Hier, dans la preuve de l'unicité de la factorisation première, nous avions besoin d'un petit résultat de type "bien-connu". Il faut être capable de le montrer. Voilà une preuve :

Lemme

Supposons $N = nm$, *ou* $n \geq 1$ *et* $m \geq 2$. *Alors* $n < N$.

Démonstration.

$n + n(m-1) = nm = N$ et $n(m-1) \geq 1$. Donc $n < N$. □

Si $n = p_1 p_2 \dots p_s$ est composé et $p_1 \leq p_2 \leq \dots$ alors $s \geq 2$ et

$$p_1^2 \leq p_1 p_2 \leq n.$$

Donc si n est composé, alors il existe un premier p tel que $p \mid n$ et $p^2 \leq n$.

Donc $n > 1$ est premier si $p \nmid n$ pour chaque premier p tels que $p^2 \leq n$

Vous comprenez la logique ? !

$p \leq \sqrt{n}$

Exemple : Pour montrer que 193 est premier, il suffit de voir que 193 n'est pas divisible par $2, 3, 5, 7, 11, 13$. (On a déjà $14^2 = 196 > 193$.) Ce qui est le cas.

$a_3(193) \stackrel{?}{=} a_3(0)$

Nous allons présenter la fameuse preuve par l'absurde d'Euclide du théorème suivant

Théorème

Il existe une infinité de nombres premiers.

Démonstration.

Supposons qu'il existe seulement un nombre fini, disons N, de nombres premiers. Soient $p_1, p_2, p_3, \ldots, p_N$ ces nombres premiers (parmi eux se trouvent bien sûr 2, 3, 5, 7, 11.) Considérons le très grand nombre

$$n = 1 + (p_1 \cdot p_2 \cdot p_3 \cdots p_{N-1} \cdot p_N).$$

Comme pour chaque nombre naturel, il existe un nombre premier p qui divise n.

Ce nombre premier p se trouve nécessairement sur la liste de tous les nombres premiers plus haut : il existe un $1 \leq i \leq N$ tel que $p = p_i$. Mais n s'écrit comme 1 plus un p_i-multiple ; donc $p_i = p$ ne divise pas n, car il y aura un reste 1 après division par p_i.

Alors p divise n ET p ne divise pas n. Ce qui est absurde !

On conclut que l'hypothèse qu'il existe seulement un nombre fini de nombres premiers est fausse ! Le théorème est donc vrai, car c'est l'opposé de cette fausse hypothèse. □

Nous avons l'habitude d'écrire les entiers en forme décimale. Par exemple, 12054 veut dire 4 unités + 5 dix + 0 cent + 2 mille + 1 dix-mille.

$$12054 = 1 \cdot 10^4 + 2 \cdot 10^3 + 0 \cdot 10^2 + 5 \cdot 10^1 + 4 \cdot 10^0.$$

On peut aussi utiliser une base autre que 10. Par exemple les bases 2 et 16 sont utilisées en informatique. Sur base 2 (forme binaire) :

$$[100101]_{(2)} = 2^5 + 2^2 + 2^0 = [\ldots]$$

Soit $b > 0$, un nombre naturel, la base choisie, alors on peut écrire n'importe quel nombre naturel n sur la forme

$$n = [c_s, c_{s-1}, \ldots, c_1, c_0]_b = c_s b^s + c_{s-1} b^{s-1} + \ldots + c_1 b^1 + c_0 b^0,$$

ou chaque "chiffre" c_i est plus petit que b.

(Ex. : Donner une preuve par induction généreuse.)

Possiblement il faut inventer des notations pour les chiffres !

Par exemple, pour base 16 on utilise les 16 chiffres

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E$$

$A = 10$ (dix), $B = 11$ (onze), $C = 12$ (douze), $D = 13$ (treize) ,
$E = 14$ (quatorze), $F = 15$ (quinze).
Par exemple

$$N = [2AE0B]_{16}$$

signifie dans notre notation décimale usuelle le nombre

$$N = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627.$$

Alternativement, on écrit

$$[2, 10, 14, 0, 11]_{16}$$

$12 = [12]_{10} = [C]_{16}$

Comment écrire un nombre N sur la base $b > 1$?

Avec division-avec-reste par b répété !

Par division avec reste il y a q_0 et c_0 tel que $N = q_0 b + c_0$, et $0 \leq c_0 < b$.

Puis il y a q_1 et c_1 tel que $q_0 = q_1 b + c_1$, et $0 \leq c_1 < b$.

Puis il y a q_2 et c_2 tel que $q_1 = q_2 b + c_2$, et $0 \leq c_2 < b$.

Et cetera.

On arrête dès que q_i devient 0. Alors

$$N = [c_s, c_{s-1}, \ldots, c_1, c_0]_b.$$

$17 = [23]_7$

$17 = 2 \cdot 7 + 3$

$2 = 0 \cdot 7 + 2$

Exemple, si $b = 16$ et $N = 357911$.

$$\begin{aligned} 357911 &= 22368 \cdot 16 + 11 \\ 22368 &= 1398 \cdot 16 + 0 \\ 1398 &= 87 \cdot 16 + 6 \\ 87 &= 5 \cdot 16 + 7 \\ 5 &= 0 \cdot 16 + 5 \end{aligned}$$

Donc (rappel : $A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$).

$$N = [357911]_{10} = [5760B]_{16}.$$

Supposons on a écrit le nombre naturel N sur la base 7 :

$$N = [6, 5, 6, 3, 0, 2, 3, 5, 0, 0]_7$$

Alors $7|N$ et même $7^2|N$.

Pourquoi ?

$100 \mid 6530\,0$

Conséquences modulo m.

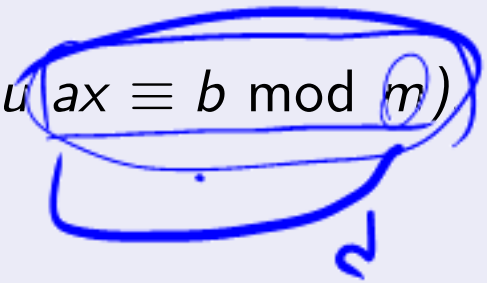
Souvent dans les mathématiques on doit résoudre des équations linéaires "modulo m".

Nos algorithmes d'Euclide et de Bézout ont des conséquences "modulo m" aussi.

Théorème

Fixons trois nombres entiers a, b, m et supposons $m > 0$. Mettons $d = \text{pgcd}(a, m)$. Considérons l'équation

$$ax \equiv_m b \ (\text{ou } ax \equiv b \bmod m)$$



On peut trouver un entier x qui satisfait cette équation
si et seulement si

$$d | b.$$

Ou exactement la même chose, mais reformulée :

Théorème

Fixons $m > 0$ et deux classes-modulo-m $\mathrm{C}\ell_m(a)$, $\mathrm{C}\ell_m(b) \in \mathbb{Z}/m\mathbb{Z}$. Mettons $d = \mathrm{pgcd}(a, m)$. Considérons l'équation

$$\mathrm{C}\ell_m(a) \cdot X = \mathrm{C}\ell_m(b).$$

On peut trouver une classe-modulo-m $X = \mathrm{C}\ell(x) \in \mathbb{Z}/m\mathbb{Z}$ qui satisfait cette équation
si et seulement si

$$d | b.$$

Démonstration.

Supposons d'abord que pour $x \in \mathbb{Z}$ on a $ax \equiv b \mod m$. Alors $m|(ax - b)$ et il existe un entier c tel que $ax - b = cm$. On a que $d|a$ et $d|m$ et on conclut que $d|(ax - cm)$ et $d|b$.

Par contre, supposons $d|b$. Il existe un entier c tel que $b = cd$. Par le théorème de Bézout, il existe deux entiers s, t tels que $sa + tm = d$; et donc aussi $csa + ctm = cd = b$. Alors $csa - b$ est divisible par m et

$$csa \equiv_m b.$$

Alors $x = cs$ satisfait l'équation. □

Peut-on résoudre-modulo-1064 l'équation

$$1351x \equiv 21 \mod 1064 \,?$$

Heureusement, nous avons déjà calculé que $\text{pgcd}(1351, 1074) = 7$, et 7 divise la partie droite 21 : une solution existe !

Par contre l'équation

$$1351x \equiv 29 \mod 1064$$

on ne peut pas résoudre, car 7 ne divise pas 29 !

Pour trouver une solution, on commence par trouver s, t par la méthode de Bézout, tels que $s1351 + t1064 = 7$. Ce que nous avons aussi déjà fait !

$$(-63) \cdot 1351 + 80 \cdot 1064 = 7$$

donc en multipliant par 3 :

$$(-3 \cdot 63) \cdot 1351 + (3 \cdot 80) \cdot 1064 = 3 \cdot 7 = 21$$

et

$$(-3 \cdot 63) \cdot 1351 \equiv 21 \mod 1064$$

Donc $x = -3 \cdot 63 = -189$ est une solution.
Si on veut une solution positive on ajoute 1064, c.-à-d.,
$x = -189 + 1064 = 875$ est aussi une solution.

$$x \equiv -189 \equiv x \pmod{875}$$

Corollaire

Soit m un entier positif, et a, b, c des entiers. Si $ac \equiv bc \mod m$ et $\text{pgcd}(c, m) = 1$, alors $a \equiv b \mod m$.

Démonstration.

Par Bézout, ils existent s et t tels que $sm + tc = 1$, donc $tc \equiv 1 \mod m$.
Donc si $ac \equiv bc \mod m$ on a aussi $atc \equiv btc \mod m$ et

$$a \equiv atc \equiv btc \equiv b \mod m.$$

□

$\frac{1}{12} \cdot 12 = 1$

Comparer :

Si a, b, c sont trois entiers et

$$ac = bc.$$

On ne peut pas conclure que $a = b$ non plus, sauf si on sait que $c \neq 0$.

Soit m un entier positif, et a, b, c des entiers. Si $ac \equiv bc \mod m$ alors on vient de voir

$$a \equiv b \mod m,$$

si $\text{pgcd}(c, m) = 1$.
On a vraiment besoin de cet hypothèse.
Par exemple : $1 \cdot 2 \equiv 3 \cdot 2 \mod 4$ mais
$1 \not\equiv 3 \mod 4$ (et $\text{pgcd}(2, 4) = 2 \neq 1$).

Soit $m > 0$.
On dit que $C\ell_m(b)$ est une *inverse-modulo-m* de $C\ell_m(a)$ si

$$C\ell_m(a)\, C\ell_m(b) = C\ell_m(1).$$

On a uitlisé un inverse-modulo-m déjà, dans la preuve du cor. avant.

Corollaire

(i) Une telle inverse existe si et seulement si $\text{pgcd}(a, m) = 1$.
(ii) m est un nombre premier, si et seulement si une inverse-modulo-m existe pour chaque $C\ell_m(a) \neq C\ell_m(0)$.

Si une inverse existe, c'est unique. Pouvez-vous montrer ça ?

Démonstration.

(i) est une corollaire, aussi une implication de (ii) est corollaire.
Si m est un nombre tel que une inverse-modulo-m existe pour chaque $\mathrm{C}\ell_m(a) \neq \mathrm{C}\ell_m(0)$. Si $m = rs$ est composé, alors $\mathrm{C}\ell(r)\,\mathrm{C}\ell(s) = \mathrm{C}\ell(m) = \mathrm{C}\ell(0)$. Soit $\mathrm{C}\ell(b)$ l'inverse de $\mathrm{C}\ell(r)$, alors

$$\mathrm{C}\ell(s) = \mathrm{C}\ell(b)\,\mathrm{C}\ell(r)\,\mathrm{C}\ell(s) = \mathrm{C}\ell(b)\,\mathrm{C}\ell(0) = \mathrm{C}\ell(0)$$

et $\mathrm{C}\ell(1) = \mathrm{C}\ell(s)\,\mathrm{C}\ell(r) = \mathrm{C}\ell(0)$. Contradiction. Donc m est premier. □

Si $C\ell_m(b)$ est une inverse-modulo-m de $C\ell_m(a)$, nous pouvons résoudre l'équation

$$C\ell_m(a)X = C\ell(c)$$

Car $C\ell_m(a) \cdot X = C\ell_m(c)$ si et seulement si

$$X = C\ell_M(b)\, C\ell_m(a)X = C\ell_m(b)\, C\ell_m(c) = C\ell_m(bc).$$

Alors $X = C\ell_m(bc)$ est la solution :

$$C\ell_m(a)\, C\ell_m(bc) = C\ell_m(a)\, C\ell_m(b)\, C\ell_m(c) = C\ell(c).$$

Si p est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. Par contre $\mathbb{Z}$ n'est pas un corps.

Conséquence : une très grande partie de MAT1600 reste valable si on remplace $\mathbb{R}$ par un corps, en particulier $\mathbb{Z}/p\mathbb{Z}$!

Résoudre un système d'équations linéaires, méthode de Gauss, forme échelonnée, matrices inversibles, déterminant, espace vectoriel.... On a beaucoup de théorèmes et méthodes sur les équations linéaires avec coefficients dans $\mathbb{Z}/p\mathbb{Z}$ sans frais additionnels, (presque] pour le même prix. Ex :

$$M = \begin{pmatrix} C\ell_5(2) & C\ell_5(3) \\ C\ell_5(1) & C\ell_5(2) \end{pmatrix}$$

M^{-1}

est inversible car son déterminant est $C\ell_5(1)$ et donc non-zéro. $M^{-1} = ?$.

$M\,M^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $1 = C\ell_5(1)$

Mentionnons sans preuve le "petit théorème de Fermat".

Théorème (Fermat)

Soit p un nombre premier et a un entier. Alors

$$a^p \equiv_p a.$$

Une preuve sera donné dans le cours MAT2600, la théorie des groupes. Pour vous c'est seulement une curiosité sans doute. Mais c'est à l'origin de beaucoup d'applications, par exemple pour une communication secure entres les banques.

Le nombre 11 est premier. Vérification :

$$14^{11} \equiv_{11} 3^{11} \equiv_{11} 3^{2\cdot 5+1} \equiv_{11} (9)^5 \cdot 3 \equiv_{11} (-2)^5 \cdot 3 \equiv_{11}$$

$$\equiv_{11} -32 \cdot 3 \equiv_{11} 1 \cdot 3 \equiv_{11} 3 \equiv_{11} 14.$$

En effet

$$14^{11} \equiv_{11} 14.$$

Nous n'avions pas besoin de calculer 14^{11} et puis calculer le reste après division par 11. Le calcul modulaire est beaucoup plus agréable que le calcul ordinaire. Les nombres impliqué restent petits ! Et ce théorème aide beaucoup pour calculer les hautes puissances.

Soit $m > 0$ et a un entier. Soit r le reste de a après division par m. C'est l'unique nombre naturel r tel que $m|(a - r)$ et $0 \leq r < m$. Donc associer r à a est vraiment une fonction avec domaine $\mathbb{Z}$ et avec codomaine les nombres naturels entre 0 et $m - 1$. On devrait écrire quelque chose comme

$$\text{Reste-après-division-par-}m(a) = r,$$

mais pour des raisons historiques on écrit $(a \bmod m) = r$, ou même

$$r = a \bmod m.$$

(Le manuel le fait.)
Aussi mod est un bouton sur certaines calculatrices, qui calcule le reste-modulo-m.

$r \equiv a \bmod m$

Malheureusement ça introduit possiblement une confusion avec la notation

$$r \equiv a \mod m$$

pour la relation d'équivalence $r \equiv_m a$! Mais il y a des liens.

On a $r = a \mod m$ si et seulement si $r \equiv a \mod m$ et $0 \leq r < m$. Et $a \equiv b \mod m$ si et seulement si $(a \mod m) = (b \mod m)$.

Soient a, b deux nombres entiers non-zéro. Posons d pour le plus grand diviseur en commun de a et b. Alors d est un maximum

$$d = \text{Max}(\{m \in \mathbb{N} |\ m|a \text{ et } m|b\})$$

mais d est aussi un minimum :

$$d = \text{Min}(\{m \in \mathbb{N} |\ m > 0 \text{ et } \exists (s,t) \in \mathbb{Z}^2\ m = sa + tb\})$$

Démonstration.

Soit $E = \{m \in \mathbb{N} |\ \exists (s,t) \in \mathbb{Z}^2\ m = sa + tb\}$ et posons $d' = \text{Min}(E)$.
Par Bézout $d \in E$, donc $d' \leq d$.
Aussi il existe s', t' tels que $d' = s'a + t'b$. Donc $d|d'$ ce qui implique $d \leq d'$. Donc $d = d'$. □

Rappelons :

Les propriétés considérées *essentielles* de l'ensemble des nombres naturels $\mathbb{N} = \{0, 1, 2, 3, \ldots, n, n+1, \ldots\}$ sont les suivantes :

1. Chaque nombre naturel n a un unique *successeur* dans $\mathbb{N}$, noté $n+1$.
2. Il existe un nombre naturel spécial, noté 0, et
3. chaque nombre naturel n différent de 0 a un unique *prédécesseur* dans $\mathbb{N}$, noté $n-1$. On a $(n+1)-1 = n$, pour tout $n \in \mathbb{N}$ et $(n-1)+1 = n$ pour tout $n \in \mathbb{N}$ tel que $n \neq 0$.
4. **Si $E \subseteq \mathbb{N}$ est un sous-ensemble de $\mathbb{N}$ tel que (i) $0 \in E$ et (ii) pour chaque $n \in E$ aussi $n+1 \in E$, alors nécessairement $E = \mathbb{N}$.**

Principe du bon ordre

Soit $E \subseteq \mathbb{N}$ un sous-ensemble non-vide de l'ensemble des nombres naturels. On dit que l'élément m est un *minimum de* E si $m \in E$ et $m \leq n$ pour chaque $n \in E$.
Par exemple 0 est le minimum de $\mathbb{N}$.
À la place d'induction ou directement la dernière propriété essentielle de $\mathbb{N}$ on peut souvent utiliser le principe du bon ordre (souvent avec une preuve par contradiction).

Theorem (Principe du bon ordre)

Tout sous-ensemble non vide de $\mathbb{N}$ a un minimum.

la preuve est sautée (pas orig.)

Démonstration.

Soit $E \subset \mathbb{N}$ un ensemble non-vide. On va montrer que E a un minimum, par une preuve par contradiction : Supposons que E n'a pas un minimum.

Considérons la fonction propositionnelle $P(n) = "n \notin E"$, où $n \in \mathbb{N}$. On va montrer par induction généreuse que $P(n)$ vraie pour chaque $n \in \mathbb{N}$.

Début : Si $0 \in E$, alors 0 serait un minimum de E (c'est même un minimum pour tout $\mathbb{N}$). Donc $0 \notin E$ et $P(0)$ est vraie.

Étape d'induction : Soit $n \in \mathbb{N}$ et supposons que pour $0 \leq m \leq n$ on a $P(m)$ vraie, c.-à-d., $m \notin E$. On va montrer que $P(n+1)$ est vraie.

Supposons au contraire que $P(n+1)$ est fausse, ou $n+1 \in E$ mais $0, 1, \ldots, n$ ne sont pas dans E par l'hypothèse d'induction. Soit $a \in E$. Alors a n'est pas un des $0, 1, \ldots, n$, qui sont les nombres naturels plus petit que $n+1$. En consèquence $a \geq n+1$. Et on conclut que $n+1$ est un minimum de E. Ce qui est une contradiction. Alors $P(n+1)$ est vraie. Par le principe d'induction généreuse, on conclut que $P(n)$ est vraie pour chaque $n \in \mathbb{N}$: pour chaque entier $n \notin E$. □

suite.

Ce qui implique que E est vide ! Une contradiction encore parce que E n'est pas vide !
Cette fois on conclut que l'hypothèse "E n'a pas un minimum" est faux : et E a en effet un minimum. □

Un minimum est en fait unique.

Lemma (Unicité)

Soit $E \subseteq \mathbb{N}$ un sous-ensemble non-vide. Alors E a un seul minimum.

Démonstration.

Par le principe du bon ordre au moins un minimum existe dans E. Soient n_1 et n_2 deux minima de E. Alors n_1 et n_2 sont dans E et pour chaque $m \in E$ on a que $n_1 \leq m$ et $n_2 \leq m$. En particulier $n_1 \leq n_2$ (car $n_2 \in E$) et $n_2 \leq n_1$ (car $n_1 \in E$). Donc $n_1 = n_2$. □

preuve en sautie pas obligatoire

Le reste d'aujourd'hui ne sera pas matière d'examen.

À partir de seulement les propriétés essentielles de $\mathbb{N}$ nous allons déduire les autres propriétés de $\mathbb{N}$ bien connues par vous.
Un peu longue, mais pas vraiment dur.

La définition de l'addition.

Definition

Fixons $a \in \mathbb{N}$. Nous allons définir pour chaque $n \in \mathbb{N}$ l'élément $a + n \in \mathbb{N}$. Au début $a + 0 = a$ et $a + 1$ est le successeur de a (qui existe et est unique par une des propriétés essentielles de $\mathbb{N}$). Puis supposons pour $n \in \mathbb{N}$ on a déjà défini $a + n$, alors on définit $a + (n + 1)$ comme le successeur de $a + n$, c.-à-d., par définition

$$a + (n + 1) := (a + n) + 1.$$

Ainsi on a défini $a + n$ pour chaque $n \in \mathbb{N}$.

Démonstration.

En effet l'addition $a + n$ est définie pour $n = 0$, et si c'est définie pour n alors c'est aussi définie pour $n + 1$. Par le principe d'induction, l'addition $a + n$ a été définie pour chaque $n \in \mathbb{N}$. □

La définition de la multiplication.

Definition

Fixons $a \in \mathbb{N}$. Nous allons définir pour chaque $n \in \mathbb{N}$ l'élément $a \cdot n \in \mathbb{N}$. Au début on définit $a \cdot 0 := 0$, $a \cdot 1 := a$. Supposons pour $n \in \mathbb{N}$ on a déjà défini $a \cdot n$, alors on définit $a \cdot (n+1) := (a \cdot n) + a$. Ainsi on a défini $a \cdot n$ pour chaque $n \in \mathbb{N}$.

L'associativité de l'addition :

Théorème

Pour tous les nombres naturels a, b, c on a

$$(a + b) + c = a + (b + c).$$

Démonstration.

Fixons a et b. Nous allons montrer par induction sur n que $(a + b) + n = a + (b + n)$.

Début : Si $n = 0$ c'est vrai : $(a + b) + 0 = a + b = a + (b + 0)$, car par définition $N + 0 = N$ pour chaque nombre naturel N.

Étape d'induction. Supposons $(a + b) + n = a + (b + n)$, pour $n \geq 0$. Alors

$$(a + b) + (n + 1) = ((a + b) + n) + 1 = ((a + (b + n)) + 1 =$$

$$= a + ((b + n) + 1) = a + (b + (n + 1)).$$

Alors le théorème est vrai par induction. □

Lemme

Pour chaque nombre naturel n on a

$$0 + n = n + 0 = n \quad \textit{et} \quad 1 + n = n + 1.$$

Démonstration.

Rappel : par définition de l'addition on a $n + 0 = n$ et
$0 + (n + 1) = (0 + n) + 1$ pour chaque nombre naturel n.
On montre que $0 + n = n + 0 = n$ par induction.
Début : si $n = 0$ c'est une tautologie : $0 + 0 = 0 + 0$.
Étape d'induction : Supposons par induction que $0 + n = n + 0 = n$. Donc

$$0 + (n + 1) = (0 + n) + 1 = n + 1 = (n + 1) + 0.$$

On conclut par induction. □

(suite).

Puis, on montre que $1 + n = n + 1$ par induction.
Début. Si $n = 0$ on a : $1 + 0 = 1 = 0 + 1$, car par définition 1 est le successeur de 0.
Étape d'induction : Supposons par induction que $1 + n = n + 1$. Alors par L'hypothèse d'inducton et l'associativité :

$$(n + 1) + 1 = (1 + n) + 1 = 1 + (n + 1).$$

Et donc par induction on conclut : $1 + n = n + 1$ pour chaque nombre naturel n. □

La commutativité de l'addition :

Théorème

Pour tous nombres naturels n et m on a

$$m + n = n + m.$$

Démonstration.

Fixons m. Nous allons montrer le théorème par induction sur n.
Début : c'est le lemme précécent.
Étape d'induction : Supposons par induction que $m + n = n + m$, pour $n \geq 0$. Donc par définition de l'addition, l'hypothése d'induction, l'associativité de l'addition, et le lemme

$$m + (n + 1) = (m + n) + 1 = (n + m) + 1 = 1 + (n + m) =$$

$$= (1 + n) + m = (n + 1) + m.$$

Donc par induction théorème est vrai. □

La distributivité :

Théorème

Pour tous nombres naturels a, b, n on a

$$(a + b) \cdot n = (a \cdot n) + (b \cdot n).$$

Démonstration.

Par induction sur n.

Début. Pour $n = 0$ on a : $(a + b) \cdot 0 = 0 = 0 + 0 = (a \cdot 0) + (b \cdot 0)$.

Étape d'induction. Supposons $(a + b) \cdot n = (a \cdot n) + (b \cdot n)$.. On a par définition de la multiplication, l'associativité et la commutativité de l'addition, et l'hypothèse d'induction :

$$(a + b) \cdot (n + 1) = ((a + b) \cdot n) + (a + b) = ((a \cdot n) + (b \cdot n)) + (a + b) =$$

$$= ((a \cdot n) + a) + ((b \cdot n) + b) = ((a \cdot (n + 1)) + ((b \cdot (n + 1)).$$

Donc par le principe d'induction, le théorème est vrai. □

L'associativité de la multiplication :

Théorème

Pour tous nombres naturels a, b, n on a

$$(a \cdot b) \cdot n = a \cdot (b \cdot n).$$

Démonstration.

Par induction sur n.

Début. Pour $n = 0$ on a : $(a \cdot b) \cdot 0 = 0 = a \cdot 0 = a \cdot (b \cdot n)$.

Étape d'induction. Supposons $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Alors par définition de la multiplication, l'hypothèse d'induction et la distributivité :

$$(a \cdot b) \cdot (n+1) = ((a \cdot b) \cdot n) + (a \cdot b) = (a \cdot (b \cdot n)) + (a \cdot b) =$$

$$= a \cdot ((b \cdot n)) + b) = a \cdot (b \cdot (n+1)).$$

Donc par le principe d'induction, le théorème est vrai. □

Lemme

Pour chaque nombre naturel n on a

$$0 \cdot n = n \cdot 0 = 0 \quad \textit{et} \quad 1 \cdot n = n \cdot 1 = n$$

Démonstration.

Rappel : par définition de la multiplication on a $n \cdot 0 = 0$ et $n \cdot 1 = n$.
On montre que $0 \cdot n = 0$ par induction. Début : si $n = 0$ on a en effet $0 \cdot 0 = 0$. Étape d'induction : Supposons par induction que $0 \cdot n = 0$. Alors par définition de la multiplication, l'hypothèse d'induction, et par définition de l'addition

$$0 \cdot (n + 1) = (0 \cdot n) + 0 = 0 + 0 = 0.$$

Donc par le principe d'induction, c'est vrai que $0 \cdot n$ pour chaque nombre naturel n.
On montre que $1 \cdot n = n$ par induction. Début : si $n = 0$ on a en effet $1 \cdot 0 = 0$, par définition. Supposons par induction que $1 \cdot n = n$. Alors par définition de la multiplication, l'hypothèse d'induction,

$$1 \cdot (n + 1) = (1 \cdot n) + 1 = n + 1$$

La commutativité de la multiplication :

Théorème

Pour tous nombres naturels a, n on a

$$a \cdot n = n \cdot a$$

Démonstration.

Par induction sur n. Début : si $n = 0$ on a en effet $a \cdot 0 = 0 = 0 \cdot a$ par le lemme. Aussi si $n = 1$ on a en effet $a \cdot 1 = a = 1 \cdot a$ par le lemme. Étape d'induction : Supposons par induction que $a \cdot n = n \cdot a$. Alors par définition de la multiplication, l'hypothèse d'induction, le lemme, la distributivité

$$a \cdot (n + 1) = (a \cdot n) + a = (n \cdot a) + 1 \cdot a = (n + 1) \cdot a.$$

Donc par le principe d'induction, le théorème est vrai. □