a et b possède un plus petit élément strictement positif appelé PPCM(a, b)

V-6-2- Propriétés

*** Si g = PGCD(a; b) et m = PPCM(a; b) alors $gm = ab$

*** Tout multiple commun de a et b est un multiple de leur PPCM.

Preuve:

On a: $a = ga'$ et $b = gb'$ avec a' et b' premiers entre eux.

Soit M un multiple commun de a et de b.

$M = ap$ et $M = bq$, donc, $ap = bq = ga'p = gb'q$

On en déduit: $a'p = b'q$

soit: a' divise $b'q$, or, a' et b' sont premiers entre eux, donc, d'après le théorème de Gauss, a' divise q.

On peut écrire: $q = ka'$, puis, $p = kb'$

Finalement: $M = ga'kb' = k(ga'b')$

Le plus petit multiple est obtenu lorsque $k = 1$, donc, $m = ga'b'$

M est par conséquent un multiple de m.

Puis $gm = (ga')(gb') = ab$

Réciproquement:

Soit M un multiple de m.

$M = km = kga'b' = (kb')a = (ka')b$

M est par conséquent un multiple commun à a et b.

V-6-3 Caractérisation du PPCM

m = PPCM(a; b) équivaut à m est un multiple de a et de b et, $\frac{m}{a}$ et $\frac{m}{b}$ sont des entiers premiers entre eux.

Preuve:

Sens direct:

m = PPCM(a; b) implique m est un multiple de a et de b

D'autre part, d'après la démonstration précédente, $m = ga'b' = ab' = ba'$ avec a' et b' premiers entre eux.

Sens réciproque:

Soit M un multiple de a et de b tel que $\frac{M}{a}$ et $\frac{M}{b}$ sont premiers entre eux.

Or, M est un multiple de m, d'où, $M = kab' = ka'b$

$\frac{M}{a} = kb'$ et $\frac{M}{b} = ka'$.

Comme $\frac{M}{a}$ et $\frac{M}{b}$ sont premiers entre eux, on a $k = 1$.

VI- Petit théorème de Fermat

VI-1- Énoncé

Si p est un entier premier et a un entier naturel non divisible par p alors $a^{p-1} - 1$ est divisible par p

ou encore

$a^{p-1} \equiv 1 \mod(p)$

VI-2- Corollaire

Si p est un entier premier et a un entier naturel alors $a^p - a$ est divisible par p

ou encore

$a^p \equiv a \mod(p)$

Preuve:

Illustration par un exemple de la démarche:

$p = 5$ $a = 13$ $A = \{13; 26; 39; 52\}$

Soit R est l'***ensemble*** des restes des éléments de A dans la division par 5

$13 = 5\times2 + 3$; $26 = 5\times5 + 1$; $39 = 5\times7 + 4$; $52 = 5\times10 + 2$ $R = \{1; 2; 3; 4\}$

On a donc : $13 \equiv 3 \pmod 5$, $26 \equiv 1 \pmod 5$, $39 \equiv 4 \pmod 5$, $52 \equiv 2 \pmod 5$.

Soit $N = 13\times26\times39\times52 = 1\times2\times3\times4\times 13^4 = 4!\times13^4$ (On note $4! = 1\times2\times3\times4$ factorielle 4)

Le reste de N par 5 est congru à $1\times2\times3\times4 = 4!$ modulo 5.

On en déduit : $4!\times13^4 \equiv 4! \pmod 5$, soit : $4!(13^4 - 1) \equiv 0 \pmod 5$.

Comme 5 ne divise pas 4! et que 5 divise le produit $4!\times(13^4 - 1)$ alors 5 divise $13^4 - 1$

Conclusion : $13^4 - 1 \equiv 0 \pmod 5$ ou encore $13^4 \equiv 1 \mod(5)$

démonstration :

Soit p est un entier premier et a un entier naturel non divisible par p

Conséquence : p et a sont premiers entre eux.

* Soit $A = \{a; 2a; ...; (p - 1)a\}$. A contient $p - 1$ éléments.

A est l'ensemble des $p - 1$ multiples de a de a à $(p - 1)a$.

p ne divise aucun entier de 1 à $p - 1$ et p ne divise pas a, donc,

aucun élément de A n'est divisible par p d'après le théorème de Gauss,

d'où, ***aucun reste*** dans la division euclidienne par p d'un élément de A ***n'est nul***.

** ***Montrons que tous ces restes sont distincts.***

(démonstration classique ... : on suppose deux restes identiques et ....)

On choisit deux éléments de A :

soit k et k' deux entiers tels que $1 \leqslant k \leqslant p - 1$, $1 \leqslant k' \leqslant p - 1$.

Supposons $ka \equiv k'a \mod(p)$ (c-à-d : ka et $k'a$ ont le même reste dans la division par p)

On a alors: $(k - k')a \equiv 0 \mod(p)$ et p ne divise pas a.

On obtient alors: $k - k'$ est divisible par p.

Or, $-(p - 2) \leqslant k - k' \leqslant p - 2$. $(|k - k'| \leqslant p - 2)$

Le seul entier divisible par p vérifiant cet encadrement est 0.

Par conséquent: $k = k'$.

On a donc $p - 1$ restes r différents (*et aucun reste n'est nul*) ,

ainsi : r est un entier et $1 \leqslant r < p$

Conclusion: L'ensemble des restes $R = \{1; 2; ...; p-1\}$

*** Soit N le produit de tous les éléments de A.

	éléments de A	Reste dans la division euclidienne par p et congruences modulo p.
$p-1$ lignes	a	Tous les entiers de 1 à $p-1$ c-à-d : $ka \equiv r \pmod p$ avec $1 \leqslant k \leqslant p-1$ et $1 \leqslant r \leqslant p-1$
	$2a$	
	$(p-1)a$	
Produit des $p-1$ lignes	$(p-1)!\ a^{p-1}$	propriété des congruences $(p-1)!\ a^{p-1} \equiv (p-1)! \pmod p$

$N = 1 \times 2 \times ... \times (p-1) \times a^{p-1} = (p-1)!\ a^{p-1}$

Le reste de la division de N par p est donc celui de $1 \times 2 \times ... \times (p-1) = (p-1)!$ d'après (**)

$N \equiv 1 \times 2 \times ... \times (p-1) \equiv (p-1)! \pmod p$.

On a alors: $(p-1)!\ a^{p-1} \equiv (p-1)! \pmod p$, soit: $(p-1)!\ (a^{p-1} - 1) \equiv 0 \pmod p$

Comme p ne divise pas $(p-1)!$, p divise $(a^{p-1} - 1)$.

Preuve du corollaire:

$a^{p-1} \equiv 1 \pmod p$ implique $a^{p-1} \times a \equiv 1 \times a \pmod p$

On a alors: $a^p \equiv a \bmod(p)$.

La réciproque est fausse,

car, $a^p \equiv a \pmod p$ mène à $a(a^{p-1} - 1) \equiv 0 \pmod p$ qui est vrai lorsque p divise a.

Quelques démonstrations

démonstration du I-1-3 (par l'absurde)

Supposons que 15 est un multiple de 2.
Il existe un entier c tel que $15 = 2\times c$, or, $14 < 15 < 16$
d'où, $2\times 7 < 2\times c < 2\times 8$
soit: $7 < c < 8$
Cette dernière proposition est fausse et découle de la proposition: 15 est un multiple de 2.
Conclusion: 15 n'est pas un multiple de 2.

démonstration du I-3-1

On a: b divise a, d'où, il existe un entier c tel que $a = bc$
On en déduit: $a = (-b)\times(-c)$ avec $-c \in \mathbb{Z}$. CQFD

démonstration du I-3-2

On a: b divise a, d'où, il existe un entier c tel que $a = bc$
d'autre part, $a \neq 0$ implique $c \neq 0$
on en déduit: $|a|=|bc|=|b|\times|c|$ avec $|c| \neq 0$
(***C'est ici qu'intervient la construction de ℕ:***) $|c|$ est un entier naturel non nul, d'où, $|c| \geqslant 1$
par conséquent: $|b|\times|c| \geqslant |b|$
conclusion: $|a| \geqslant |b|$ CQFD

démonstration du I-3-3

Nécessairement $a \neq 0$ et $b \neq 0$ d'après les hypothèses (un diviseur n'est jamais nul)
On a: b divise a, d'où, il existe un entier c tel que $a = bc$ *(i)*
a divise b, d'où, il existe un entier c' tel que $b = ac'$ *(ii)*
on déduit de (*i*) et (*ii*): $a = (ac')\times c = a\times(cc')$
Comme $a \neq 0$, il vient: $cc' = 1$.
Comme $(c, c') \in \mathbb{Z}^2$, on obtient: $c = c' = 1$ ou $c = c' = -1$
conclusion: $a = b$ ou $a = -b$ CQFD
Une autre démonstration en utilisant I- 3- 2 donne: $|b| \leqslant |a|$ et $|a| \leqslant |b|$, d'où, $|a| = |b|$

démonstration du I-3-4 (transitivité)

On a: a divise b, d'où, il existe un entier q tel que $b = aq$ *(i)*
b divise c, d'où, il existe un entier q′ tel que $c = bq'$ *(ii)*
on déduit de (*i*) et (*ii*): $c = (aq)q' = a(qq')$ avec $qq' \in \mathbb{Z}$. CQFD

démonstration du I-3-5 (combinaison linéaire)

On a: a divise b, d'où, il existe un entier q tel que $b = aq$ *(i)*
a divise c, d'où, il existe un entier q′ tel que $c = aq'$ *(ii)*
x et y étant des entiers quelconques,

on déduit de (*i*) et (*ii*): $bx + cy = (aq)x + (aq')y = a(qx + q'y)$ avec $qx + q'y \in \mathbb{Z}$. CQFD

démonstration du I-3-6

On a: *a* divise *b*, d'où, il existe un entier *q* tel que $b = aq$ *(i)*
d'où, pour tout entier c, on a: $bc = (aq)c = a(qc)$ CQFD

démonstration du II-1 : division euclidienne

Existence du couple :

b étant non nul et entier positif, alors $b \geqslant 1$
Les multiples de *b* forment donc une suite strictement croissante.

0 *b* 2*b* 3*b* … *ab* (*a*+1)*b* …

Or, $b \geqslant 1$ implique $ab \geqslant a$.
L'entier *a* est donc soit un multiple de *b* dans la liste {0; *b*, ..., *ab*}
soit compris entre deux multiples consécutifs de *b* dans cette liste
On obtient: $qb \leqslant a < (q + 1)b$ On peut donc écrire: $a = bq + r$ avec $0 \leqslant r < b$
L'entier *r* est la distance de *a* à *bq* $r = a - bq$

qb ◀ *r* ▶ *a* (*q*+1)*b*

Unicité du couple :

Pour démontrer que ce couple est unique, supposons qu'il existe un deuxième couple (q' ; r') vérifiant les mêmes conditions.

on a : $bq + r = bq' + r' \Leftrightarrow b(q - q') = r' - r$.

Or : $0 \leqslant r < b$ donc $-b < -r \leqslant 0$

$0 \leqslant r' < b$

On en déduit alors que : $-b < r' - r < b$ c'est-à-dire $|r' - r| < b$

D'autre part : $r' - r = b(q - q')$, donc $r' - r$ est un multiple de *b*.

Le seul multiple de *b* compris strictement entre $-b$ et *b* est 0.

On a donc : $r' - r = 0$ et par conséquent $b(q' - q) = 0$, donc $q' - q = 0$

On obtient alors : $r' = r$ *et* $q' = q$.

Le couple (*q ; r*) est donc unique.

Démonstration du III-1

Sens direct

On sait: $a = cq + r$ et $b = cq' + r$ avec $0 \leqslant r < |c|$

d'où, $a - b = c(q - q')$ CQFD

Sens réciproque:

On sait: $a - b = ck$

Soit: $a = cq + r$ avec $0 \leqslant r < |c|$ et $b = cq' + r'$ avec $0 \leqslant r' < |c|$

$a - b = c(q - q') - (r - r')$
On en tire: $r - r' = a - b - c(q - q') = ck - c(q - q') = c(k - q - q')$
Par conséquent: c divise $r - r'$,
or, $0 \leqslant r < |c|$ et $0 \leqslant r' < |c|$, d'où, $-|c| < r - r' < |c|$
Le seul multiple de c strictement compris entre $-c$ et c est 0. CQFD

démonstration du III-3

Données : $a \equiv a' \bmod(c)$ et $b \equiv b' \bmod(c)$

d'où : $a - a'$ et $b - b'$ sont des multiples de c.

Leur somme $(a - a') + (b - b') = (a + b) - (a' + b')$ et leur différence $(a - a') - (b - b') = (a - b) - (a' - b')$ sont donc des multiples de c, ce qui prouve :

$a + b \equiv a' + b' \bmod(c)$ et $a - b \equiv a' - b' \bmod(c)$

$ab - a'b' = ab - a'b + a'b - a'b' = b(a - a') + a'(b - b')$.
Comme $a - a'$ et $b - b'$ sont des multiples de c, la combinaison linéaire $b(a - a') + a'(b - b')$ est un multiple de c, ce qui prouve que $ab - a'b'$ est un multiple de c, soit : $a.b \equiv a'.b' \bmod(c)$.

Si $a = b$ et $a' = b'$ alors $a^2 \equiv a'^2 \bmod(c)$
Raisonnement par récurrence :

Propriété à démontrer : si $a \equiv a' \bmod(c)$ alors $a^n \equiv a'^n \bmod(c)$

Initialisation : voir ci-dessus : $a^2 \equiv a'^2 \bmod(c)$

Hérédité : Soit un entier n tel que $a^n \equiv a'^n \bmod(c)$.

comme $a \equiv a' \bmod(c)$, par produit, on obtient : $a^{n+1} \equiv a'^{n+1} \bmod(c)$.

Conclusion :

D'après l'axiome de récurrence la propriété est vraie pour tout entier $n \geqslant 2$.

elle est évidemment vraie pour $n = 0$ et $n = 1$

démonstration du IV-2

$n \geqslant 2$.

Deux cas :

n est premier ou n n'est pas premier.

Dans les deux cas, n divise n.

* Si n est premier, n divise n et n est premier.

** Si n n'est pas premier, il existe au moins un diviseur différent de 1 et différent de n. (diviseur propre).

(Un diviseur différent de 1 et n est dit " diviseur propre " de n).

Soit l'ensemble des diviseurs propres de n.

$\mathscr{D}_p$ est **non vide**, il existe donc **un plus petit élément** p.

p est nécessairement premier, car, un diviseur k de p est un diviseur de n, et si k est différent de 1 et différent de p, $k \in \mathscr{D}_p$ et $k < p$ ce qui est impossible.

On a alors: il existe q entier tel que $pq = n$ avec $q \geqslant p$, d'où, $pq \geqslant p^2$.

Finalement: $p^2 \leqslant n$. Ce qui prouve le théorème énoncé.

Démonstration du IV-3 : (démonstration d'Euclide)

(*Traduite en langage mathématique actuel*)

Proposition XX: les nombres premiers sont en plus grande quantité que toute quantité proposée de nombres premiers

Soit $\mathscr{L} = \{ p_1 ; p_2 ; ... ; p_n \}$ une liste finie de nombres premiers.

On construit l'entier $N = p_1 \times p_2 \times \ldots \times p_n + 1$

1er cas) N est premier et $N > p_n$.

2ème cas) N n'est pas premier et il existe un diviseur positif premier q.

Montrons par un raisonnement par l'absurde que q n'est pas un élément de la liste $\mathscr{L}$.

Supposons que $q \in \mathscr{L}$. ($q = p_i$ avec $1 \leqslant i \leqslant n$)

q divise le produit $p_1 \times p_2 \times \ldots \times p_n$ et q divise N, donc, q divise la différence $N - p_1 \times p_2 \times \ldots \times p_n = 1$

Ce qui contredit l'hypothèse.

q est donc un nombre premier supplémentaire de la liste.

Exemple pour illustrer la démarche:

$\mathscr{L} = \{2; 3; 5\}$. $N = 2 \times 3 \times 5 + 1 = 31$ et N est premier

$\mathscr{L} = \{2; 3; 5; 7; 11; 13\}$. $N = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031$ et N n'est pas premier, mais, $N = 59 \times 509$ et 59 est un nombre premier qui n'est pas dans la liste.

V-4-2 Identité de Bezout

Sens direct. Donnée: "a et b sont premiers entre eux"

On note $\mathscr{E}$ l'ensemble de tous les entiers de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.

$\mathscr{E}$ est non vide et contient a ($a = a \times 1 + b \times 0$)

Par conséquent, il existe un plus petit entier strictement positif dans $\mathscr{E}$. On note m cet entier et $m = au_1 + bv_1$

Montrons que $m \mid a$ et $m \mid b$.

On peut écrire $a = mq + r$ avec $0 \leqslant r < m$, soit $a = (au_1 + bv_1)q + r$

On en tire: $r = a(1 - qu_1) + b(-qv_1)$. r est de la forme $au + bv$ donc $r \in \mathscr{E}$.

Comme $0 \leqslant r < m$ et que m *est le* plus petit entier positif dans $\mathscr{E}$ alors $r = 0$

Par conséquent $m \mid a$

La même démarche montre que $m \mid b$.

m est donc un diviseur commun à a et b et comme a et b sont premiers entre eux, il vient: $m = 1$

Conclusion: il existe deux entiers relatifs u et v tels que $au + bv = 1$

Sens réciproque: Donnée: "il existe deux entiers relatifs u et v tels que $au + bv = 1$"
Soit g un diviseur commun positif de a et de b.
g divise a et g divise b, donc, g divise $au + bv$
Or, $au + bv = 1$, donc, $g = 1$
Conclusion: a et b sont premiers entre eux

Démonstration du V-4-3

a* premier avec *b d'où, il existe des entiers u et v tels que $au + bv = 1$
a* premier avec *c d'où, il existe des entiers u' et v' tels que $au' + cv' = 1$
En multipliant membre-à-membre, il vient:
$(au+bv)(au'+bv') = 1$
soit, $a(auu'+ucv'+u'bv) + bc(vv') = 1$.
Comme $auu'+ucv'+u'bv$ et vv' sont des entiers, on en déduit d'après le théorème de Bezout que a et bc sont premiers entre eux.

En déduire par récurrence que: $n \in \mathbb{N}$ et $p \in \mathbb{N}$, si a et b sont premiers entre eux alors a^n et b^p sont premiers entre eux.

En posant $c = b$, on obtient: a est premier avec b^2 (Initialisation)
Supposons a premier avec b^p, on en déduit alors a premier avec $b^p \times b = b^{p+1}$ (hérédité)
L'axiome de récurrence permet de conclure:
pour tout entier naturel non nul p, a est premier avec b^p

On a donc aussi b^p premier avec $a \times a = a^2$ (Initialisation)
Supposons b^p premier avec a^n, on en déduit alors b^p premier avec $a^n \times a = a^{n+1}$ (hérédité)
L'axiome de récurrence permet de conclure:
pour tout entier naturel non nul n, b^p est premier avec a^n

a et b entiers premiers entre eux. Montrer que $a + b$ et a sont premiers entre eux
On sait: il existe deux entiers u et v tels que $au + bv = 1$
Peut-on trouver deux entiers x et y tels que $(a + b)x + ay = 1$?.
Comme $(a + b)x + ay = a(x + y) + bx$ il suffit de prendre $x + y = u$ et $x = v$.
En posant $x = v$ et $y = u – v$, on a: $(a + b)v + a(u – v) = au + bv = 1$ CQFD

Remarque*: a et b sont interchangeables, d'où, $a + b$ et b sont premiers entre eux

D'après la propriété montrée précédemment:
Si a est premier avec b et premier avec c alors a est premier avec bc.
Comme: $a + b$ et a sont premiers entre eux et $a + b$ et b sont premiers entre eux, on obtient: $a + b$ et ab sont premiers entre eux.
on en déduit aussi: $(a+b)^2$ et ab sont premiers entre eux.
Il existe donc deux entiers u_1 et v_1 tels que $(a+b)^2 u_1+(ab)v_1 = 1$
On en tire: $(a^2+b^2)u_1+(ab)(v_1+2u_1)=1$, ce qui prouve que a^2+b^2 et ab sont premiers entre eux.

Démonstration du V-5-1

pour démontrer l'équivalence des trois propositions, on montre (i) ⇒ (ii) ⇒ (iii) ⇒ (i)
(i) ⇒ (ii)

Donnée: g est le pgcd de a et de b donc $g \mid a$ et $g \mid b$
On pose $a' = \frac{a}{g}$ et $b' = \frac{b}{g}$
Soit d un diviseur commun à a' et b'
On a: $a' = dp$ et $b' = dq$
d'où, $a = (dp)g = (dg)p$ et $b = (dq)g = (dg)q$.
dg est donc un diviseur commun de a et de b et comme g =pgcd(a,b), on a nécessairement $d = 1$
Ce qui prouve (ii)

(ii) ⇒ (iii)
Donnée: g est un diviseur de a et de b et les entiers $a' = \frac{a}{g}$ et $b' = \frac{b}{g}$ sont premiers entre eux
d'où, il existe deux entiers u et v tels que $a'u + b'v = 1$
En multipliant les deux membres par g, on prouve (iii)

(iii) ⇒ (i)
Donnée: g est un diviseur de a et de b et il existe deux entiers u et v tels que $au + bv = g$.
Soit d = pgcd(a,b)
On a: $d \mid a$ et $d \mid b$ donc $d \mid au + bv$ (voir I-3-5)
d'où, $d \mid g$.
Comme $g \mid a$ et g $\mid b$ alors g divise leur pgcd, d'où, $g \mid d$.
$d \mid g$ et $g \mid d$, donc, $d = g$ ce qui prouve (i)

Important pour (iii), il ne suffit pas d'avoir deux entiers u et v tels que $au + bv = g$ pour conclure.
Contre-exemple: $52 = 8\times4004 - 82\times390$
mais, 52 ne divise pas 390. $4004 = 52\times77$ $390 = 52\times7 + 26$
En simplifiant l'égalité par 2, il vient: $26 = 4\times4004 - 41\times390$. $4004 = 26\times154$ $390 = 15\times26$
Comme26 divise 4004 et 26 divise 390, pgcd(a,b) = 26