CHAPITRE 1 : Divisibilité - Nombres premiers - Congruences

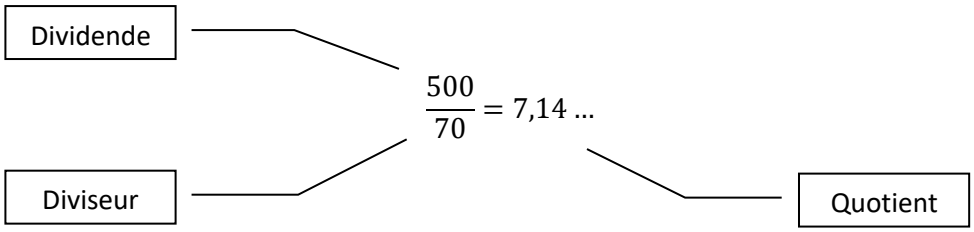
CHAPITRE 1 : Divisibilité - Nombres premiers - Congruences

1 Divisibilité dans $\mathbb{Z}$

1.1 Deux sortes de divisions

On distingue couramment deux types de divisions :

- La division « exacte »



- La **division euclidienne**[1] appelée aussi **division entière** qui est une division « avec reste »

Dans l'antiquité, Euclide explique dans son ouvrage « Les éléments » comment diviser un dividende en faisant des soustractions successives.

Exemple :

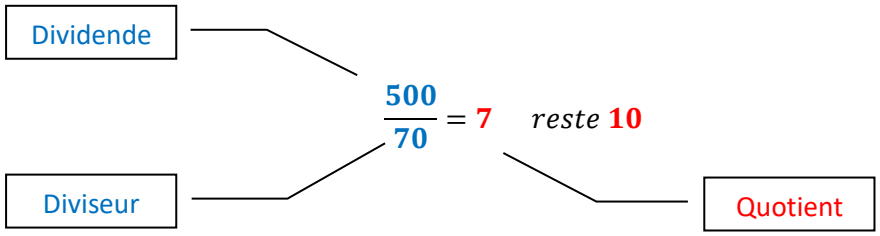
*Comment partager équitablement 500 € entre **70 personnes** ?*

- On prend 70 € que l'on répartit en donnant 1 € à chaque personne. Il reste 430 €
- On continue en prenant encore 70 € que l'on distribue aux 70 personnes. Celles-ci possèdent 2 € et il en reste 360…
- À la dernière étape, chaque personne possède 7 € et il en reste 10 que l'on ne peut plus partager si on respecte la règle qui veut qu'on ne calcule qu'avec des nombres entiers.

A chaque étape on peut écrire $500 = 70 \times 1 + 430$, $500 = 70 \times 2 + 360$, $500 = 70 \times 3 + 290$ …

qui sont des égalités correctes mais ne correspondent pas à une division euclidienne car la distribution n'est pas complète. Celle-ci est complète lorsque le **reste est strictement inférieur à 70**.

$\mathbf{500 = 70 \times 7 + 10}$ en vérifiant que $\mathbf{0 \leq 10 < 70}$



[1] **Euclide**, né vers -325, mort vers -265 à Alexandrie, est un mathématicien de la Grèce antique, auteur des *Éléments*, qui sont considérés comme l'un des textes fondateurs des mathématiques modernes.

En arithmétique, la **division euclidienne ou division entière** est une opération qui, à deux entiers appelés **dividende a** et **diviseur b**, associe deux entiers appelés **quotient q** et **reste r**. Initialement définie pour deux entiers naturels non nuls, elle se généralise aux entiers relatifs.

Cette division est à la base des théorèmes de l'arithmétique élémentaire. On peut aussi définir une division euclidienne sur d'autres ensembles comme l'ensemble des polynômes.

1.2 Diviseurs

Définition :

On rappelle que l'ensemble des entiers relatifs $\mathbb{Z} = \{\dots\dots ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3 ; 4 ; \dots\dots\}$

Soit a un entier relatif et b un entier relatif *non nul*.

S'il existe un entier relatif k tel que $\boldsymbol{bk = a}$, alors **b divise a**

On dit aussi : a est divisible par b ; **b est un diviseur de a** ; On note : $\boldsymbol{b|a}$ et on lit **b divise a.**[2]

Exemples :

- Les diviseurs de 12 sont :
$$\boldsymbol{D(12)} = \{\mathbf{1} ; \mathbf{2} ; 3 ; \mathbf{4} ; 6 ; 12 ; -\mathbf{1}; -\mathbf{2} ; -3 ; -\mathbf{4} ; -6; -12\}$$
- Les diviseurs de -16 sont :
$$\boldsymbol{D(-16)} = \{\mathbf{1} ; \mathbf{2} ; \mathbf{4} ; 8 ; 16 ; -\mathbf{1}; -\mathbf{2} ; -\mathbf{4} ; -8 ; -16\}$$
- Les **diviseurs communs** de 12 et -16 sont : $\boldsymbol{D(12, -16)} = \{1 ; 2 ; 4 ; -1; -2 ; -4\}$
- Ainsi on a $1|12$; $2|12$; $3|12$;… $1|-16$; $2|-16$; $4|-16$; $-1|-16$; $-2|-16$; etc.

Propriétés :

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Les propositions suivantes sont équivalentes :

- $b|a$
- $-b|a$
- $b|-a$
- $-b|-a$

Démonstration de l'équivalence $\boldsymbol{b|a \Leftrightarrow -b|a}$:

Les propositions suivantes sont équivalentes :

- $b|a$
- Il existe $k \in \mathbb{Z}$ tel que $bk = a$
- Il existe $-k \in \mathbb{Z}$ tel que $-b \times -k = a$
- $-b|a$

Les autres propositions équivalentes s'obtiennent avec la même méthode.

Conséquence :

- a et $-a$ ont les mêmes diviseurs b dans $\mathbb{Z}$
- Les diviseurs négatifs de a sont les opposés des diviseurs positifs de a.
- On étudie souvent seulement les diviseurs qui sont dans $\mathbb{N}$. On obtient facilement tous les diviseurs en prenant aussi leurs opposés.

[2] Il est équivalent de dire que a est un multiple de b.

Propriété :

Soit $a \in \mathbb{N}^*$

Tout diviseur positif b de a est tel que $1 \leq b \leq a$

Démonstration :

Soit un entier $a \in \mathbb{N}^*$ et soit $b \in \mathbb{N}^*$ un diviseur de a.

Donc, il existe $k \in \mathbb{N}^*$ tel que $bk = a$

Comme $k \geq 1$, on a $bk \geq b$

D'où $a \geq b$. Tout diviseur strictement positif b est inférieur ou égal à a.

Ainsi, a a au plus a diviseurs dans $\mathbb{N}^*$.

Et donc, a a au plus $2a$ diviseurs dans $\mathbb{Z}^*$.

Conséquence :

Tout $a \in \mathbb{Z}^*$ a un nombre fini de diviseurs, tous compris entre $-a$ et a

Remarques :

- $b \times 0 = 0$ est vrai pour tout $b \in \mathbb{Z}^*$ donc **0 a comme diviseurs tous les entiers b non nuls.** Par exemple 37 est un diviseur de 0 car il existe un entier relatif k tel que $0 = 37k$ **$(k = 0)$**
- Tout $a \in \mathbb{Z}\backslash\{1\}$ s'écrit $1 \times a = a$. Donc tout entier relatif a sauf 1, a au moins deux diviseurs dans $\mathbb{Z}$: $b = \mathbf{1}$; $b = \boldsymbol{a}$
- **$a = 1$ a exactement un diviseur**

1.3 Nombres premiers entre eux

Définition : Deux entiers relatifs a et b **sont premiers entre eux**[3] équivaut à :

a et b n'ont que **deux diviseurs communs** : 1 et -1 ou $PGCD(a, b) = 1$

Exemple -35 (qui a pour diviseurs $\mathbf{1}$; 5 ; 7; 35 ; $-\mathbf{1}$; -5 ; -7; -35) et 12 sont **premiers entre eux.**

Remarques : **1 et -1** sont premiers avec tout entier. **0** n'est premier avec aucun (sauf 1 et -1)

Pour tout $p \in \mathbb{Z}$ et tout $q \in \mathbb{Z}^*$, $\frac{\boldsymbol{p}}{\boldsymbol{q}}$ **est irréductible** équivaut **à $\boldsymbol{p}$ et $\boldsymbol{q}$ sont premiers entre eux**.

1.4 Transitivité de la division

Pour tous entiers $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, $c \in \mathbb{Z}^*$: **Si $\boldsymbol{c}$ divise $\boldsymbol{b}$ et $\boldsymbol{b}$ divise $\boldsymbol{a}$ alors $\boldsymbol{c}$ divise $\boldsymbol{a}$**

Démonstration :

D'après la définition de diviseur : Si **$\boldsymbol{c}$ est un diviseur** de b alors il existe $k \in \mathbb{Z}$ tel que $\boldsymbol{kc} = b$

Si **$\boldsymbol{b}$ est un diviseur de $\boldsymbol{a}$** alors il existe $k' \in \mathbb{Z}$ tel que $\boldsymbol{k'b} = a$

D'où : $\boldsymbol{k'kc} = a$

$k'k$ est un entier relatif. Donc c divise a.

Exemples :

- 2 divise 4 et 4 divise 12 donc 2 divise 12
- Si b divise 16 , et puisque 16 divise $16\,n$, alors b divise $16n$.

[3] On dit aussi parfois « a et b sont **étrangers** »

1.5 Divisibilité de toute combinaison linéaire par tout diviseur commun

On appelle *combinaison linéaire entière* des entiers a et b l'entier $\boldsymbol{ua + vb}$ où u et v sont des entiers relatifs.

Exemple : $-3a + 4b$ est une combinaison linéaire entière de a et b.

Pour tout $a \in \mathbb{Z}$, pour tout $b \in \mathbb{Z}$, pour tout $c \in \mathbb{Z}^*$:

Si c est un diviseur commun à a et b **alors** c divise toute combinaison linéaire entière de la forme $ua + vb$ où u et v sont des entiers relatifs.

Cas particuliers

* *Cas :* $u = 1$ et $v = 1$ Si c divise a et b alors c divise la somme $a + b$

Par exemple, 4 est un diviseur commun à 12 et 16 donc 4 divise $12 + 16 = 28$

* *Cas :* $u = 1$ et $v = -1$ Si c divise a et b alors c divise la différence $a - b$

Par exemple, 4 est un diviseur commun à 12 et 16 donc 4 divise $12 - 16 = -4$

Démonstration :

Si c est un diviseur commun à a et b alors d'après la définition de diviseur :

Il existe deux entiers relatifs k et k' tels que $\boldsymbol{kc = a}$ et $\boldsymbol{k'c = b}$

Donc la combinaison linéaire $ua + vb$ s'écrit $ua + vb = u\boldsymbol{kc} + v\boldsymbol{k'c}$

$$ua + vb = (uk + vk') \times c$$

$uk + vk'$ est un entier relatif. Puisque $(\boldsymbol{uk + vk'})c = ua + vb$ alors **c divise** $ua + vb$

Exemple :

* Soit c un diviseur commun de 3 et 5 Proposer un ensemble dans lequel on est certain de trouver c.

Réponse : **Si** $\begin{cases} c \text{ divise } 3 \\ c \text{ divise } 5 \end{cases}$ **alors** c divise également $2 \times 5 + 3 \times 3 = 19$

Comme 19 n'a que quatre diviseurs : 1, 19 et -1, -19 on en déduit que $c \in \{1; 19; -1; -19\}$.

2 La division euclidienne de a par b

2.1 Théorème sur l'existence et l'unicité d'un couple d'entiers naturels $(q ; r)$

Pour tout couple $(\boldsymbol{a} ; \boldsymbol{b}) \in \mathbb{N} \times \mathbb{N}^*$ il ***existe*** un couple ***unique*** d'entiers naturels $(\boldsymbol{q} ; \boldsymbol{r})$ tels que

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

* $\boldsymbol{a}$ est le dividende (valeur à partager)
* $\boldsymbol{b}$ est le diviseur (nombre de parts)
* $\boldsymbol{q}$ est le quotient (valeur d'une part)
* $\boldsymbol{r}$ est le reste (qui ne peut plus être divisé, toujours strictement inférieur au diviseur b).

Exemple :

Si $\boldsymbol{a = 500}$ et $\boldsymbol{b = 70}$

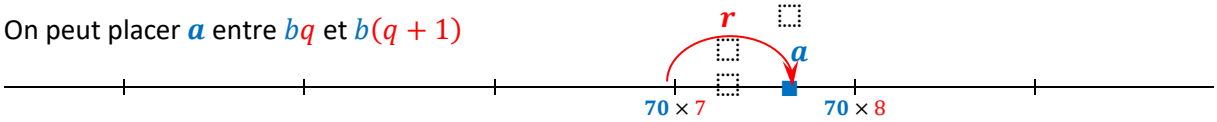
Alors $500 = 70 \times 7 + 10$ avec $0 \leq 10 < 70$

Donc la division euclidienne associe au couple $(\boldsymbol{a} ; \boldsymbol{b}) = (\boldsymbol{500} ; \boldsymbol{70})$ le couple $(\boldsymbol{q} ; \boldsymbol{r}) = (\boldsymbol{7} ; \boldsymbol{10})$

Illustration graphique :

Sur l'axe des multiples positifs de b :

On peut placer a entre bq et $b(q+1)$



Remarque 1 :

Parmi les multiples écritures $a = bq + r$, seule celle où $0 \leq r < b$ est la relation de la division euclidienne de a par b

$500 = 70 \times 0 + 500$; $500 = 70 \times 1 + 430$; $500 = 70 \times 2 + 360$; $500 = 70 \times 3 + 290$ …

Seule, $\mathbf{500 = 70 \times 7 + 10}$ est *la relation de division euclidienne* de 500 par 70 car $0 \leq \mathbf{10} < \mathbf{70}$

Remarque 2 :

Pour trouver q, on peut faire la division exacte de a par b. q est la partie entière[4] de $\frac{a}{b}$

Exemple :

$$\frac{500}{70} = 7{,}14\ldots$$

Si $a = 500$ et $b = 70$ alors la division euclidienne du dividende a par b donne le quotient $q = 7$.

Remarque 3 :

Comme la division euclidienne doit respecter la condition $0 \leq r < b$ alors le reste r ne peut prendre que $\boldsymbol{b}$ valeurs possibles : tous les entiers de $\mathbf{0}$ à $\boldsymbol{b} - \mathbf{1}$

Exemple : dans la division par $\boldsymbol{b = 70}$ le reste $\boldsymbol{r}$ peut prendre l'une des 70 valeurs entières de 0 à 69.

Remarque 4 :

La division de a par b a pour reste $\boldsymbol{r = 0}$ équivaut à $\boldsymbol{b}$ divise $\boldsymbol{a}$ (noté $b|a$)

Par exemple, si $\boldsymbol{a = 60}$ et $\boldsymbol{b = 5}$ alors $\boldsymbol{q = 12}$ et $\boldsymbol{r = 0}$ $\mathbf{5}$ divise $\mathbf{60}$ (noté $5|60$)

Remarque 5 :

Dans notre système de numération décimale, le chiffre des unités est le reste de la division euclidienne du nombre par 10.

Exemple : si $\boldsymbol{a = 357}$ et $\boldsymbol{b = 10}$ alors $\boldsymbol{q = 35}$ et $\boldsymbol{r = 7}$ (avec $0 \leq r < 10$)

Démonstration du théorème de la division euclidienne dans $\mathbb{N}$ pour tout couple $(a\,;b) \in \mathbb{N} \times \mathbb{N}^*$

∗ Démontrons l'existence d'au moins un couple $(q\,;r)$ d'entiers naturels tels que $a = bq + r$.

La suite des multiples positifs de b est : $0\,;b\,;2b\,;\ldots;kb\,;\ldots$ avec $k \in \mathbb{N}$.

Si a est divisible par b, alors a est un des termes de la suite ci-dessus. Donc dans ce cas on a $a = bk + 0$ avec $k \in \mathbb{N}$. Donc q et r existent ($q = k$ et $r = 0$).

[4] **Fonction partie entière** : Cette fonction notée E associe à tout réel x l'entier relatif immédiatement inférieur ou égal à x. Par exemple, $E(5{,}2) = 5$; $E(-3{,}2) = -4$; $E(6) = 6$. Sur la calculatrice TI, pour avoir la partie entière de 500/70, aller dans **math**, menu NUM, 5 :partEnt(500/70) ou 5 :int(500/70) en anglais.

Si a n'est pas divisible par b alors il existe des multiples de b inférieurs à a et d'autres supérieurs à a. Ainsi il existe un entier relatif q tel que $bq < a < b(q+1)$.

* Démontrons l'unicité du couple $(q\,;r)$

On a vu qu'il existe au moins un couple d'entiers naturels $(\boldsymbol{q}\,;\boldsymbol{r})$ vérifiant les deux conditions :

$\boldsymbol{a = bq + r}$ **et** $\boldsymbol{0 \leq r < b}$

Alors en ajoutant bq aux trois membres de l'inégalité on a : $bq \leq bq + r < bq + b$

Soit $bq \leq a < b(q+1)$. En divisant par b on a $q \leq \frac{a}{b} < q + 1$

D'où, comme q et $q+1$ sont deux entiers consécutifs, $q = E\left(\frac{a}{b}\right)$. Donc q est unique et donc r aussi.

2.2 Division euclidienne dans $\mathbb{Z}$

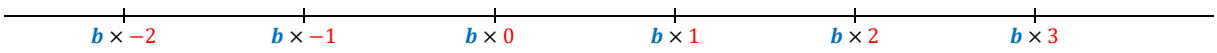
On a démontré que, dans tous les cas, étant donnés $a \in \mathbb{N}$ *et* $b \in \mathbb{N}^*$, il existe un couple d'entiers unique $(q\,;r) \in \mathbb{N} \times \mathbb{N}$ tels que $a = bq + r$ *et* $0 \leq r < b$.

On peut démontrer aussi que :

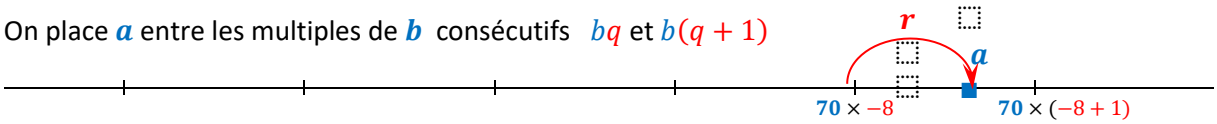
Etant donné $a \in \mathbb{Z}$ *et* $b \in \mathbb{N}^*$, il existe un couple d'entiers unique $(q\,;r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r$ *et* $0 \leq r < \boldsymbol{b}$.

Illustration graphique :

Sur l'axe des réels gradué tous les $\boldsymbol{bk}$ avec $k \in \mathbb{Z}$ (multiples de b)



On place $\boldsymbol{a}$ entre les multiples de $\boldsymbol{b}$ consécutifs bq et $b(q+1)$



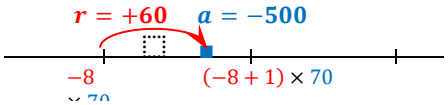
Exemple :

Si $\boldsymbol{a = -500}$ et $\boldsymbol{b = 70}$

Alors $-500 = 70 \times -8 + 60$ avec $0 \leq 60 < 70$

Donc $(\boldsymbol{q}\,;\boldsymbol{r}) = (-8\,;60)$

Graduations : multiples de $\boldsymbol{70}$



2.3 Propriétés de la relation de division euclidienne de a par b

Soit un couple $(a\,;b) \in \mathbb{Z} \times \mathbb{N}^*$

b divise a si, et seulement, dans la division euclidienne de a par b, le reste $r = 0$.

On donne un entier naturel $\boldsymbol{b}$ supérieur ou égal à 2.

Tout entier relatif a s'écrit sous l'une, et une seule, des formes suivantes :

$$bq, bq+1, bq+2, \ldots, bq+(b-1)$$

Exemple avec $b = 70$:

Tout entier relatif a s'écrit sous l'une, et une seule, des formes suivantes :

$$70q + 0\,,\quad 70q + 1\,,\quad 70q + 2\,,\ldots,\quad 70q + 69$$

Par exemple, si on choisit $a = -500$, a s'écrit $70 \times q + 60$

On donne un entier naturel b supérieur ou égal à 2.
Parmi b entiers consécutifs, un et un seul est multiple de b.

Exemple avec $b = 70$:

Dans la suite des 70 entiers consécutifs $100\ ;\ 101\ ;102\ ;\ \ldots ;\ 169$, un et un seul est multiple de **70**.

Autre exemple :

Soit $n \in \mathbb{Z}$. Dans la suite $n-1\ ;\ n\ ;\ n+1\ ;\ n+2\ ;\ n+3$, il y a un et un seul multiple de **5**.

3 Les nombres premiers

3.1 Définition d'un nombre premier

Un nombre premier p est un naturel qui possède *exactement deux* diviseurs positifs : 1 et lui-même.

Exemples :

p	Diviseurs positifs de p	Nombre de diviseurs positifs	p est-il premier ?
0	$1\ ;2\ ;3\ ;4\ ;5\ ;6\ ;7\ ;8\ ;9\ ;10\ ;\ldots$	Une infinité	non
1	1	1	non
2	$1\ ;2$	**2**	**oui**
3	$1\ ;3$	**2**	**oui**
4	$1\ ;2\ ;4$	3	non
5	$1\ ;5$	**2**	**oui**
6	$1\ ;2\ ;3\ ;6$	4	non

Vocabulaire :

Un nombre entier naturel supérieur ou égal à 2 non premier est dit *nombre composé*.
Par exemple, 4 et 6 sont composés.

Remarques :

1. Le plus petit nombre premier est 2. C'est le seul qui soit pair.
2. Les nombres premiers inférieurs ou égaux à 50 sont
   $2\ ;3\ ;5\ ;7\ ;11\ ;13\ ;17\ ;19\ ;23\ ;29\ ;31\ ;37\ ;41\ ;43\ ;47$. il y en a 15. On note $\pi(50) = 15$
3. Les nombres premiers ont une définition simple, mais peuvent conduire à des problèmes difficiles. Par exemple, la conjecture[5] « Tout nombre **pair** différent de deux peut être décomposé en somme de deux nombres premiers » semble vraie, mais elle n'a pas encore été démontrée.
4. Ne pas confondre « a et b sont des nombres premiers » et « a et b sont des nombres premiers entre eux »

Exemples :

a	b	Diviseurs positifs de a	Diviseurs positifs de b	a et b sont premiers	Diviseurs positifs communs	a et b sont premiers entre eux
2	2	$1\ ;2$	$1\ ;2$	oui	$1\ ;2$	non
2	3	$\mathbf{1}\ ;2$	$\mathbf{1}\ ;3$	oui	1	oui
2	4	$1\ ;2$	$1\ ;2\ ;4$	non	$1\ ;2$	non
3	4	$\mathbf{1}\ ;3$	$\mathbf{1}\ ;2\ ;4$	non	1	oui

[5] Cette conjecture fut émise par **Christian Goldbach**, mathématicien allemand, en 1742

5. Pour **tout nombre premier $\boldsymbol{p}$** et pour tout $n \in \mathbb{N}$, on est *dans l'une ou bien dans l'autre* des situations :

* p divise n
* p est premier avec n

Exemples :

p	n	Diviseurs positifs de p	Diviseurs positifs de n	p divise n	p et n sont premiers entre eux
2	2	1 ; 2	1 ; 2	oui	
2	3	**1** ; 2	**1** ; 3		oui
2	4	1 ; 2	1 ; 2 ; 4	oui	
2	5	**1** ; 2	**1** ; 5		oui
3	2	**1** ; 3	**1** ; 2		oui
3	3	1 ; 3	1 ; 3	oui	
3	4	**1** ; 3	**1** ; 2 ; 4		oui
3	5	**1** ; 3	**1** ; 5		oui
5	2	**1** ; 5	**1** ; 2		oui
5	3	**1** ; 5	**1** ; 3		oui
5	4	**1** ; 5	**1** ; 2 ; 4		oui
5	5	1 ; 5	1 ; 5	oui	

3.2 Théorème des diviseurs premiers

Pour tout $n \in \mathbb{N}$, tel que $n \geq 2$ on est *dans l'une ou bien dans l'autre* des situations :

* Si n est premier alors n admet **<u>un seul</u> diviseur premier : lui-même**
* Si n est composé alors n admet **<u>au moins un</u> diviseur premier $\boldsymbol{p}$** qui vérifie la relation $p \leq \sqrt{n}$

Par exemple :

n	$\sqrt{n}$	Diviseurs positifs de n	Diviseurs premiers de n	n admet <u>un seul</u> diviseur premier : lui-même	n admet <u>au moins un</u> diviseur premier $\boldsymbol{p}$ <u>tel que $p \leq \sqrt{n}$</u>
2	$\approx 1{,}414$	1 ; **2**	2	oui	
3	$\approx 1{,}732$	1 ; **3**	3	oui	
4	2	1 ; **2** ; 4	2		oui
5	$\approx 2{,}336$	1 ; **5**	5	oui	
6	$\approx 2{,}449$	1 ; **2** ; 3 ; 6	2 ; 3		oui
7	$\approx 2{,}646$	1 ; **7**	7	oui	
8	$\approx 2{,}828$	1 ; **2** ; 4 ; 8	2		oui
9	3	1 ; **3** ; 9	3		oui
10	$\approx 3{,}162$	1 ; **2** ; 5 ; 10	2 ; 5		oui
11	$\approx 3{,}317$	1 ; **11**	11	oui	
12	$\approx 3{,}464$	1 ; **2** ; **3** ; 4 ; 6 ; 12	2 ; 3		oui

Remarque : Un entier N peut avoir un diviseur premier supérieur à $\sqrt{N}$. Exemple : $985 = 5 \times \mathbf{197}$

Démonstration du théorème des diviseurs premiers :

Pour tout $n \in \mathbb{N}$, tel que $n \geq 2$:

- Si n est premier alors n admet exactement deux diviseurs : 1 et lui-même. Mais comme 1 n'est pas premier, alors n admet bien un seul diviseur premier : lui-même.
- Si n n'est pas premier alors n admet d'autres diviseurs d_0 ; d_1 ; d_2; … différents de 1 et de lui-même avec $1 < d_0 < d_1 < d_2 < \cdots < n$

1. Montrons que parmi ces diviseurs, le plus petit d_0 est premier :

Supposons que d_0 soit composé, c'est-à-dire que d_0 a des diviseurs autres que 1 est lui-même.

Si d_0 n'est pas premier alors d_0 admet d'autres diviseurs d'_0 ; d'_1 ; d'_2; … différents de 1 et de lui-même avec $1 < d'_0 < d'_1 < d'_2 < \cdots < d_0$

d'_0 ; d'_1 ; d'_2; … étant des diviseurs de d_0 qui est un des diviseurs de n seraient aussi des diviseurs de n

On aurait donc $1 < d'_0 < d'_1 < d'_2 < \cdots < d_0 < d_1 < d_2 < \cdots < n$

et donc d_0 ne serait pas le plus petit des diviseurs de n.

On voit que la *supposition* conduit à une contradiction. Donc elle est fausse.

Conclusion : d_0, le plus petit des diviseurs de n, est premier

Notons $p = d_0$ le plus petit diviseur premier de n

2. Montrons que, le plus petit diviseur p est tel que $p \leq \sqrt{n}$:

Cela équivaut à montrer que $\boldsymbol{p^2 \leq n}$

On a $1 < p < n$ où p est un diviseur de n

donc il existe aussi un diviseur de n noté q tel que $p \times q = n$ où $q \geq p$ (puisque p est le plus petit des diviseurs autres que 1)

On a donc $p \leq q$

$p^2 \leq p \times q$

$p^2 \leq n$

Conclusion :

- Dans le cas où n n'est pas premier, il a au moins un diviseur premier p tel que $p \leq \sqrt{n}$
- Dans le cas où n n'est pas premier, le plus petit de ses diviseurs d_0 (différent de 1) est premier.

3.3 Tester la primalité

Soit un nombre $n \in \mathbb{N}$ supérieur ou égal à 2.

D'après le théorème des diviseurs premiers, si n n'a aucun diviseur premier p inférieur ou égal à $\sqrt{n}$ alors n est premier.

Exemple :

Tester la primalité de $n = 2011$

Le test consiste à essayer de diviser 2011 par les premiers nombres premiers dans l'ordre croissant :

$$2\ ;\ 3\ ;\ 5\ ;\ 7\ ;\ 11\ ;\ 13\ ;\ 17\ ;\ 19\ ;\ 23\ ;\ 29\ ;\ 31\ ;\ 37\ ;\ 41\ ;\ 43$$

On sait que $\sqrt{2011} \approx 44{,}844$. Donc on ne cherchera pas si n est divisible par un nombre premier strictement supérieur à 44

d		$n = 2011$ est divisible par d
2	2011 n'est pas pair	non
3	$2 + 0 + 1 + 1 = 4$ n'est pas un multiple de 3	non
5	2011 ne se termine pas par 0 ou 5	non
7	$\overline{a_3 a_2 a_1} - 2a_0 = 201 - 2 \times 1 = 199$ non divisible par 7	non
11	$(a_0 + a_2) - (a_1 + a_3) = (1 + 0) - (1 + 2) = -2$ non divisible par 11	non
13	$2011/13 \approx 154{,}692$	non
17	$2011/17 \approx 118{,}294$	non
19	$2011/19 \approx 105{,}842$	non
23	$2011/23 \approx 87{,}435$	non
29	$2011/29 \approx 69{,}345$	non
31	$2011/31 \approx 64{,}871$	non
37	$2011/37 \approx 54{,}351$	non
41	$2011/41 \approx 49{,}049$	non
43	$2011/43 \approx 46{,}767$	non

Conclusion : $n = 2011$ est premier.

Remarques :

- Tester la primalité d'un nombre n peut demander beaucoup de calculs.
- Pour obtenir un tableau de nombres premiers, plutôt que d'effectuer le test de primalité pour chaque nombre, on peut utiliser **un crible**, c'est-à-dire une méthode d'élimination en raisonnant par exemple avec les multiples.

Ainsi, le crible d'Eratosthène[6] consiste à dresser un tableau des entiers naturels de 1 à n et à barrer 1 puis les entiers multiples de 2 sauf 2, puis les multiples de 3 sauf 3, puis les multiples de 5 sauf 5. Ainsi de suite. On barre les multiples des premiers nombres premiers p en commençant par barrer p^2. On s'arrête si p^2 est strictement supérieur à n. Donc pour connaitre la primalité des entiers jusqu'à $n = 39000$ par exemple, il suffira de tester la primalité des entiers compris entre 2 et 198 car $198^2 = 39204$. On trouve 45 nombres premiers inférieurs ou égaux à 198.

[6] **Eratosthène**, 3ème siècle avant J-C. Mathématicien grec qui a vécu à Alexandrie. Il détermina que la Terre était ronde en calculant son diamètre à 12540 km (alors qu'en réalité il mesure 12760 km).

3.4 Théorème sur l'infinité des nombres premiers

Théorème :

Il existe une infinité de nombres premiers.

Démonstration :

On considère les n premiers nombres premiers $p_1 = 2$; $p_2 = 3$; $p_3 = 5$; … ; p_n

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

Exemples :

N	N	N premier ?
$p_1 + 1$	$2 + 1 = 3$	oui
$p_1 \times p_2 + 1$	$2 \times 3 + 1 = 7$	oui
$p_1 \times p_2 \times p_3 + 1$	$2 \times 3 \times 5 + 1 = 31$	oui
$p_1 \times p_2 \times p_3 \times p_4 + 1$	$2 \times 3 \times 5 \times 7 + 1 = 211$	oui
$p_1 \times p_2 \times p_3 \times p_4 \times p_5 + 1$	$2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$	oui
$p_1 \times p_2 \times p_3 \times p_4 \times p_5 \times p_6 + 1$	$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$	non[7]
$p_1 \times p_2 \times p_3 \times p_4 \times p_5 \times p_6 \times p_7 + 1$	$2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 + 1 = 510511$	non[8]

1. Cas où N est premier

Dans ce cas, comme N est strictement supérieur au produit des n premiers nombres premiers, nous obtenons un autre nombre premier que l'un des n premiers nombres premiers considérés au départ. Donc on peut obtenir autant de nombres premiers que l'on veut. Autrement dit, il y a une infinité de nombres premiers.

2. Cas où N est composé. Montrons que l'un des facteurs de N est un nombre premier différent des n premiers nombres premiers p_1 ; p_2 ; … ; p_n

D'après le théorème des diviseurs premiers, si N est composé alors N admet au moins un **diviseur premier** p (qui vérifie la relation $p \leq \sqrt{n}$).

Supposons que p soit l'un des premiers nombres premiers p_1 ; p_2 ; … ; p_n. Donc on peut écrire :

$$N = p_1 \times p_2 \times \ldots \times \boldsymbol{p} \times \ldots \times p_n + 1$$

$$N = p\left(p_1 \times p_2 \times \ldots\ldots \times p_n + \frac{1}{p}\right)$$

Comme $\frac{1}{p}$ n'est pas un entier alors la somme $p_1 \times p_2 \times \ldots\ldots \times p_n + \frac{1}{p}$ n'est pas un entier

ce qui est contradictoire avec le fait que $p\left(p_1 \times p_2 \times \ldots\ldots \times p_n + \frac{1}{p}\right)$ est un entier.

On voit que la *supposition* conduit à une contradiction. Donc elle est fausse.

Conclusion : L'entier N permet d'obtenir un nombre premier différent des n premiers nombres premiers considérés au départ. Donc on peut obtenir autant de nombres premiers que l'on veut. Autrement dit, il y a une infinité de nombres premiers.

Exemple : On peut trouver de très grands nombres premiers comme $M_{57885161} = 2^{57885161} - 1$

Remarque : Un nombre $M_p = 2^p - 1$ *où* p *est premier* est un nombre de **Mersenne**. Les 4 premiers nombres de Mersenne M_2 ; M_3 ; M_5 ; M_7 sont premiers, mais la plupart comme M_{11} ne le sont pas.

[7] 30031 est divisible par $p_{17} = 59$

[8] 510511 est divisible par $p_8 = 19$

4 Existence et unicité de la décomposition en facteurs premiers

4.1 Théorème fondamental de l'arithmétique

- Pour tout entier naturel n supérieur ou égal à 2 **il existe une décomposition** en produit de facteurs premiers.
- Pour un entier n donné, cette décomposition est **unique**, à l'ordre des facteurs près.

Exemples :

$n = 2011$ n est premier. La décomposition est $\boldsymbol{n = 2011}$

$n = 3760$ n n'est pas premier. On commence par déterminer le plus petit diviseur premier.

Ici, c'est 2 $\frac{3760}{2} = 1880$

1880 est aussi divisible par $\frac{1880}{2} = 940$

etc.

On présente plus rapidement les calculs dans un tableau où apparaissent les diviseurs premiers dans l'ordre croissant :

3760	2
1880	2
940	2
470	2
235	5
47	47
1	

La décomposition de $n = 3760$ est donc $\boldsymbol{n = 2^4 \times 5 \times 47}$

La forme générale de la décomposition de n est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots p_k^{\alpha_k}$

où p_1 ; p_2 ; … ; p_n sont des nombres premiers distincts et où α_1 ; α_2 ; … ; α_n sont des entiers naturels non nuls

Remarque :

Tout entier n supérieur ou égal à 2 s'écrivant $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots p_k^{\alpha_k}$ est divisible par p_1 ; p_2 ; … ; p_k et aussi par tout produit partiel de ses facteurs premiers. Par exemple n est divisible par $p_1 \times p_2$; $p_1 \times p_3$; … ; ${p_1}^2 \times p_2$; $p_1 \times {p_2}^2$; ${p_1}^2 \times {p_2}^2$; …

De façon générale, n est divisible par $p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times \dots p_k^{\beta_k}$ où β_1 ; β_2 ; … ; β_n sont des entiers naturels inférieurs ou égaux à α_1 ; α_2 ; … ; α_n

Exemple :

$3760 = 2^4 \times 5 \times 47$ $3760 = (2^2) \times (2^2 \times 5 \times 47)$ 3760 est divisible par $2^2 \times 5 \times 47 = 940$

Démonstration du théorème fondamental de l'arithmétique :

1. Existence d'une décomposition de n en produit de facteurs premiers

D'après le théorème des diviseurs premiers :

Pour tout $n \in \mathbb{N}$, tel que $n \geq 2$ n admet **au moins un diviseur premier** p_1

- Lorsque n est premier on a $n = p_1$

  D'où $\boxed{n = p_1}$ avec p_1 qui est premier. *Le théorème est démontré dans ce cas.*

- Lorsque n est composé on a $n = p_1 \times n_1$ avec $1 < p_1 < n$ et $1 < n_1 < n$
  Comme n_1 est un entier strictement supérieur à 1, d'après le théorème des diviseurs premiers, n_1 admet **au moins un diviseur premier** p_2

  - Lorsque n_1 est premier on a $n_1 = p_2$

    D'où $\boxed{n = p_1 \times p_2}$ avec p_1 et p_2 qui sont premiers. *Le théorème est démontré dans ce cas*.

  - Lorsque n_1 est composé on a $n_1 = p_2 \times n_2$ avec $1 < p_2 < n_1$ et $1 < n_2 < n_1$

    Comme n_2 est un entier strictement supérieur à 1, d'après le théorème des diviseurs premiers, n_2 admet **au moins un diviseur premier** p_3

    - Lorsque n_2 est premier on a $n_2 = p_3$
      D'où $\boxed{n = p_1 \times p_2 \times p_3}$ avec p_1 p_2 et p_3 qui sont premiers. *Le théorème est démontré dans ce cas*

    - Lorsque n_2 est composé on a $n_2 = p_3 \times n_3$ avec $1 < p_3 < n_2$ et $1 < n_3 < n_2$
      Comme n_3 est un entier strictement supérieur à 1, d'après le théorème des diviseurs premiers, n_3 admet **au moins un diviseur premier** p_4

On poursuit le même raisonnement tant que l'entier n_i est composé. On obtient une suite d'entiers tels que $1 < \cdots < n_i < \cdots < n_3 < n_2 < n_1 < n$.

La liste des entiers positifs n_i est strictement décroissante et est minorée par 1. Donc cette liste est finie la plus petite valeur éventuellement prise par n_i étant 2 qui est un nombre premier).

Donc au bout d'un nombre fini d'étapes, on aboutit à n_i est premier et on a $n_i = p_i$.

Donc dans tous les cas, on finit par obtenir la décomposition de n en un produit fini de facteurs premiers :

$$\boxed{n = p_1 \times p_2 \times p_3 \times \ldots \times p_i}$$

2. Unicité de la décomposition de n en produit de facteurs premiers

Soit un entier naturel $n \geq 2$

Supposons que n ait deux décompositions en facteurs premiers :

$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \ldots p_k^{\alpha_k}$ et $n = y_1^{\beta_1} \times y_2^{\beta_2} \times y_3^{\beta_3} \times \ldots y_m^{\beta_m}$.

Alors l'un des **facteurs** y_i, par exemple y_1, **divise** n autrement dit, y_1 divise $p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \ldots p_k^{\alpha_k}$

Or y_1 est premier donc y_1 n'est pas composé. Donc y_1 n'est pas égal à un produit de facteurs premiers p_1 ; p_2 ; … ; p_k Mais y_1 est *égal à* l'un des facteurs premiers p_1 ; p_2 ; … ; p_k
En reprenant le raisonnement pour les autres facteurs premiers y_2 y_3 … y_m on aboutit à la même conclusion. Ainsi la décomposition primaire d'un nombre entier naturel $n \geq 2$ est unique.

4.2 Théorème sur la forme des diviseurs

Pour tout entier naturel n supérieur ou égal à 2 il existe une décomposition unique en produit de facteurs premiers $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots p_k^{\alpha_k}$ où α_1 ; α_2 ; … ; α_n sont des entiers naturels non nuls.
Tout diviseur positif d de n s'écrit sous la forme $d = p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times \dots p_k^{\beta_k}$ où β_1 ; β_2 ; … ; β_n sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1$; $0 \leq \beta_2 \leq \alpha_2$; $0 \leq \beta_3 \leq \alpha_3$; … ; $0 \leq \beta_n \leq \alpha_n$

Exemple :
Soit $n = 3760$. On décompose n en facteurs premiers :

3760	2
1880	2
940	2
470	2
235	5
47	47
1	

$\boldsymbol{n = 2^4 \times 5 \times 47}$
Un diviseur d de $n = 3760$ est par exemple $d = 2^3 \times 5^1 \times 47^0 = 40$

Démonstration :
1. Montrons que si $\boldsymbol{d = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots p_k^{\beta_k}}$ où $\boldsymbol{\beta_1}$; $\boldsymbol{\beta_2}$; … ; $\boldsymbol{\beta_n}$ sont des entiers tels que $\boldsymbol{0 \leq \beta_1 \leq \alpha_1}$; $\boldsymbol{0 \leq \beta_2 \leq \alpha_2}$; … ; $\boldsymbol{0 \leq \beta_n \leq \alpha_n}$ alors $\boldsymbol{d}$ divise $\boldsymbol{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots p_k^{\alpha_k}}$
Comme les entiers β_i sont tels que $0 \leq \beta_1 \leq \alpha_1$; $0 \leq \beta_2 \leq \alpha_2$; … ; $0 \leq \beta_n \leq \alpha_n$, alors il existe des entiers γ_i tels que $\beta_1 + \gamma_1 = \alpha_1$; $\beta_2 + \gamma_2 = \alpha_2$; … ; $\beta_n + \gamma_n = \alpha_n$
et donc : $n = p_1^{\beta_1+\gamma_1} \times p_2^{\beta_2+\gamma_2} \times \dots p_k^{\beta_k+\gamma_k}$
$n = p_1^{\beta_1} \times p_1^{\gamma_1} \times p_2^{\beta_2} \times p_1^{\gamma_1} \times \dots p_k^{\beta_k} \times p_1^{\gamma_k}$
$n = \left(p_1^{\beta_1} \times p_2^{\beta_2} \times \dots p_k^{\beta_k}\right) \times \left(p_1^{\gamma_1} \times p_2^{\gamma_2} \times \dots p_k^{\gamma_k}\right)$
$n = d \times \left(p_1^{\gamma_1} \times p_2^{\gamma_2} \times \dots p_k^{\gamma_k}\right)$
Conclusion : d divise n

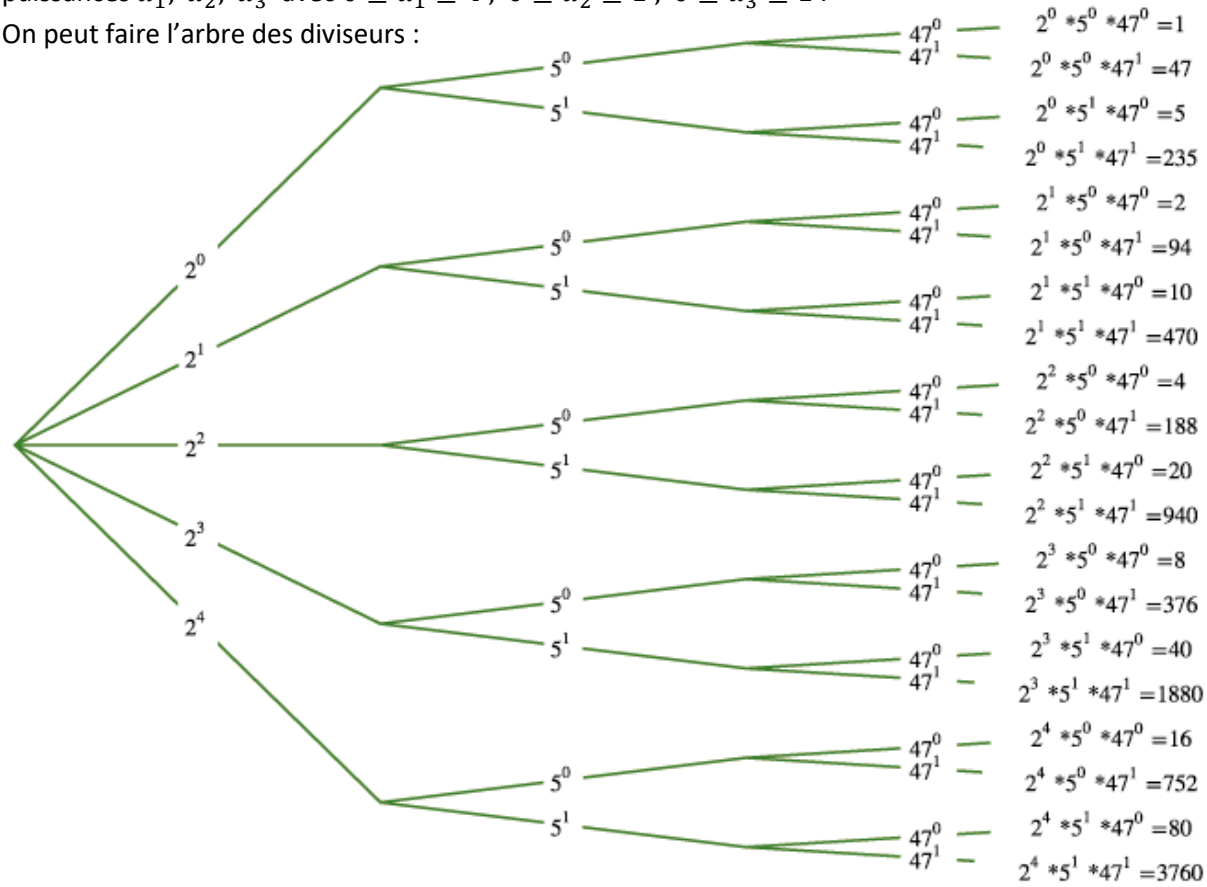
2. Réciproque : montrons que si $\boldsymbol{d}$ divise $\boldsymbol{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots p_k^{\alpha_k}}$ alors $\boldsymbol{d = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots p_k^{\beta_k}}$ où $\boldsymbol{\beta_1}$; $\boldsymbol{\beta_2}$; … ; $\boldsymbol{\beta_n}$ sont des entiers tels que $\boldsymbol{0 \leq \beta_1 \leq \alpha_1}$; $\boldsymbol{0 \leq \beta_2 \leq \alpha_2}$; … ; $\boldsymbol{0 \leq \beta_n \leq \alpha_n}$
d divise n alors $n = d \times d'$ où d et d' sont des entiers tels que $1 \leq d \leq n$ et $1 \leq d' \leq n$.
Les entiers d et d' se décomposent chacun en produit de facteurs premiers.
Le produit de ces produits est donc un produit de facteurs premiers égale à $\boldsymbol{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots p_k^{\alpha_k}}$
D'après le théorème fondamental de l'arithmétique, la décomposition en facteurs premiers de n est *unique*. Donc $d \times d' = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots p_k^{\alpha_k}$
Donc les facteurs premiers intervenant dans la décomposition du diviseur d sont les nombres premiers p_i avec une puissance β_i inférieure ou égale à α_i. Ce qui s'écrit :
$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots p_k^{\beta_k}$ avec β_1 ; β_2 ; … ; β_n tels que $0 \leq \beta_1 \leq \alpha_1$; $0 \leq \beta_2 \leq \alpha_2$; … ; $0 \leq \beta_n \leq \alpha_n$
Conclusion : Tout diviseur positif d de n s'écrit sous la forme $d = p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times \dots p_k^{\beta_k}$ où β_1 ; β_2 ; … ; β_n sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1$; $0 \leq \beta_2 \leq \alpha_2$; $0 \leq \beta_3 \leq \alpha_3$; … ; $0 \leq \beta_n \leq \alpha_n$
Remarque :

$\beta_i = 0$ lorsque le nombre premier p_i n'intervient pas dans la décomposition du diviseur d
Par exemple pour $n = 2^4 \times 5 \times 47 = 3760$, un des diviseurs est $d = 2^3 \times 5^1 \times 47^{\mathbf{0}} = 40$ dans la décomposition duquel 47 n'intervient pas.

4.3 Nombre de diviseurs d'un entier naturel supérieur ou égal à 2

Exemple : Reprenons $\boldsymbol{n = 2^4 \times 5 \times 47}$. Les diviseurs de n sont :
$2^0 \times 5^0 \times 47^0$; $2^0 \times 5^0 \times 47^1$; $2^0 \times 5^1 \times 47^0$; $2^0 \times 5^1 \times 47^1$; $2^1 \times 5^0 \times 47^0$; $2^1 \times 5^0 \times 47^1$; …

Pour obtenir tous les diviseurs de $\boldsymbol{n = 2^{\alpha_1} \times 5^{\alpha_2} \times 47^{\alpha_3}}$, on doit essayer toutes les listes de puissances α_1; α_2; α_3 avec $0 \leq \alpha_1 \leq 4$; $0 \leq \alpha_2 \leq 1$; $0 \leq \alpha_3 \leq 1$.
On peut faire l'arbre des diviseurs :



Le nombre de diviseurs positifs de 3760 est : $(4+1) \times (1+1) \times (1+1) = 20$

De façon générale, **le nombre de diviseurs positifs** de $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \ldots p_k^{\alpha_k}$ est :
$\boldsymbol{(\alpha_1 + 1) \times (\alpha_2 + 1) \times (\alpha_3 + 1) \times \ldots \times (\alpha_k + 1)}$ où α_1 ; α_2 ; … ; α_n sont des naturels non nuls.

Remarque : 3760 a 19 *diviseurs propres*[9]. La somme des diviseurs propres de 3760 est $\sigma(3760) = 1 + 47 + \cdots + 752 + 80 = 5168 \neq 3760$. Donc 3760 n'est pas un *nombre parfait*[10].

[9] Les **diviseurs propres** (ou **diviseurs stricts**) d'un entier naturel n sont tous ses diviseurs positifs y compris 1 sauf n lui-même.
[10] Un **nombre parfait** est un entier naturel égal à la somme de ses diviseurs propres. Par exemple, 28 est parfait puisque $\boldsymbol{28 = 1 + 2 + 4 + 7 + 14}$ est égal à la somme de ses diviseurs propres. Les nombres parfaits pairs sont liés aux nombres de Mersenne premiers. On connait 47 nombres parfaits (le plus petit est 6 et le plus grand connu est $2^{43112608} \times M_{43112609} = 2^{43112608} \times (2^{43112609} - 1)$).

5 Congruences dans $\mathbb{Z}$

5.1 Définition

Soit $c \in \mathbb{N}^*$. Pour tous couples $(a\,;b)$ d'entiers relatifs, il est équivalent de dire :

- a et b ont le même reste dans la division par c
- $a-b$ est un multiple de c (c'est-à-dire c divise $a-b$)
- a et b sont ***congrus modulo*** c

Exemple : -8 et 28 sont « congrus modulo 12 » car $(-8)-28=-\mathbf{3}\times\mathbf{12}$. On écrit $-8\equiv 28\ (12)$

Symbole introduit en 1801 par C. F. Gauss

12 est le ***diviseur*** également appelé ***module***

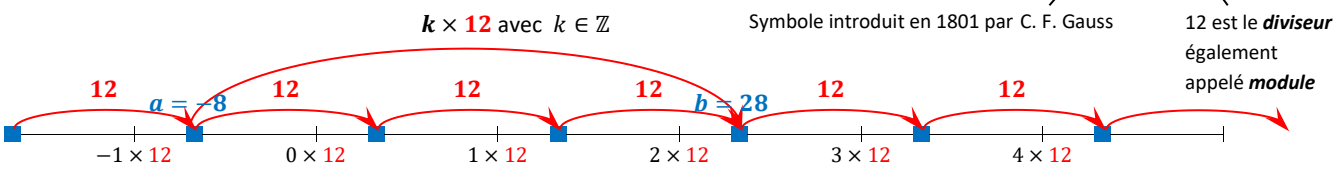
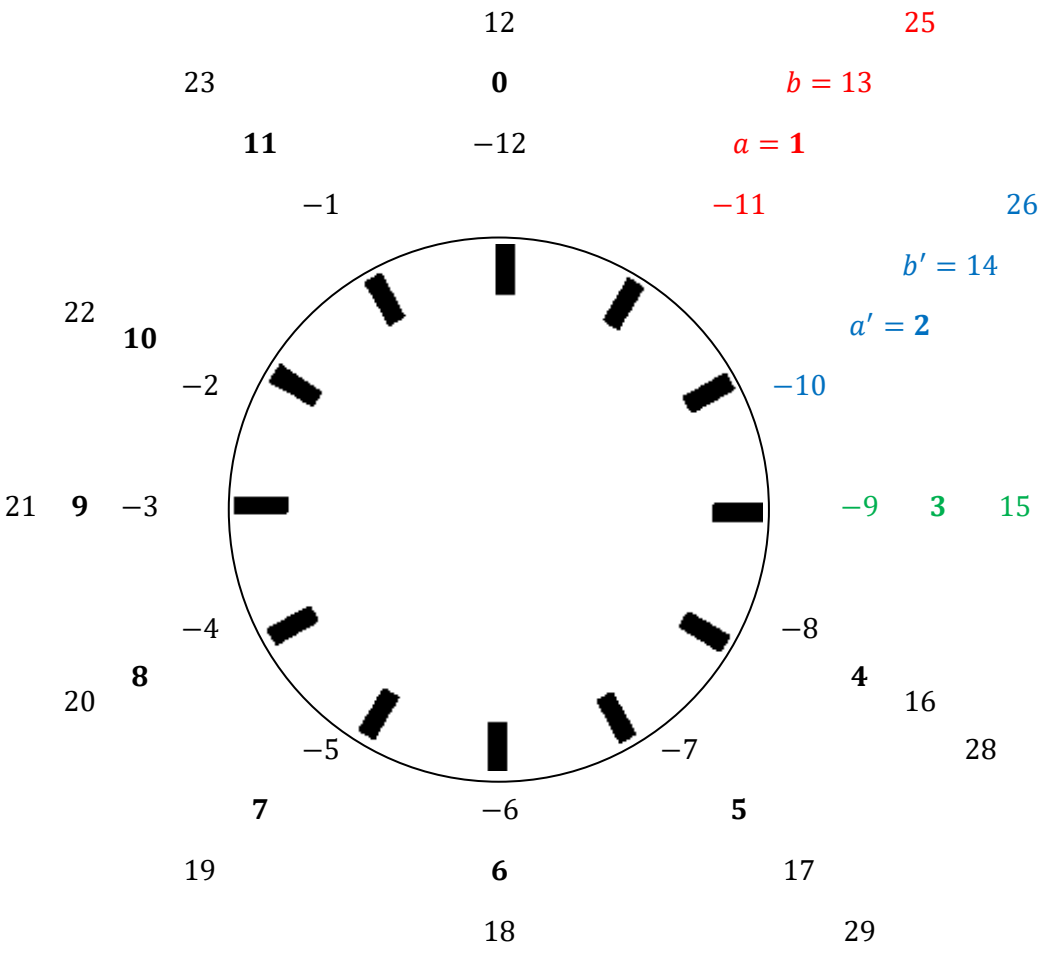


Illustration sur un cercle : Tous les entiers situés sur un même rayon sont congrus modulo 12.

Exemples :

$a=1\quad b=13\qquad 13-1=\mathbf{1}\times\mathbf{12}\qquad$ donc $\quad a\equiv b\ (12)$

$a'=2\quad b'=14\qquad 14-2=\mathbf{1}\times\mathbf{12}\qquad$ donc $\quad a'\equiv b'\ (12)$



$a\times a'=\mathbf{2}$ et $b\times b'=\mathbf{182}$

$182-2=180=\mathbf{15}\times\mathbf{12}$

$a\times a'\equiv b\times b'(12)$

En multipliant **membre à membre** ou en additionnant membre à membre les entiers de 2 congruences modulo c on obtient une congruence modulo c

$a+a'=\mathbf{3}$ et $b+b'=\mathbf{27}$

$27-3=24=\mathbf{2}\times\mathbf{12}$

$a+a'\equiv b+b'(12)$

$a'\times a'=\mathbf{4}$ **et** $b'\times b'=\mathbf{196}$

$196-4=192=\mathbf{16}\times\mathbf{12}$

$a'\times a'\equiv b'\times b'(12)$

$a'^2\equiv b'^2(12)$

⚠

$a\times b=\mathbf{13}$ et $a'\times b'=\mathbf{28}$	$28-13=15\neq \boldsymbol{k}\times\mathbf{12}$	$a\times b$ *et* $a'\times b'$ ne sont pas congrus modulo 12
$a+b=\mathbf{14}$ et $a'+b'=\mathbf{16}$	$16-14=2\neq \boldsymbol{k}\times\mathbf{12}$	$a+b$ *et* $a'+b'$ ne sont pas congrus modulo 12

5.2 Propriétés des congruences

5.2.1 Transitivité de la congruence

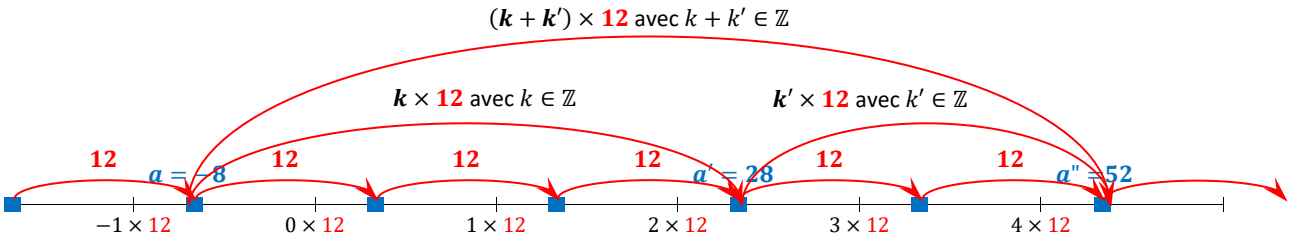
Soit $c \in \mathbb{N}^*$. Pour tous entiers relatifs $a, a' et\ a"$

Si $a \equiv a'(c)$ et si $a' \equiv a"(c)$ alors $a \equiv a"(c)$

Exemple : $-8 \equiv 28\ (12)$ car $28 - (-8) = \mathbf{3} \times \mathbf{12}$

$28 \equiv 52(12)$ car $52 - 28 = \mathbf{2} \times \mathbf{12}$

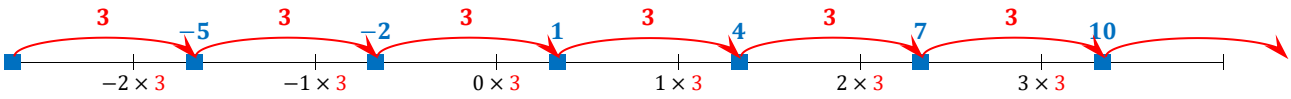
Donc, par transitivité, $-8 \equiv 52(12)$



Remarques :

- Soit $c \in \mathbb{N}^*$. Tout entier relatif a est congru à lui-même modulo c
  $\boldsymbol{a \equiv a\ (c)}$ car $a - a = \mathbf{0} \times c$
- $3842 \equiv 1992(10)$ car le reste dans la division par 10 de ces deux entiers naturels est 2
- Soit $c \in \mathbb{N}^*$. L'entier relatif a est un multiple de c équivaut à $\boldsymbol{a \equiv 0\ (c)}$
- Soit $c \in \mathbb{N}^*$ et $a \in \mathbb{Z}$.
  Si r est le reste de la division euclidienne de a par c alors $\boldsymbol{a \equiv r\ (c)}$
  ⚠" Si $\boldsymbol{a \equiv r\ (c)}$ alors r est le reste de la division euclidienne de a par c " **est fausse** (cette proposition réciproque est vraie seulement si $0 \leq r < c$).
- Les entiers relatifs a congrus à b modulo c s'écrivent $b + kc,\ \ k \in \mathbb{Z}$

Exemple : les entiers relatifs $\boldsymbol{a}$ congrus à 1 modulo 3 s'écrivent $\boldsymbol{1 + 3k},\ \ k \in \mathbb{Z}$



- Les entiers relatifs qui s'écrivent $1 + 2k,\ \ k \in \mathbb{Z}$ sont les entiers congrus à 1 modulo 2, c'est-à-dire les entiers impairs.
- Soit $c \in \mathbb{N}^*$. Pour tous couples $(a\ ;b)$ d'entiers relatifs, il est équivalent de dire :

∗ $a \equiv b\ \ (c)$
∗ c divise $a - b$
∗ Il existe un entier relatif k tel que $a - b = kc$
∗ Il existe un entier relatif k tel que $a = b + kc$

Exemple : les entiers relatifs $\boldsymbol{a}$ et $\boldsymbol{b}$ sont congrus modulo 12 ⇔ il existe $k \in \mathbb{Z}$ tel que $\boldsymbol{a = b + 12k}$

5.2.2 Compatibilité de la congruence avec l'addition membre à membre

Soit $c \in \mathbb{N}^*$. Pour tous couples $(a\,;b)$ et $(a'\,;b')$ d'entiers relatifs,

Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors $a + a' \equiv b + b'\ (c)$

Démonstration :

Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors il existe deux entiers relatifs k et k' tels que $a = b + kc$ et $a' = b' + k'c$

Donc en additionnant les deux égalités membre à membre :

$a + a' = b + b' + (k + k')c$

$k + k'$ est un entier relatif, donc $a + a' \equiv b + b'\ (c)$

Exemple :

$1 \equiv 13\ (12)$ et $2 \equiv 14\ (12)$ donc $1 + 2 \equiv 13 + 14\ (12)$ $\boxed{3 \equiv 27\ (12)}$

Cas particulier :

Soit $c \in \mathbb{N}^*$. Pour tous entiers relatifs a, b et a', si $a \equiv b\ (c)$ alors $a + a' \equiv b + a'\ (c)$

Exemple :

$1 \equiv 13\ (12)$ donc $1 + 1 \equiv 13 + 1\ (12)$ $\boxed{2 \equiv 14\ (12)}$

Ainsi, on peut additionner aux deux membres le même entier k dans les congruences.

5.2.3 Compatibilité de la congruence avec la soustraction membre à membre

Soit $c \in \mathbb{N}^*$. Pour tous couples $(a\,;b)$ et $(a'\,;b')$ d'entiers relatifs,

Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors $a - a' \equiv b - b'\ (c)$

Démonstration :

Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors il existe deux entiers relatifs k et k' tels que $a = b + kc$ et $a' = b' + k'c$

Donc en soustrayant les deux égalités membre à membre :

$a - a' = b - b' + (k - k')c$

$k - k'$ est un entier relatif, donc $a - a' \equiv b - b'\ (c)$

Exemple :

$1 \equiv 13\ (12)$ et $2 \equiv 14\ (12)$ donc $1 - 2 \equiv 13 - 14\ (12)$ $\boxed{-1 \equiv -1\ (12)}$

Cas particulier :

Soit $c \in \mathbb{N}^*$. Pour tous entiers relatifs a et b $a - b \equiv 0\ (c)$ équivaut à $a \equiv b\ (c)$

Démonstration :

Si $a - b \equiv 0\ (c)$ et comme $b \equiv b\ (c)$ alors $a - b + b \equiv 0 + b\ (c)$ c'est-à-dire $a \equiv b\ (c)$

Réciproquement, si $a \equiv b\ (c)$ et comme $b \equiv b\ (c)$ alors $a - b \equiv b - b\ (c)$ soit $a - b \equiv 0\ (c)$

Exemple :

$1 \equiv 13\ (12)$ équivaut à $\boxed{1 - 13 \equiv 0\ (12)}$

Ainsi, on peut « transposer » dans les congruences.

5.2.4 Compatibilité de la congruence avec la multiplication membre à membre

Soit $c \in \mathbb{N}^*$. Pour tous couples $(a\,;b)$ et $(a'\,;b')$ d'entiers relatifs,

Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors $aa' \equiv bb'\ (c)$

Démonstration :

Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors il existe deux entiers relatifs k et k' tels que $a = b + kc$ et $a' = b' + k'c$

Donc en multipliant les deux égalités membre à membre :

$aa' = (b + kc)(b' + k'c)$

$aa' = bb' + bk'c + kcb' + kk'c^2$

$aa' = bb' + (bk' + kb' + kk'c)c$

$bk' + kb' + kk'c$ est un entier relatif, donc $aa' \equiv bb'\ (c)$

Exemple :

$1 \equiv 13\ (12)$ et $2 \equiv 14\ (12)$ donc $1 \times 2 \equiv 13 \times 14\ (12)$ $\boxed{2 \equiv 182\ (12)}$

Cas particulier :

Soit $c \in \mathbb{N}^*$. Pour tous entiers relatifs a, b et a', si $a \equiv b\ (c)$ alors $aa' \equiv ba'\ (c)$

Démonstration :

On a vu que si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors $aa' \equiv bb'\ (c)$

Or pour tout entier relatif a', on sait que $a' \equiv a'\ (c)$

Donc : $aa' \equiv ba'\ (c)$

Exemples :

$1 \equiv 13\ (12)$ donc $1 \times -3 \equiv 13 \times -3\ (12)$ $\boxed{-3 \equiv -39\ (12)}$

$2 \equiv 14\ (12)$ donc $2k \equiv 14k\ (12)$ pour tout $k \in \mathbb{Z}$

Ainsi, on peut multiplier les deux membres par un même entier k dans les congruences.

Conséquence pour les combinaisons linéaires d'entiers congrus modulo c :

Soit $c \in \mathbb{N}^*$. Pour tous couples $(a\,;b)$ et $(a'\,;b')$ d'entiers relatifs, pour tous entiers relatifs $\boldsymbol{k}$ et $\boldsymbol{k'}$

Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors $\boldsymbol{k}a + \boldsymbol{k'}a' \equiv \boldsymbol{k}b + \boldsymbol{k'}b'\ (c)$

Exemples :

$1 \equiv 13\ (12)$ et $2 \equiv 14\ (12)$ donc $-\mathbf{3} \times 1 + \mathbf{5} \times 2 \equiv -\mathbf{3} \times 13 + \mathbf{5} \times 14\ (12)$

d'où $\boxed{7 \equiv 31\ (12)}$

$1 \equiv 13\ (12)$ et $2 \equiv 14\ (12)$ donc pour tous entiers $\boldsymbol{k}$ et $\boldsymbol{k'}$ $k + 2k' \equiv 13k + 14k'\ (12)$

⚠ La congruence ***n'est pas compatible avec la division membre à membre***

La proposition Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors $\frac{a}{a'} \equiv \frac{b}{b'}\ (c)$ **est fausse**.

Contre exemples :

La proposition $2 \equiv 14\ (12)$ donc $1 \equiv 7\ (12)$ est fausse.

La proposition $2a \equiv 2b\ (12)$ donc $a \equiv b\ (12)$ est fausse.

La proposition $2a \equiv 2b\ (c)$ donc $a \equiv b\ (c)$ est fausse.

Ainsi, on ne peut pas diviser les deux membres par un même entier k dans les congruences (sauf si on divise aussi le module c par k). Par exemple : $\boldsymbol{2x \equiv 4\ (6) \Leftrightarrow x \equiv 2(3)}$

5.2.5 Compatibilité de la congruence avec les puissances

Soit $c \in \mathbb{N}^*$. Pour tout couple $(a\,;b)$ d'entiers relatifs, et pour tout $\boldsymbol{n} \in \mathbb{N}^*$

Si $a \equiv b\ (c)$ alors $a^{\boldsymbol{n}} \equiv b^{\boldsymbol{n}}\ (c)$

Démonstration par récurrence :

Dans toute cette démonstration, on suppose que l'hypothèse $a \equiv b\ (c)$ est vraie.

- Initialisation :

Pour $n = 1$

$a^1 = a$ et $b^1 = b$

Si $a \equiv b\ (c)$ alors $a^1 \equiv b^1\ (c)$

D'où la proposition est vraie pour $n = 1$

- Hérédité :

On suppose que pour un certain entier naturel non nul k on ait :

$a^k \equiv b^k\ (c)$

Montrons *qu'alors* $a^{k+1} \equiv b^{k+1}\ (c)$

On a : $a^k \equiv b^k\ (c)$ (hypothèse de récurrence) et $a \equiv b\ (c)$ (hypothèse de départ)

D'après la compatibilité de la congruence avec la multiplication, on a :

$a^k \times a \equiv b^k \times b\ (c)$

$a^{k+1} \equiv b^{k+1}\ (c)$

D'où la proposition est héréditaire

- Conclusion :

Pour tous entiers relatifs a et b et pour tout entier naturel non nul n, si $a \equiv b\ (c)$ alors $a^n \equiv b^n\ (c)$

Exemple :

$2 \equiv 14\ (12)$ donc $2^2 \equiv 14^2\ (12)$ $\boxed{4 \equiv 196\ (12)}$

Conséquence pour les combinaisons linéaires de puissances d'entiers congrus modulo c :

Soit $c \in \mathbb{N}^*$. Pour tous couples $(a\,;b)$ et $(a'\,;b')$ d'entiers relatifs, pour tous entiers naturels non nuls n et n'

Si $a \equiv b\ (c)$ et si $a' \equiv b'\ (c)$ alors $ka^n + k'(a')^{n'} \equiv kb^n + k'(b')^{n'}\ (c)$

Exemples :

$1 \equiv 13\ (12)$ et $2 \equiv 14\ (12)$ donc $-3 \times 1^2 + 5 \times 2^3 \equiv -3 \times 13^2 + 5 \times 14^3\ (12)$

d'où $37 \equiv 13213\ (12)$

⚠ La congruence ***n'est pas compatible avec les racines***

La proposition Si $a^2 \equiv b^2\ (c)$ alors $a \equiv b\ (c)$ **est fausse**.

Contre exemple :

La proposition " $1 \equiv 49\ (12)$ donc $1 \equiv 7\ (12)$ " est fausse.

5.3 Applications des congruences

Exemple 1 :

Montrer que pour tout $n \in \mathbb{N}^*$ l'entier $5^{6n+1} + 2^{3n+1}$ est un multiple de 7

Réponse : On transforme la question de façon à utiliser les congruences :

$5^{6n+1} + 2^{3n+1}$ est un multiple de 7 équivaut à $5^{6n+1} + 2^{3n+1} \equiv 0 \ (7)$

On fait apparaitre une combinaison linéaire du type $ka^n + k'(a')^{n'}$

$$5^{6n+1} + 2^{3n+1} = 5 \times 5^{6n} + 2 \times 2^{3n}$$

Or, $5^6 = 2232 \times 7 + 1$ donc $5^6 \equiv \mathbf{1} \ (7)$ et $2^3 = 1 \times 7 + 1$ donc $2^3 \equiv \mathbf{1} \ (7)$

Donc pour tout $n \in \mathbb{N}^*$, $(5^6)^n \equiv 1^n \ (7)$ c'est-à-dire $5^{6n} \equiv 1 \ (7)$

et $(2^3)^n \equiv 1^n \ (7)$ c'est-à-dire $2^{3n} \equiv 1 \ (7)$

Par compatibilité de la relation de congruence avec la multiplication :

$5 \times 5^{6n} \equiv 5 \times 1 \ (7)$ et $2 \times 2^{3n} \equiv 2 \times 1 \ (7)$ d'où $5^{6n+1} \equiv 5 \ (7)$ et $2^{3n+1} \equiv 2 \ (7)$

Par compatibilité de la relation de congruence avec l'addition :

$5^{6n+1} + 2^{3n+1} \equiv 7 \ (7)$ soit encore $5^{6n+1} + 2^{3n+1} \equiv 0 \ (7)$

Exemple 2 :

Montrer que pour tout $n \in \mathbb{N}$ l'entier $n(n+1)(2n+1)$ est un multiple de 6

Réponse : On transforme la question de façon à utiliser la compatibilité de la congruence avec la multiplication. Le reste de la division de n par 6 peut être 0, 1, 2, 3, 4, 5. Etudions les 6 cas :

- Premier cas : Le reste de la division de n par 6 est 0 c'est-à-dire $n \equiv \mathbf{0} \ (6)$

Par compatibilité de la congruence avec l'addition, on a : $n + 1 \equiv \mathbf{1} \ (6)$

Par compatibilité de la congruence avec la multiplication, on a : $2n \equiv 0 \ (6)$ donc : $2n + 1 \equiv \mathbf{1} \ (6)$

Finalement : $n(n+1)(2n+1) \equiv \mathbf{0} \times \mathbf{1} \times \mathbf{1} (6)$ soit $n(n+1)(2n+1) \equiv \mathbf{0}(6)$

On en déduit que dans le cas où $n \equiv \mathbf{0} \ (6)$ $n(n+1)(2n+1)$ est un multiple de 6

- On procède de même pour les autres cas, en simplifiant si possible.

Par exemple $2n \equiv 8 \ (6)$ équivaut à $2n \equiv 2 \ (6)$ car $8 \equiv 2 \ (6)$

- Les 6 cas sont résumés dans le tableau suivant :

n	$n+1$		$2n+1$	
$n \equiv \mathbf{0} \ (6)$	$n+1 \equiv \mathbf{1} \ (6)$	$2n \equiv 0 \ (6)$	$2n+1 \equiv \mathbf{1} \ (6)$	$n(n+1)(2n+1) \equiv \mathbf{0}(6)$
$n \equiv \mathbf{1} \ (6)$	$n+1 \equiv \mathbf{2} \ (6)$	$2n \equiv 2 \ (6)$	$2n+1 \equiv \mathbf{3} \ (6)$	$n(n+1)(2n+1) \equiv 6 \equiv \mathbf{0}(6)$
$n \equiv \mathbf{2} \ (6)$	$n+1 \equiv \mathbf{3} \ (6)$	$2n \equiv 4 \ (6)$	$2n+1 \equiv \mathbf{5} \ (6)$	$n(n+1)(2n+1) \equiv 30 \equiv \mathbf{0}(6)$
$n \equiv \mathbf{3} \ (6)$	$n+1 \equiv \mathbf{4} \ (6)$	$2n \equiv 6 \equiv 0 \ (6)$	$2n+1 \equiv \mathbf{1} \ (6)$	$n(n+1)(2n+1) \equiv 12 \equiv \mathbf{0}(6)$
$n \equiv \mathbf{4} \ (6)$	$n+1 \equiv \mathbf{5} \ (6)$	$2n \equiv 8 \equiv 2 \ (6)$	$2n+1 \equiv \mathbf{3} \ (6)$	$n(n+1)(2n+1) \equiv 60 \equiv \mathbf{0}(6)$
$n \equiv \mathbf{5} \ (6)$	$n+1 \equiv 6 \equiv \mathbf{0} \ (6)$	$2n \equiv 10 \equiv 4 \ (6)$	$2n+1 \equiv \mathbf{5} \ (6)$	$n(n+1)(2n+1) \equiv \mathbf{0}(6)$

Dans tous les cas, on obtient $n(n+1)(2n+1) \equiv \mathbf{0}(6)$

Conclusion : pour tout $n \in \mathbb{N}$, $n(n+1)(2n+1)$ est un multiple de 6

On a étudié tous les cas possibles. C'est la méthode de ***disjonction des cas***. On dit aussi que c'est la méthode ***exhaustive***.

Exemple 3 :

Quel est le reste de la division de 352^{14546} par 5 ?

Réponse :

- On commence par transformer la question de façon à utiliser la congruence modulo 5 avec un nombre plus petit que 352 :

$$\frac{352}{5} = 70{,}4$$
$$352 = 70 \times 5 + 2$$

d'où $352 \equiv 2 \ (5)$

et donc, $352^{14546} \equiv 2^{14546} \ (5)$

- On cherche ensuite une puissance de 2 qui soit congrue à **1** modulo 5

(cela permet d'utiliser la propriété $1^n = 1 \ pour \ tout \ n \in \mathbb{N}$)

$2^1 = 2$	$2^1 = 0 \times 5 + \mathbf{2}$	$2^1 \equiv \mathbf{2} \ (5)$
$2^2 = 4$	$2^2 = 0 \times 5 + \mathbf{4}$	$2^2 \equiv \mathbf{4} \ (5)$
$2^3 = 8$	$2^3 = 1 \times 5 + \mathbf{3}$	$2^3 \equiv \mathbf{3} \ (5)$
$2^4 = 16$	$2^4 = 3 \times 5 + \mathbf{1}$	$2^4 \equiv \mathbf{1} \ (5)$

Après quelques essais, on trouve $2^4 = 16$

$$2^4 \equiv 1 \ (5)$$

On fait apparaitre **4** dans l'exposant on a $14546 = 4 \times 3636 + 2$

$$2^{14546} = 2^{4 \times 3636 + 2}$$
$$2^{14546} = (2^4)^{3636} \times 2^2$$

d'où $2^4 \equiv 1 \ (5)$

$(2^4)^{3636} \equiv 1^{3636} \ (5)$

$(2^4)^{3636} \equiv 1 \ (5)$

$$(2^4)^{3636} \times 2^2 \equiv 1 \times 2^2 \ (5)$$
$$2^{14546} \equiv 4 \ (5)$$

et donc, $352^{14546} \equiv 4 \ (5)$

Conclusion : le reste de la division de 352^{14546} par 5 est **4**.

Une variante de cette méthode consiste à chercher une puissance qui soit congrue à **-1**

(On utilise la propriété $(-1)^n = 1 \ pour \ tout \ n \in \mathbb{N} \ pair \ et \ (-1)^n = -1 \ pour \ tout \ n \in \mathbb{N} \ impair$)

Exemple 4 :

Quel est le reste de la division par 5 de 4^{2003} ?

$4^1 = 4$	$4^1 = 0 \times 5 + \mathbf{4}$	$4^1 \equiv \mathbf{4} \ (5)$
Ou encore	$4^1 = 1 \times 5 - \mathbf{1}$	$4^1 \equiv -\mathbf{1} \ (5)$

d'où $4^1 \equiv -1 \ (5)$

$4^{2003} \equiv (-1)^{2003} \ (5)$ 2003 est impair donc $(-1)^{2003} = -1$

$4^{2003} \equiv -1 \ (5)$

Donc on a $4^{2003} \equiv 4 \ (5)$ avec $0 \leq 4 < 5$ d'où le reste de la division par 5 de 4^{2003} est **4**.

Exemple 5 :

Les propositions suivantes sont-elles vraies ?

1.

Soit $m \in \mathbb{N}^*$. Pour tous entiers relatifs a, b, c et pour tout entier relatif d tel que $b \equiv d \ \ (m)$, $a \times b \equiv c \ \ (m) \quad \Leftrightarrow \quad a \times d \equiv c \ \ (m)$

2.

Soit $m \in \mathbb{N}^*$. Pour tous entiers relatifs a, b, c et pour tout entier relatif d tel que $b \equiv d \ \ (m)$, $a + b \equiv c \ \ (m) \quad \Leftrightarrow \quad a + d \equiv c \ \ (m)$

Réponse :

Proposition 1 :

On a $b \equiv d \ \ (m)$

Par compatibilité de la congruence avec la multiplication, on a $a \times b \equiv a \times d \ \ (m)$

Et par transitivité de la congruence :

Si $\begin{cases} a \times b \equiv c \ \ (m) \\ a \times b \equiv a \times d \ \ (m) \end{cases}$ alors $a \times d \equiv c \ \ (m)$ et Si $\begin{cases} a \times d \equiv c \ \ (m) \\ a \times b \equiv a \times d \ \ (m) \end{cases}$ alors $a \times b \equiv c \ \ (m)$

Conclusion : La proposition 1 est vraie

Proposition 2 :

On a $b \equiv d \ \ (m)$

Par compatibilité de la congruence avec l'addition, on a $a + b \equiv a + d \ \ (m)$

Et par transitivité de la congruence :

Si $\begin{cases} a + b \equiv c \ \ (m) \\ a + b \equiv a + d \ \ (m) \end{cases}$ alors $a + d \equiv c \ \ (m)$ et Si $\begin{cases} a + d \equiv c \ \ (m) \\ a + b \equiv a + d \ \ (m) \end{cases}$ alors $a + b \equiv c \ \ (m)$

Conclusion : La proposition 2 est vraie

Conséquence :

Dans une combinaison linéaire, on peut remplacer un ou plusieurs des termes ou facteurs par un autre qui lui soit congru. On obtient une relation de congruence équivalente.

Application numérique :

- $125a + 25b \equiv 3 \ \ (13)$

équivaut successivement à :

- $8a + 12b \equiv 3 \ \ (13)$ car $125 \equiv 8 \ \ (13)$ et $25 \equiv 12 \ \ (13)$
- $8a - b \equiv 3 \ \ (13)$ car $12 \equiv -1 \ \ (13)$
- $8a \equiv 3 + b \ \ (13)$

⚠ Dire « pour tout $n \in \mathbb{N}^*$, $a^n \equiv 1 \ \ (5)$ ***équivaut à*** $a \equiv 1 \ \ (5)$ » **est faux**

car a^n et a ne sont pas congrus modulo 5 pour tout $n \in \mathbb{N}^*$

(Mais par compatibilité de la congruence avec les puissances « pour tout $n \in \mathbb{N}^*$, ***si*** $a \equiv 1 \ \ (5)$ ***alors*** $a^n \equiv 1 \ \ (5)$ » est vrai)

Exemple 6 : Diverses manipulations sur les congruences

Congru à 0 Soit $d \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ $d \mid a$ se lit « d divise a » et s'écrit avec les congruences : $a \equiv 0 \quad (d)$ ***Dans une congruence, a est congru à 0 modulo d, si et seulement d divise a***	*Exemple 1 :* $12 \mid 24$ (12 divise 24) s'écrit avec les congruences : $24 \equiv 0 \quad (12)$ *Exemple 2 :* Pour tout $d \in \mathbb{N}^*$ et pour tout $k \in \mathbb{Z}$ on a $d \mid kd$ Ce qui s'écrit avec les congruences : $kd \equiv 0 \quad (d)$
Utilisation de la* compatibilité *avec l'addition de* 0** Pour tout $d \in \mathbb{N}^*$ et pour tout $k \in \mathbb{Z}$ on a $kd \equiv 0 \quad (d)$ Donc $a \equiv b \quad (d)$ Equivaut successivement à $a \equiv b + 0 \quad (d)$ $a \equiv b + kd \quad (d)$ ***Dans une congruence, on peut ajouter à l'un des membres, un multiple du module	*Exemple :* Pour tout $k \in \mathbb{Z}$ $12k$ est un multiple de 12 $0 \equiv 12k \quad (12)$ Donc par exemple $a \equiv 5 \quad (12)$ Equivaut à $a \equiv 5 + 12k \quad (12)$
Utilisation de la* compatibilité *avec la multiplication par* 1** Pour tout $d \in \mathbb{N}^*$ et pour tout $k \in \mathbb{Z}$ on a $kd \equiv 0 \quad (d)$ $kd + 1 \equiv 1 \quad (d)$ Donc : $a \equiv b \quad (d)$ Equivaut successivement à $a \equiv b \times 1 \quad (d)$ $a \equiv b(kd + 1) \quad (d)$ ***Dans une congruence, on peut multiplier l'un des membres, par un nombre congru à 1	*Exemple :* Pour tout $k \in \mathbb{Z}$ $12k \equiv 0 \quad (12)$ $12k + 1 \equiv 1 \quad (12)$ Donc par exemple $a \equiv 5 \quad (12)$ Equivaut à $a \equiv 5(12k + 1) \quad (12)$
Déduction d'une congruence modulo un diviseur du module Pour tous naturels non nuls n et p et pour tous entiers relatifs a et b : ***Si*** $a \equiv b \quad (np)$ ***alors*** $a \equiv b \quad (n)$ ⚠ La réciproque est *fausse* *Exemples :* Comme $5 \equiv 17 \quad (12)$ et 12 a comme diviseurs 2 ; 3 ; 4 ; 6 Alors : $5 \equiv 17 \quad (2)$; $5 \equiv 17 \quad (3)$; $5 \equiv 17 \quad (4)$; $5 \equiv 17 \quad (6)$	*Preuve :* $a \equiv b \quad (np)$ Equivaut à : $a - b \equiv 0 \quad (np)$ np divise $a - b$ Il existe $k \in \mathbb{Z}$ tel que $a - b = knp$ *Donc* Il existe $k' \in \mathbb{Z}$ tel que $a - b = k'n$ n divise $a - b$ $a - b \equiv 0 \quad (n)$ $a \equiv b \quad (n)$
Congruence modulo 2 * $a \equiv b \quad (2)$ équivaut successivement à * Il existe $k \in \mathbb{Z}$ tel que $a = b + 2k$ * ***a et b ont la même parité***	*Exemple :* Pour tous entiers x *et* y *:* $2y \equiv 0 \quad (2) \quad \Leftrightarrow \quad y \equiv -y \quad (2)$ d'où $x + y \equiv x - y \quad (2)$ $x + y$ et $x - y$ ont la même parité