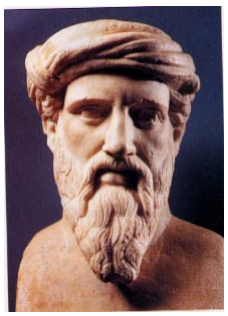
Multiples et diviseurs dans $\mathbb{Z}$

Ce chapitre est le premier des chapitres d'Arithmétique de **4emmeMATH**. Le mot *arithmétique* vient du grec ἀριθμός [arithmos] qui signifie *nombre* (sous-entendu entier). Pythagore a fondé toute sa théorie et toute son Ecole sur l'idée que les nombres entiers (et leurs rapports : les fractions) expliquaient l'univers (κόσμος [kosmos]).



Pendant de nombreux siècles l'Arithmétique a été très étudiée par les mathématiciens du monde entier (chinois, arabes, indiens, ...) Elle était aimée car nécessitait souvent de grandes astuces pour la résolution de ses problèmes. Elle concernait exclusivement les nombres entiers : les problèmes dont les solutions étaient des nombres entiers ont été appelés *problèmes diophantiens* en l'honneur du grec Diophante d'Alexandrie (IIe siècle ap. J.-C.)

Il existe à ce jour de célèbres problèmes diophantiens toujours non démontrés comme la célèbre conjecture de Goldbach : *tout entier pair supérieur ou égal à 4 est somme de deux nombres premiers.* Pourtant une somme d'un million de dollars est prévue pour le mathématicien qui démontrera cette ancienne conjecture (elle date du XVIIIe siècle).

Au XVIIe siècle, un juriste, mais mathématicien de passion, Pierre DE FERMAT énonça un problème diophantien qui restera célèbre :

*Si n est un entier supérieur ou égal à 3, l'équation $x^n + y^n = z^n$ n'a pas de solution entière non nulle (*i.e. *telle que $xyz = 0$).*

Si l'un des entiers est nul, par exemple y il est évident qu'il y a des solutions : par exemple $(3, 0, 3)$ etc. il est donc nécessaire d'écarter ces solutions triviales. Si $n = 2$ on sait depuis longtemps qu'il y a des solutions (non triviales) : $3^2 + 4^2 = 5^2$ marche par exemple (cela fait penser au théorème de Pythagore n'est-ce pas ?). Pour narguer ces lecteurs, Fermat écrit dans la marge de son cahier : *j'ai trouvée une preuve merveilleuse de ce fait, mais la marge est trop petite pour la contenir*. Nul doute que Fermat se trompait, car il fallut attendre 1994 pour qu'un mathématicien britanique, Andrew WILES, démontre ce théorème de façon spectaculaire (une démonstration de 800 pages d'un théorème qui une fois démontré impliquait une chaîne de résultats aboutissant finalement au théorème de Fermat). Wiles devient immédiatement mondialement connu pour avoir vaincu une conjecture de 300 ans.


Les mathématiciens tels que Wiles étudient des Arithmétiques très sophistiquées, sur d'autres ensembles de nombres que ceux que l'on connaît. En Terminale nous étudions seulement l'Arithmétique de $\mathbb{Z}$, et peut-être un peu celle des polynômes réels.

On rappelle que l'on note $\mathbb{Z}$ l'ensemble des *entiers relatifs*, *i.e.* des entiers positifs et négatifs :

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

L'ensemble des entiers naturels (*i.e.* positifs) se note quant à lui : $\mathbb{N}$. Dans cet ensemble $\mathbb{Z}$ existent deux opérations (ou *lois internes*) importantes : $+$ et $\times$. Rappelons leurs propriétés :

1. La loi $+$ est *associative* : $\forall x, y, z \in \mathbb{Z}\ (x + y) + z = x + (y + z)$,
2. La loi $+$ possède un *élément neutre* noté 0 : $\forall x \in \mathbb{Z}\ x + 0 = 0 + x = x$,
3. Chaque $x \in \mathbb{Z}$ possède un *élément symétrique* pour $+$ (appelé *opposé*) que l'on note $-x$: $\forall x \in Z\ x + (-x) = (-x) + x = 0$,

4. La loi + est *commutative* : $\forall x, y \in \mathbb{Z}\ x + y = y + x$,
5. La loi $\times$ est *associtative* : $\forall x, y, z \in \mathbb{Z}\ (x \times y) \times z = x \times (y \times z)$,
6. La loi + possède un *élément neutre* noté 1 : $\forall x \in \mathbb{Z}\ x \times 1 = 1 \times x = x$,
7. La loi $\times$ est *distributive* à gauche et à droite par rapport à la loi + : $\forall x, y, z \in \mathbb{Z}\ x \times (y+z) = (x \times y) + (x \times z)$ et $(y+z) \times x = (y \times x) + (z \times x)$,
8. La loi $\times$ est *commutative* : $\forall x, y \in \mathbb{Z}\ x \times y = y \times x$.

On résume toutes ces propriétés élémentaires et connues depuis l'Ecole Primaire en disant que le triplet $(\mathbb{Z}, +, \times)$ est un *anneau*. Comme la deuxième loi $(\times)$ est commutative on dit même que $(\mathbb{Z}, +, \times)$ est un *anneau commutatif*.

On remarquera que $(\mathbb{N}, +, \times)$ n'est pas un anneau (pourquoi ?). C'est pour cela qu'en Arithmétique nous étudions plutôt $\mathbb{Z}$ que $\mathbb{N}$. On peut résumer (de façon réductrice) l'Arithmétique en disant que c'est l'étude de la relation de divisibilité dans un anneau (cf. section suivante). Notre anneau cette année sera $\mathbb{Z}$.

1 La relation de divisibilité dans $\mathbb{Z}$

Il est important de bien maîtriser la définition qui va suivre. Ceci est fondamental pour le reste du cours d'Arithmétique.

Définition 1.1 *Soit a et b deux entiers relatifs. On dit que a est un* multiple *de b s'il existe $k \in \mathbb{Z}$ tel que $a = bk$. On dit alors, à l'inverse, que b est un* diviseur *de a ou encore que b* divise *a (ou bien encore que a est* divisible *par a). On note cela :*

$$b|a$$

qui se lit «b divise a»

Exemples.

- 63 est un multiple de 7 car $63 = 7k$ avec $k = 9$. Ainsi $7|63$.
- 20 est un multiple de -5 car $20 = -5k$ avec $k = -4$. Ainsi $-5|20$.
- -35 est un multiple de -5 car $-35 = -5k$ avec $k = 7$. Ainsi $-5|-35$.
- 11 est un diviseur de 33 puisque 3
  $3 = 11k$ avec $k = 3$. Ainsi $11|33$.
- 0 est un multiple de 11 car $0 = 11k$ avec $k = 0$. Ainsi $11|0$
- 11 n'est pas un multiple de 0 car sinon il existerait un k tel que $11 = 0 \times k$ ce qui donnerait $11 = 0$ (absurde).

– 0 est un multiple de 0 car $0 = 0 \times k$ avec $k = \ldots$ ce que veut ! A l'inverse, 0 divise donc 0 (eh oui !) : $0|0$.

Le dernier exemple montre qu'il ne faut pas confondre la relation de divisibilité $|$ et l'opération de division $/$: la divisibilité est une relation : $a|b$ est une affirmation mathématique qui peut être vraie ou fausse. En revanche la division est une opération : a/b est un nombre. Les élèves de secondes savent tous bien que

$$b|a \Longleftrightarrow a/b \in \mathbb{Z}$$

mais cela n'est valable seulement quand b n'est pas nul ; en effet, $0|0$ pourtant l'opération «$0/0$» n'a pas de sens.

Notations. On notera :

$$n\mathbb{Z}$$

l'ensemble des multiples de l'entier n. Ainsi, par exemple, $2\mathbb{Z}$ est l'ensemble des nombres multiples de 2 autrement dit des *nombres pairs*. Cette notation s'explique car :

$$n\mathbb{Z} = \{nk \ ; \ k \in \mathbb{Z}\}$$

Par exemple $3\mathbb{Z}$ est l'ensemble des nombres s'écrivant $3k$ où k est un entier relatif quelconque. On a bien sûr $0\mathbb{Z} = \{0\}$, mais à part ce cas, si $n \neq 0$ l'ensemble $n\mathbb{Z}$ possède une infinité d'éléments.

On notera aussi :

$$\mathscr{D}(n)$$

l'ensemble des diviseurs de l'entier n. Par exemple

$$\mathscr{D}(6) = \{1; 2; 3; 6; -1; -2; -3; -6\}$$

Il ne faut pas oublier les entiers négatifs ! Remarquons que 0 possède tous les entiers comme diviseurs : $\mathscr{D}(0) = \mathbb{Z}$ mais à part ce cas, quel que soit l'entier relatif non nul $n \in \mathbb{Z}^*$, l'ensemble $\mathscr{D}(n)$ est toujours un ensemble fini puisque ses éléments sont tous compris entre $-|n|$ et $|n|$. On peut aussi remarquer que $\mathscr{D}(n) = \mathscr{D}(-n)$ quel que soit $n \in \mathbb{Z}$.

Remarquons donc, mais ceci n'est qu'un jeu de définitions et de notations que si a, b sont des entiers relatifs on a :

$$a \in b\mathbb{Z} \Longleftrightarrow b \in \mathscr{D}(a) \Longleftrightarrow b|a$$

Etablissons maintenant les propriétés élémentaires de la relation $|$.

Propriété 1 (Réfléxivité). Quel que soit $n \in \mathbb{Z}$: $n|n$.

Ainsi n se divise lui-même et est son propre multiple, ce qui peut s'écrire aussi bien $n \in \mathscr{D}(n)$ ou $n \in n\mathbb{Z}$. C'est évident.

Propriété 2. Soit a et b deux entiers relatifs. Si $a|b$ et $b|a$ alors $a = b$ ou $a = -b$.

Preuve. Si jamais $a = 0$ alors le fait que $a|b$ entraîne que $b = 0$ car le seul multiple de 0 est 0 et on a bien $a = b$.

Sinon $a \neq 0$. On a $a|b$ donc $b = ka$ avec $k \in \mathbb{Z}$. Si maintenant $b|a$ c'est que $a = k'b$ avec $k' \in \mathbb{Z}$. On a donc $a = k'b = kk'a$. Comme $a \neq 0$ on peut simplifier par a et on a : $kk' = 1$. Comme k et k' sont des entiers on a forcément $k, k' \in \{-1; 1\}$ ce qui termine la preuve. □

Propriété 3 (transitivité). Soit a, b et c trois entiers relatifs. Si $a|b$ et $b|c$ alors $a|c$.

Preuve. Les hypothèses s'écrivent $b = ka$ et $c = k'b$ avec $k, k' \in \mathbb{Z}$. On a donc $c = k'ka$ et comme $kk' \in \mathbb{Z}$ on a $a|c$. □

Propriété 4. Soit a, b et c trois entiers relatifs. Si c divise à la fois a et b alors c divise aussi : $a + b$, $a - b$, et plus généralement c divise tout entier de la forme $am + bn$ où $m, n \in \mathbb{Z}$.

Preuve. En effet, par hypothèse on a $a = kc$ et $b = k'c$ avec $k, k' \in /Z$. On a donc :

$$am + bn = kcm + k'cn = (km + k'n)c = Kc$$

avec $K \in \mathbb{Z}$. Donc $am + bn$ est un multiple de c. □

Remarque. Un entier de la forme $am+bn$ s'appelle une *combinaison linéaire entière* de a et de b.

Exercice 1. Trouver tous les entiers relatifs n pour lesquels la fraction

$$\frac{n + 17}{n + 4}$$

est entière.

Exercice 2. Déterminer des entiers naturels a et b tels que $a^2 - 4b^2 = 20$.

2 Division euclidienne dans $\mathbb{N}$ et dans $\mathbb{Z}$

Rappelons que faire une division euclidienne c'est répondre aux problèmes dont le type est le suivant :

Si j'ai 23 allumettes et que je désire faire des paquets de 6, combien de paquets vais-je obtenir ? combien d'allumettes va-t-il me rester alors ?

On dit qu'on a effectué une *division euclidienne* de 23 par 6. Le nombre de paquets s'appellera le *quotient* et le nombre d'allumettes restantes s'appellera le *reste* de la division euclidienne de 23 par 6. Pour les connaître on procède comme à l'Ecole Primaire et on trouve facilement que :

$$23 = 6 \times 3 + 5$$

Ainsi on formera 3 paquets de 6 allumettes et il restera 5 allumettes.

Plus généralement :

Théorème (Division euclidienne dans $\mathbb{N}$). Soit a et b deux entiers naturels avec $b \neq 0$. Il existe un unique couple (q, r) d'entiers naturels tels que :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b$$

L'entier a s'appelle le *dividende*, l'entier b s'appelle le *diviseur*. L'entier q s'appelle le *quotient* et l'entier r s'appelle le *reste* de la division euclidienne de a par b.

Remarque 1. Le reste r ne peut en aucun cas être supérieur ou égal au diviseur (sinon c'est qu'on peut faire un autre paquet). En revanche, r peut très bien être nul.

Remarque 2. Une division euclidienne permet d'encadrer a entre deux multiples consécutifs de b :

$$bq \leqslant a < b(q+1)$$

(ceci parce que $r < b$) et donc, en divisant par b on s'aperçoit que q est la partie entière[1] de $\frac{a}{b}$.

[1] On rappelle que pour chaque réel x il existe un entier relatif unique $n \in \mathbb{Z}$ tel que $n \leqslant x < n+1$: cet entier s'appelle *la partie entière* de x et se note $E(x)$. Par exemple $E(2.3) = 2$, $E(\pi) = 3$, $E(1) = 1$, $E(-3) = -3$ et $E(-2.4) = -3$.

Ce théorème si souvent utilisé depuis l'enfance n'a jamais été démontré. Il est temps de le faire (mais cela n'est pas exigible au Baccalauréat).

Preuve. On remarque que dans les conclusions du théorème il y a en fait deux résultats : une existence et une unicité. Nous allons démontrer l'une puis l'autre.

Démontrons l'existence du couple (q, r). Si $a < b$ on le couple $(q, r) = (0, a)$ convient (il n'y a pas assez d'allumettes pour faire un paquet). Sinon supposons que $a \geqslant b$. Puisque $b \neq 0$ les multiples de b (0, b, $2b$, $3b$, ...) forme une suite strictement croissante : il existe donc un multiple de b qui va dépasser[2] a : notons alors Qb le plus petit des multiples de b qui dépassent (strictement) a. Le multiple précédent, $(Q-1)b$ est donc inférieur ou égal à a on a donc :

$$(Q-1)b \leqslant a < Qb$$

Il suffit alors de prendre $q = Q - 1$. On est sûr que $q \geqslant 0$ car $a \geqslant b$ par hypothèse. Pour le reste il suffit de poser $r = a - bq$. D'après la double inégalité $qb \leqslant a < (q+1)b$ on a bien $0 \leqslant r < b$ (en retranchant bq de chaque côté).

Démontrons l'unicité du couple (q, r). Imaginons qu'il y en ait un autre qui conviennent *i.e.* supposons que :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases} \quad \text{et} \quad \begin{cases} a = bq' + r' \\ 0 \leqslant r' < b \end{cases}$$

Il s'agit alors de montrer que $q = q'$ et que $r = r'$. En effet on a en soustrayant les égalités ci-dessus :

$$0 = b(q - q') + (r - r')$$

ce qui s'écrit encore $r - r' = b(q' - q)$. Or $0 \leqslant r' < b$ donc $-b < -r' \leqslant 0$ et puisque $0 \leqslant r < b$, on a en ajoutant (on peut toujours ajouter deux inégalités, c'est soustraire qu'on ne peut pas) :

$$-b < r - r' < b$$

Mais on vient de voir que $r - r' = b(q' - q)$: c'est donc un multiple de b qui est strictement compris entre $-b$ et b : ce ne peut être que 0. Ainsi $r = r'$. Mais alors l'égalité $r - r' = b(q' - q)$ devient $b(q' - q) = 0$ et comme $b \neq 0$ il vient $q - q'$. □

PIEGE ! Une écriture de la forme $a = bq + r$ n'est pas forcément une division euclidienne de a par b. Par exemple $25 = 3 \times 5 + 10$ pourtant 10 n'est inférieur ni 3, ni à 5, donc ce n'est pas une division euclidienne. La D.E. de 25 par 5 est $25 = 5 \times 5 + 0$ et la D.E. de 25 par 3 est $25 = 3 \times 8 + 1$.

On peut étendre sans difficulté la division euclidienne à tous les entiers relatifs, en rajoutant une condition sur le reste. $\mathbb{Z}$ est donc un anneau dans

[2]En mathématiques cette propriété importante se traduit en disant que $\mathbb{Z}$, muni de son ordre $\leqslant$, est un anneau *archimédien*

lequel une division euclidienne est possible : un tel anneau s'appelle un *anneau euclidien*.

Théorème (Division euclidienne dans $\mathbb{Z}$). Soit a et b deux entiers relatifs avec $b \neq 0$. Il existe un unique couple (q, r) d'entiers relatifs tels que :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < |b|$$

Bien observer la différence avec la division euclidienne dans $\mathbb{N}$: le reste, contrairement au quotient est toujours positif ! Faisons quelques exemples avant de démontrer ce théorème.

Exemple 1. Division euclidienne de -31 par 7. On fait la D.E. de 31 par 7 : $31 = 7 \times 4 + 3$ donc $-31 = 7 \times (-4) - 3$. Malheureusement le «reste» n'est pas positif : on procède alors à l'astuce suivante :

$$-31 = 7 \times (-4) - 3 = 7 \times (-4) - 3 + 7 - 7 = 7 \times (-5) + 4$$

et on a bien le reste comme il faut.

Exemple 2. Division euclidienne de 23 par -5. On fait la D.E. de 23 par 5 : $23 = 5 \times 4 + 3$ donc $23 = (-5) \times (-4) + 3$ et on a bien $0 \leqslant 3 < |-5|$.

Exemple 3. Division euclidienne de -41 par -11. On fait la D.E. de 41 par 11 : $41 = 11 \times 3 + 8$ donc $-41 = (-11) \times 3 - 8$. On recommence l'astuce de l'exemple 1 pour obtenir un reste positif :

$$-41 = (-11) \times 3 - 8 = (-11) \times 3 - 8 + 11 - 11 = (-11) \times 4 + 3$$

et le reste vérifie bien $0 \leqslant 3 < |-11|$.

Faites la preuve en exercice en vous inspirant de ces trois exemples.

Lien entre la division euclidienne et la divisibilité. Il est évident, mais il faut toujours avoir en tête que :

Si $b \neq 0$, b divise a si et seulement si le reste de la D.E. de a par b est nul.

En effet on a alors $a = bq + 0 = bq$ et on donc a est un multiple de b.

On se servira de ce fait dans la section importante suivante, qui parle des congruences.

3 La relation de congruence modulo un entier

On a déjà rencontré les congruences en 1ère S en Trigonométrie pour dire que deux angles sont congrus modulo 2π. Par exemple $\frac{\pi}{2}$ et $\frac{-3\pi}{2}$ sont congrus modulo 2π car $\frac{\pi}{2} = \frac{-3\pi}{2} + 2\pi$ On note alors cela $\frac{\pi}{2} \equiv \frac{-3\pi}{2}$ $[2\pi]$. Cela signifie concrètement que l'on a fait un tour de cercle (2π) pour passer de $\frac{-3\pi}{2}$ à $\frac{\pi}{2}$. On peut aussi faire plusieurs tours de cercle (2π, 4π, 6π, ..., $2k\pi$, ...) et aussi tourner dans le sens négatif (-2π, -4π, -6π, ... $2k\pi$ avec $k \in \mathbb{Z}$).

On imite cela, sans π, donc plus simplement, en posant la définition suivante :

Définition 3.1 *Soit a, b, n trois entiers relatifs quelconques. On dit que a est congru à b modulo n et on note cela*

$$a \equiv b \ [n]$$

lorsque $a - b \in n\mathbb{Z}$ autrement dit s'il existe un entier relatif $k \in \mathbb{Z}$ tel que $a = b + kn$.

D'autres notations que l'on peut trouver dans les ouvrages sont :

$$a \equiv b \ (n) \quad \text{ou} \quad a \equiv b \text{ mod. } n$$

Choisissez la vôtre ! (mais ne changez pas de notation dans une même copie).

Exemple. On a $13 \equiv 1$ [12]. Ceci est bien connu ! car 13h et 1h sur une pendule à aiguilles (comportant 12 secteurs) se placent au même endroit. On a de toute façon $13 - 1 = 12$ et 12 est bien un multiple de 12.

Remarque 1. Puisque les multiples de n sont exactement les multiples de $-n$ il n'a pas beaucoup d'intérêt de parler de congruence modulo -5 : la congruence modulo 5 est exactement la même chose.

Remarque 2. La relation de congruence modulo 0 a elle non plus pas beaucoup d'intérêt : $a \equiv b$ $[0] \iff a = b$: c'est la relation d'égalité !

Remarque 3 (importante). Si $n \neq 0$, dire que $a \equiv b$ $[n]$ c'est exactement dire que a et b ont même reste dans la division euclidienne par n. Par exemple dire que $a \equiv b$ [2] c'est dire que a et b ont même parité (tous les deux impairs ou tous les deux pairs). En effet un nombre est pair si et seulement si son reste dans la D.E. par 2 vaut 0.

3.1 Premières propriétés de la relation $\equiv$

La relation de congruence modulo n possède les trois premières propriétés suivantes :

Réflexivité. Quel que soit $a \in \mathbb{Z}$: $a \equiv a\ [n]$.

Un nombre est donc congru à lui-même. C'est évident car $a - a = 0 \in n\mathbb{Z}$.

Symétrie. Si $a \equiv b\ [n]$ alors $b \equiv a\ [n]$.

En effet si $a - b \in n\mathbb{Z}$ alors $b - a = -(a - b) \in n\mathbb{Z}$.

Transitivité. Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$.

En effet si $a - b \in n\mathbb{Z}$ et $b - c = -(a - b) \in n\mathbb{Z}$ on a alors $a - c = (a - b) + (b - c) \in n\mathbb{Z}$ (la somme de deux multiples de n est un multiple de n).

On résume ces trois propriétés (réflexivité, symétrie, transitivité) en disant que $\equiv$ est une *relation d'équivalence*[3] sur $\mathbb{Z}$.

Congruence et divisibilité. Si $n \neq 0$, dire que a est divisible par n c'est exactement dire que $a \equiv 0\ [n]$.

(En fait ceci est valable même si $n = 0$). Cette dernière propriété est à bien retenir, malgré sa simplicité.

3.2 Opérations sur les congruences

Peut-on ajouter, multiplier deux relations de congruences ? élever au carré une relation de congruence ? ajouter un nombre dans une relation de congruence ? toutes ses questions trouvent leur réponse ici.

[3]Sur l'ensemble des droites du plan, la relation de parallélisme est une relation d'équivalence, par exemple. La relation de perpendicularité n'en est pas une : elle n'est ni réflexive ni transitive.

Théorème. Les congruences se comportent bien avec toutes les opérations, comme l'égalité : on peut ajouter, soustraire, multiplier deux congruences (relatif au même module n évidemment). Mathématiquement : si $a \equiv b\ [n]$ et si $a' \equiv b'\ [n]$ alors :

$$a + a' \equiv b + b'\ [n] \qquad a - a' \equiv b - b'\ [n] \qquad aa' \equiv bb'\ [n]$$

Preuve. Par hypothèse $a - b = kn$ et $a' - b' = k'n$ avec k et k' dans $\mathbb{Z}$. On a donc :

$$(a + a') - (b + b') = (a - b) + (a' - b') = kn + k'n = Kn$$

avec $K = k + k' \in \mathbb{Z}$: ainsi $a + a' \equiv b + b'\ [n]$. On a ensuite :

$$(a - a') - (b - b') = (a - b) - (a' - b') = kn - k'n = K'n$$

avec $K' = k - k' \in \mathbb{Z}$: ainsi $a - a' \equiv b - b'\ [n]$. Enfin on a (grande astuce en maths...) :

$$aa' - bb' = aa' - ab' + ab' - bb' = a(a' - b') + (a - b)b' = ak'n + knb' = K''n$$

avec $K'' = ak' + kb' \in \mathbb{Z}$ donc $aa' \equiv bb'\ [n]$. □

En particulier, puisque $x \equiv x\ [n]$ pour tout entier x et puisque $a^p = a \times a \times \ldots a$ (p fois) on a :

Corollaire. Si $a \equiv b\ [n]$ et si $x \in \mathbb{Z}$ est un entier relatif quelconque et $p \in \mathbb{N}$ un entier naturel quelconque alors :

$$a + x \equiv b + x\ [n] \qquad a^p \equiv b^p\ [n] \qquad ax \equiv bx\ [n]$$

PIEGE ! Il y a quand même des interdits : on ne peut pas simplifier dans une congruence, en général. Par exemple $14 \equiv 6\ [8]$ mais on ne peut pas simplifier par 2 car sinon on aurait $7 \equiv 3\ [8]$ ce qui est FAUX ! (par contre on a bien $7 \equiv 3\ [4]$). Nous étudierons plus tard dans quel cas on peut simplifier.

Exemple. Cet exemple va vous convaincre de l'extrême efficacité des congruence. Montrer que pour tout entier $n \in \mathbb{N}$, $1 + 6^n + 11^n + 26^n + 31^n$ est toujours un multiple de 5.

On pourrait penser à un raisonnement par récurrence car la propriété à démontrer porte sur un «pour tout $n \in \mathbb{N}$». On invite le lecteur à en rédiger la (longue) démonstration. On peut aussi utiliser les congruence modulo 5. On sait en effet que :

$$6 \equiv 1\ [5] \qquad 11 \equiv 1\ [5] \qquad 26 \equiv 1\ [5] \qquad 31 \equiv 1\ [5]$$

donc d'après les propriétés des congruences on a :

$$6^n \equiv 1^n (= 1)\ [5] \qquad 11^n \equiv 1^n (= 1)\ [5] \qquad 26^n \equiv 1^n (= 1)\ [5] \qquad 31^n \equiv 1^n (= 1)\ [5]$$

et en ajoutant, ce qu'on a le droit de faire avec des congruences :

$$1 + 6^n + 11^n + 26^n + 31^n \equiv 1 + 1 + 1 + 1 + 1 \ [5]$$

i.e. finalement $1 + 6^n + 11^n + 26^n + 31^n \equiv 0 \ [5]$. Ce qui prouve le résultat !