ARITHMETIQUE

Partie des mathématiques étudiant les propriétés élémentaires des nombres entiers.

Introduction : Le développement de l'informatique et plus généralement de ce qu'on appelle «le numérique », est étroitement lié à l'arithmétique. Lorsqu'on a besoin de traiter des informations, de faire fonctionner des documents multimédias (textes, sons, images) sur des machines, il est souvent nécessaire de les coder.
Toute information peut être codée en utilisant des suites formées uniquement des deux symboles 0 et 1. On parle de représentation binaire …

$\mathbb{N}$ désigne l'ensemble des entiers naturels et $\mathbb{Z}$ désigne l'ensemble des entiers relatifs

Les trois axiomes fondamentaux

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément. (Faux dans $\mathbb{Z}$)

Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

Toute suite d'entiers naturels strictement décroissante est finie. (Faux dans $\mathbb{Z}$)

Divisibilité dans $\mathbb{Z}$: diviseurs, multiples d'un entier

Définitions : Soit a et b deux entiers relatifs.
On dit que a divise b s'il existe un entier q tel que $b = a.q$.
On écrit alors $a \mid b$.
On dit aussi : «b est divisible par a »
«a est un diviseur de b ».
«b est un multiple de a ».

Théorèmes :

1) Si $a \mid b$ alors $a \mid bc$ quel que soit l'entier c.
2) Si $a \mid b$ et si $b \mid c$ alors $a \mid c$.
3) Si $a \mid b$ et si $a \mid c$ alors a divise toute combinaison linéaire de b et c, $\alpha.b + \beta.c$ où α et β sont des entiers relatifs.
4) Si $a \mid b$ et $b \neq 0$ alors $|a| \leq |b|$. Ainsi, tout entier non nul admet un nombre fini de diviseurs.
5) Si $a \mid b$ et si $b \mid a$ alors $a = \pm b$.

Démonstrations.

1) Si $a \mid b$ alors il existe un entier q tel que $b = a.q$. Alors $b.c = (a.q).c = a.(qc)$ donc $a \mid bc$.
2) Si $a \mid b$ et si $b \mid c$ alors il existe deux entiers q et r tels que $b = aq$ et $c = br$ donc $c = (aq)r = a(qr)$ d'où $a \mid c$.
3) Si $a \mid b$ et $a \mid c$ alors il existe deux entiers q et r tels que $b = aq$ et $c = ar$ donc $\alpha b + \beta c = \alpha(aq) + \beta(ar) = a(\alpha q + \beta r)$ donc $a \mid (\alpha b + \beta c)$.

4) Si $a \mid b$ *et* $b \neq 0$ *alors il existe un entier* q *non nul tel que* $b = aq$ *donc* $|b| = |a||q|$ *et* $|q| \geq 1$ *d'où* $|b| \geq |a|$.
5) Si $a \mid b$ *et* $b \mid a$ *alors* $|a| \leq |b|$ *et* $|b| \leq |a|$ *donc* $|a| = |b|$, *soit* $a = \pm b$.

Nombres premiers

Tout entier naturel $n \neq 1$ possède au moins deux diviseurs : 1 et n.

Exercice : chercher «tous » les diviseurs de 150, de 12, de 7 ….

Une disposition pratique :

150	1
75	2
50	3
30	5
25	6
15	10

7	1

12	1
6	2
4	3

Remarque : si $n = p \times q$ avec $p \leq q$ alors $p \leq \sqrt{n}$.
En effet, (par l'absurde) si $p > \sqrt{n}$ alors $q > \sqrt{n}$ et $pq > n$!

$q \mid p$

<u>Définition</u> : Un entier naturel différent de 1 est dit «premier » si ses seuls diviseurs <u>positifs</u> sont 1 et lui-même.

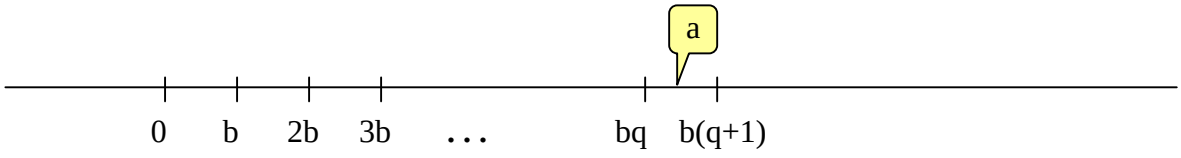
Par définition : 1 n'est pas premier.
0 n'est pas premier.
Quelques nombres premiers : ... 2, 3, 5, 7, 11, 13,... , 37, ..., 41,... , 19 999 999,...
(on démontrera que la suite des nombres premiers est infinie)

Division euclidienne

<u>Propriété d'Archimède</u> : Soit a **un entier naturel et** b **un entier naturel non nul.**
Alors il existe un entier naturel n **tel que** $n.b \geq a$.
Preuve :
Si $a = 0$ *alors* $n = 1$ *convient ; si* $a \neq 0$ *alors* $n = a$ *convient car* $b \geq 1$ *implique* $a.b \geq a$.

<u>Conséquence</u> : étant donnés deux entiers naturels a **et** b **(**$b \neq 0$**), il existe un entier naturel** q **tel que :** $bq \leq a < b(q+1)$ **.**

a est compris entre deux multiples consécutifs de b.
Intuitivement, les intervalles $[\![bq ; b(q+1)[\![$ « recouvrent » l'ensemble $\mathbb{Z}$.



Démonstration :
Soit E l'ensemble des entiers naturels n tels que n.b > a.
D'après la propriété d'Archimède, il existe un entier n tel que nb≥a+1, soit nb>a donc E n'est pas vide.
E possède donc un plus petit élément p. (cf. axiomes de $\mathbb{N}$ *)*
On a : p∈E mais p-1∉E, donc (p - 1)b ≤ a < pb
D'où qb ≤ a < (q+1)b en posant $q = p - 1$ *.*

Théorème : soit *a* un entier naturel et *b* un entier naturel non nul. Alors il existe un unique couple d'entiers naturels (*q* ; *r*) tels que *a* = *b*.*q* + *r* avec 0 ≤ *r* < *b*.

Démonstration :

Existence : d'après le résultat précédent, il existe q∈ N tel que qb ℂ a< (q+1)b, soit $0 \leq a-bq < b$.
En posant $r = a - bq$, *on obtient :* $a = bq + r$ *et* $0 \leq r < b$.

Unicité :
Supposons trouvés deux couples $(q_1 ; r_1)$ *et* $(q_2 ; r_2)$ *tels que*
$a = b.q_1 + r_1$ *et* $a = b.q_2 + r_2$
avec $0 \leq r_1 < b$ *et* $0 \leq r_2 < b$
En ajoutant membre à membre les inégalités $0 \leq r_1 < b$ *et* $-b < -r_2 \leq 0$ *, on obtient :* $-b < r_1 - r_2 < b$
De plus, $r_1 - r_2 = b.(q_1 - q_2)$ *donc* $r_1 - r_2$ *est multiple de b.*
Or le seul multiple de b strictement compris entre b et -b est 0.
On a donc $r_1 - r_2 = 0$. *Par suite* $q_1 - q_2 = 0$ *soit* $q_1 = q_2$.

Division euclidienne dans $\mathbb{Z}$:

Théorème : soit *a* un entier relatif et *b* un entier relatif non nul. Alors il existe un unique couple d'entiers relatifs (*q* ; *r*) tels que *a* = *b*.*q* + *r* avec 0 ≤ *r* < $|b|$.

L'existence peut être prouvé à l'aide du résultat précédent. (exercice)
L'unicité se prouve de la même manière que dans la démonstration précédente. (exercice)

Définition : L'opération permettant de passer du couple (*a* ; *b*), $a \in \hat{I}$, $b \in \hat{I}\backslash\{0\}$ au couple (*q* ; *r*) s'appelle « **la division euclidienne de *a* par *b*** ». *a*, *b*, *q* et *r* sont respectivement le **dividende**, le **diviseur**, le **quotient** et le **reste** de cette division.

Nombres ayant même reste dans la division euclidienne par un entier non nul – notion de congruence - Compatibilité avec les opérations usuelles.

Définition : Lorsque deux entiers relatifs a et b ont le même reste dans la division euclidienne par un entier naturel n non nul, on dit qu'ils sont congrus modulo n et on note $a \equiv b \bmod n$.

Théorème :

Soit a et b deux entiers relatifs et n un entier naturel non nul.
Alors a et b ont le même reste dans la division euclidienne par n si et seulement si $a - b$ est multiple de n.

Démonstration : $a = nq + r$, avec $0 \leq r < n$

$b = nq' + r'$, avec $0 \leq r' < n$

par différence on obtient : $a - b = n(q - q') + (r - r')$, avec $-n < r - r' < n$

- si $r = r'$ alors $a - b$ est multiple de n.
- si $a - b$ est multiple de n alors $r - r'$ est un multiple de n,
  or $-n < r - r' < n$ donc $r - r' = 0$, soit $r = r'$.

Théorème : Soit a, b, a', b' des entiers relatifs et n un entier naturel non nul.
Si a et b ont respectivement les mêmes restes que a' et b' dans la division euclidienne par n.
Alors dans la division euclidienne par n :

- **$a + b$ a le même reste que $a' + b'$**
- **$a - b$ a le même reste que $a' - b'$**
- **ab a le même reste que $a'b'$**
- **a^k a le même reste que a'^k (pour tout k de $\mathbb{Z}$)**

Démonstration : il existe des entiers q et q' tels que :

$a - a' = nq$

$b - b' = nq'$

Alors, $a + b = n(q + q') + (a' + b')$

$a - b = n(q - q') + (a' - b')$

$ab = n(nqq' + qs + q'r) + a'b'$

On montre par récurrence sur k que $a^k = nq_k + a'^k$.

En termes de congruences, le théorème s'énonce :

Si $a \equiv a' \bmod n$ et $b \equiv b' \bmod n$ alors :

$$a + b \equiv a' + b' \bmod n$$
$$a - b \equiv a' - b' \bmod n$$
$$ab \equiv a'b' \bmod n$$
$$a^k \equiv a'^k \bmod n$$

Des critères de divisibilité

Exercice : énoncer un critère de **divisibilité par 2**

Divisibilité par 3

Exemple : $456 = 4 \times 10^2 + 5 \times 10 + 6$
or $10 = 3 \times 3 + 1$; $10^2 = 3 \times 33 + 1$
donc $456 = 4 \times (3 \times 33 + 1) + 5 \times (3 \times 3 + 1) + 6$
$456 = 4 + 5 + 6 + (4 \times 3 \times 33 + 5 \times 3 \times 3)$
$456 = 15 + 3 \times (4 \times 33 + 5 \times 3)$
par suite 456 est divisible par 3 car 15 est divisible par 3 et réciproquement.

Démonstration du cas général :
(voir annexe 2 : systèmes de numération)

$n = \overline{a_n a_{n-1} \ldots a_1 a_0} = a_0 + a_1 \times 10 + \ldots + a_{n-1} \times 10^{n-1} + a_n \times 10^n$
On a : $10 \equiv 1 \bmod 3$ donc $10^k \equiv 1 \bmod 3$ pour tout entier k.
Par suite : $n \equiv a_n + a_{n-1} + \ldots + a_1 + a_o \bmod 3$
n et $a_n + a_{n-1} + \ldots + a_1 + a_o$ ont le même reste dans la division par 3.
En particulier :

n est divisible par 3 si et seulement si $a_n + a_{n-1} + \ldots + a_1 + a_o$ est divisible par 3.

Démontrer les critères suivants :

Divisibilité par 5

n est divisible par 5 si et seulement si a_o est divisible par 5.

Divisibilité par 9

n est divisible par 9 si et seulement si $a_n + a_{n-1} + \ldots + a_1 + a_o$ est divisible par 9.

Divisibilité par 11

n est divisible par 11 si et seulement si $\sum_{k=0}^{n} (-1)^k a_k$ est divisible par 11.

Conjecturer puis démontrer des critères de divisibilité par 13, 17, 19 et 25.

PGCD et algorithme d'Euclide.

Définition :

On notera D(a) l'ensemble des diviseurs positifs d'un entier naturel a.
Soit a et b deux entiers naturels tels que l'un au moins est non nul.
Les ensembles D(a) et D(b) ont au moins un élément commun : 1.
L'ensemble $D(a) \cap D(b)$ est une partie non vide de $\mathbb{N}$ et majorée (par *max*(a ; b)) donc possède un plus grand élément appelé PGCD de a et de b (Plus Grand Commun Diviseur de a et de b).

Le PGCD de a et de b est noté $a \wedge b$ ou pgcd (a , b).
Si a et b sont des entiers relatifs alors on définit pgcd (a , b) = pgcd ($|a|, |b|$)

Exemple : pour déterminer le PGCD de 48 et 64,

- on peut écrire en extension les ensembles D(48) et D(64).

D(48) = {1, 2, 3, 4, 8, 12, 16, 24, 48}
D(64) = {1, 2, 4, 8, 16, 32, 64}
$D(48) \cap D(64)$ = {1, 2, 4, 8, 16} d'où pgcd(48 , 64) = 16.

- on peut utiliser l'algorithme d'Euclide décrit ci-dessous.

L'algorithme d'Euclide

Etape 1 : étant donnés deux entiers naturels a et b, avec b non nul, on fait la division euclidienne de a par b. On a : $a = b.q_0 + r_0$ avec $0 \leq r_0 < b$ et on démontre que $D(a) \cap D(b) = D(b) \cap D(r_0)$.

Etape 2 : si $r_0 \neq 0$ on recommence l'étape 1 avec le couple $(b ; r_0)$. $b = q_1.r_0 + r_1$ avec $0 \leq r_1 < r_0$.
On a alors $D(a) \cap D(b) = D(b) \cap D(r_0) = D(r_0) \cap D(r_1)$.
Et ainsi de suite, on construit une suite d'entiers $r_0, r_1, \ldots r_n$ vérifiant $0 \leq r_n < r_{n-1} < \ldots < r_1 < r_0$ et $D(a) \cap D(b) = D(r_{n-1}) \cap D(r_n)$.
Ce processus est nécessairement fini car (r_n) est une suite strictement décroissante d'entiers naturels.

Etape 3 : la dernière étape a lieu lors de l'apparition du premier reste nul,
Si $r_n = 0$ avec $r_{n-1} \neq 0$ on a $D(a) \cap D(b) = D(r_{n-1}) \cap D(0) = D(r_{n-1})$.
Le PGCD de a et de b est donc égal au dernier reste non nul obtenu dans les divisions successives.

Démonstrations :

- *étape 1 : par double inclusion...*

Soit c un élément de $D(a) \cap D(b)$. $c \mid a$ *et* $c \mid b$ *donc* $c \mid a - bq_0$
or $r_0 = a - bq_0$ *donc* $c \mid r_0$ *, soit* $c \in D(r_0)$
d'où $c \in D(b) \cap D(r_0)$.
Réciproquement, si $c \in D(b) \cap D(r_0)$ *alors* $c \mid b$ *et* $c \mid r_0$ *donc* $c \mid b.q_0 + r_0$
or, $a = b.q_0 + r_0$ *donc* $c \mid a$ *soit,* $c \in D(a) \cap D(b)$.

- *étape 3 :* $D(0) = \mathbb{N}$ ...

Remarque : on a prouvé que $D(a) \cap D(b) = D(a \wedge b)$.
L'ensemble des diviseurs communs de a et b est l'ensemble des diviseurs de leur PGCD.

Autrement dit : $d \mid a$ et $d \mid b \Leftrightarrow d \mid \text{pgcd}(a, b)$

Exemple : Calculons le PGCD de 64 et 48 en utilisant cet algorithme.

$64 = 48.1 + \mathbf{16}$ TI 92 mod(64,48) = 16

$48 = 16.3 + \mathbf{0}$ mod(48,16) = 0.

donc pgcd(64,48) = 16

Quelques propriétés du PGCD :

a, b et k sont des entiers naturels non nuls.

$\text{pgcd}(a,1) = 1$; $\text{pgcd}(a,a) = a$; $\text{pgcd}(a,0) = a$; $\text{pgcd}(a,b) = \text{pgcd}(b,a)$

$a \mid b \Leftrightarrow \text{pgcd}(a,b) = a$; $\text{pgcd}(ka,kb) = k \times \text{pgcd}(a,b)$

Si $k \mid a$ et $k \mid b$ alors $\text{pgcd}\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{1}{k} \times \text{pgcd}(a,b)$

Si a est premier et a ne divise pas b alors $\text{pgcd}(a,b) = 1$ (exercices)

Entiers premiers entre eux

Définition :

Deux entiers naturels non nuls sont dits premiers entre eux lorsque leur PGCD est 1.

Théorèmes de Bézout et de Gauss

Calculons le PGCD (25 872, 484)

$25\,872 = 484 \times 53 + \mathbf{220}$

$484 = 220 \times 2 + \mathbf{44}$

$220 = 44 \times 5 + \mathbf{0}$ donc (25 872, 484) = 44.

On peut utiliser les calculs précédents pour écrire 44 comme combinaison linéaire de 25 872 et 484.

$44 = 484 - 2 \times 220$

$= 484 - 2.(25\,872 - 484 \times 53)$

$= 484 \times (1 + 2 \times 53) + 25\,872 \times (-2)$

$\boxed{44 = (-2) \times 25\,872 + 107 \times 484}$ Cette égalité est appelée : identité de Bézout.

Théorème :

Soit a et b deux entiers naturels non nuls et d leur pgcd.
Il existe deux entiers relatifs u et v tels que $a.u + b.v = d$.

Démonstration :

Soit $E = \{n.a + m.b / n \in \mathbb{Z} \text{ et } m \in \mathbb{Z}\}$

$E \cap \mathbb{N}^* \neq \varnothing$ *car* $a \in E$ *(prendre* $n = 1$ *et* $m = 0$*)*

$E \cap \mathbb{N}^*$ *étant une partie non vide de* $\mathbb{N}$ *possède un plus petit élément ; notons-le d.*

Comme $d \in E$ *il existe deux entiers naturels u et v tels que* $d = a.u + b.v$.

- E *contient clairement tous les multiples de d.*
- *Réciproquement, soit x un élément de* $E \cap \mathbb{N}^*$
  Il existe deux entiers q *et* r *tels que :* $x = dq + r$ *avec* $0 \leq r < d$.
  Alors $r = x - dq$ *donc* $r \in E$ *(différence de deux éléments de E).*

Si r était non nul, on aurait $r \in E \cap \mathbb{N}^*$; impossible car $r < d$ (plus petit élément de $E \cap \mathbb{N}^*$), donc $r = 0$.
Par suite x est un multiple de d.
On a prouvé que $E \cap \mathbb{N}^*$ *est l'ensemble des multiples de son plus petit élément d*
Montrons que d est le PGCD de a et de b.

Soit $d' = a \wedge b$

- $d' \mid a$ *et* $d' \mid b$ *donc* $d' \mid a.u + b.v$ *donc* $d' \mid d$.
- $d \mid a$ *et* $d \mid b$ *donc* $d \mid d'$.

$d' \mid d$ *et* $d \mid d'$ *donc* $d = d'$.

Théorème de Bezout :

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

Preuve :

- Si $a \wedge b = 1$ alors $1 = a.u + b.v$ comme conséquence immédiate du théorème précédent avec $d = 1$
- Si $a.u + b.v = 1$ alors tout diviseur commun à a et à b divise $a.u + b.v = 1$ donc $a \wedge b \mid 1$, d'où $a \wedge b = 1$.

Remarque :

Les nombres u et v ne sont pas uniques.
Par exemple, 2 et 3 sont premiers entre eux.
En effet, $3 \times 1 + 2 \times (-1) = 1$ ou $3 \times (-5) + 2 \times 8 = 1$.

Théorème de Gauss :

Si *a* divise le produit *bc* et si *a* est premier avec *b*, alors *a* divise *c*.

Démonstration :

a divise $b.c$ donc il existe un entier k tel que $b.c = k.a$
De plus d'après le théorème de Bézout, a et b étant premiers entre eux, il existe deux entiers u et v tels que $a.u + b.v = 1$; en multipliant par c on obtient
$a.u.c + b.c.v = c$ puis $c = a.u.c + k.a.v$ soit $c = a.(u.c + k.v)$
d'où a divise c.

Conséquences :

Soit a, b, c trois entiers naturels non nuls.
1) Si a et b divisent c et si a et b sont premiers entre eux alors ab divise c.
2) Si un nombre premier p divise un produit ab alors p divise a ou p divise b.
(C'est un exercice !)

Equations diophantiennes
Exemple de résolution dans $\mathbb{Z}^2$ de $ax + by = d$ avec $d = pgcd(a , b)$

Un exemple : Soit à résoudre dans $\mathbb{Z}$, l'équation $9x + 6y = 15$ (E)

- S'il existe une solution, 15 est une combinaison linéaire de 9 et de 6 donc leur PGCD divise 15.

Or pgcd(9,6) = 3 et 15 = 3×5 donc l'équation (E) est équivalente à l'équation (E') :
$3.x + 2.y = 5$ où 3 et 2 premiers entre eux.

D'après le théorème de Bézout, il existe u et v tels que $3.u + 2.v = 1$.
Par exemple $u = 3$ et $v = -4$ (les coefficients de Bezout ne sont pas uniques)
On obtient une solution particulière de (E) en multipliant u et v par 5 :

$$x_o = 5\times 3 = 15 \qquad \text{et} \qquad y_o = 5\times(-4)$$

(On vérifie que $9 \times 15 + 6 \times (-20) = 15$)

Existe-t-il d'autres solutions ?

- Si (x , y) est un couple de solutions de (E) , on a

  $$9x + 6y = 15 \qquad \text{or,} \quad 9x_o + 6y_o = 15$$

  Après soustraction membre à membre et simplifications on obtient :

  $$3.(x - x_o) = 2.(y_o - y)$$

  Donc 2 divise $3.(x - x_o)$ et puisque 2 et 3 sont premiers entre eux, 2 divise $(x - x_o)$ (théorème de Gauss).
  Il existe k tel que $\boxed{x = x_o + 2.k}$. Si bien que $3.2k = 2.(y_o - y)$, par suite $\boxed{y = y_0 - 3.k}$

- D'autre part, on vérifie immédiatement, que pour tout k de $\mathbb{Z}$, le couple (x , y) défini précédemment convient.

Conclusion : l'ensemble des solutions de (E) est l'ensemble des couples d'entiers (x , y) tels que $x = 15 + 2.k$ et $y = -20 - 3.k$ où k est un entier relatif.

Remarques : notons $d = pgcd(a , b)$

On considère l'équation $ax + by = c$.
Si d ne divise pas c alors l'équation n'admet pas de solution.
Si d divise c alors on simplifie par d et on obtient une équation du type $a'x + b'y = c'$ avec a' et b' premiers entre eux.

PPCM de deux entiers naturels

Exemple : écrivons l'ensemble A des multiples strictement positifs de 12, puis l'ensemble B des multiples strictement positifs de 15, puis A∩B. Alors on remarque que le plus petit élément de A∩B est 60. C'est à la fois un multiple de 12 et de 15, d'où son nom... $ppcm(12\,;15) = 60$.

Sur TI 92 *Lmc(12, 15) = 60.*

Définition : Soit a et b deux entiers naturels non nuls.
L'ensemble des multiples communs strictement positifs de a et de b est non vide (il contient ab) donc il possède un plus petit élément appelé plus petit commun multiple de a et de b et noté $ppcm(a\,;b)$.

Si a et b sont des entiers relatifs alors on convient que $ppcm(a\,;b) = ppcm(|a|,|b|)$

Premières propriétés : a et b sont des entiers naturels non nuls.

$ppcm(a\,,b) = ppcm(b\,,a)$; $ppcm(a\,,a) = a$
$ppcm(a\,,1) = a$; $a \mid ppcm(a\,,b)$ et $b \mid ppcm(a\,,b)$
Si a divise b alors $ppcm(a\,,b) = b$.
$a \mid m$ et $b \mid m \Leftrightarrow ppcm(a,b) \mid m$

Lien entre PGCD et PPCM

Théorème : Soit *a* et *b* des entiers naturels non nuls.
Alors : $pgcd(a\,,b) \times ppcm(a\,,b) = ab$

Démonstration :
Posons $m = ppcm(a\,,b)$, $d = pgcd(a\,,b)$ **,**
$a' = \frac{a}{d}$ *et* $b' = \frac{b}{d}$. a' et b' sont premiers entre eux.
Remarquons que : $ab = d^2a'b' = d \times da'b'$

- $da'b' = ab' = a'b$ donc $da'b'$ est multiple de a et de b d'où $\boxed{m \leq da'b'}$.
- Il existe des entiers naturels non nuls p *et* q tels que $m = pa$ et $m = qb$.

Comme $pa = qb$, on a $pa' = qb'$ (en divisant par d).
Par suite $b' \mid pa'$ et $pgcd(a'\,,b') = 1$ donc $b' \mid p$ (théorème de Gauss).
Il existe un entier $k \geq 1$ tel que $p = kb'$. On a donc $m = kb'a = k(da'b')$, d'où $\boxed{m \geq da'b'}$.

Conclusion : $m = da'b'$.
En multipliant par d , on obtient $md = da'db' = ab$ *c.q.f.d.*

Conséquences : a, b et k sont des entiers naturels non nuls.

- $ppcm(ka\,,kb) = k \times ppcm(a\,,b)$
- Si $k \mid a$ et $k \mid b$ alors $ppcm(\frac{a}{k}\,,\frac{b}{k}) = \frac{1}{k} \times ppcm(a,b)$

Algorithme d'essai de division par les nombres premiers successifs pour reconnaître si un entier donné est premier

Théorème 1 : ***Soit n entier naturel strictement supérieur à 1, alors :***

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

Démonstration :
Soit E l'ensemble des diviseurs de n strictement supérieurs à 1.
E n'est pas vide car il contient n.
E étant une partie non vide de $\mathbb{N}$ *admet un plus petit élément p.*
On sait que $p > 1$ *et que p divise n.*
Montrons que p est premier :
Soit q un diviseur de p strictement supérieur à 1.
$q \leq p$ *et* $q \mid n$ *(car* $q \mid p$ *et* $p \mid n$*)*
donc $q = p$ *(p étant le plus petit élément de E).*
Si n n'est pas premier, n s'écrit $n = pk$ *avec* $p \leq k$ *(p étant le plus petit des diviseurs de n strictement supérieurs à 1), d'où* $p^2 \leq pk$ *soit* $p^2 \leq n$ *. c.q.f.d.*

Comment savoir si un entier donné est premier ou non ?

Un entier naturel $n > 1$ est premier s'il n'est divisible par aucun nombre premier inférieur à $\sqrt{n}$.

D'où un algorithme de recherche de primalité par essai de division par les nombres premiers successifs à partir de 2 :

Si *n* est divisible par 2, *n* n'est pas premier et c'est fini.
Sinon, on divise *n* par 3. Si $3 \mid n$ c'est fini
Sinon, on divise par l'entier premier suivant 5, etc...

On arrête les divisions au plus grand entier premier p tel que $p \leq \sqrt{n}$.
Encore faut-il connaître la liste des nombres premiers inférieurs à $\sqrt{n}$!
Cf. annexe 1 : *Crible d'Ératosthène*

Exemple : n = 409 est-il premier ?
$\sqrt{409} \approx 20{,}22$ *On essaie donc les divisions successives par les entiers premiers inférieurs ou égaux à 20 soit : 2, 3, 5, 7, 11, 13, 17, et 19.*
409 est premier.

Existence d'une infinité de nombres premiers.

Théorème : l'ensemble des nombres premiers est infini.

Une démonstration par l'absurde
Soit E l'ensemble des nombres premiers.
Supposons que E est fini et que E contient n éléments $p_1, p_2, p_3, \ldots, p_n$.
Considérons l'entier naturel $a = p_1 . p_2 . p_3 \ldots . p_n + 1$.
$a \geq 2$ *donc a possède au moins un diviseur premier q.*
q est l'un des p_i *donc* $q \mid p_1 . p_2 . p_3 \ldots . p_n$, *par suite* $q \mid a - p_1 . p_2 . p_3 \ldots . p_n$, *soit* $q \mid 1$ *donc* $q = 1$. *Impossible car 1 n'est pas premier.*
L'hypothèse « E fini » a conduit à une impossibilité donc E est infini.

Théorème : Tout naturel *n*, strictement supérieur à 1, peut s'écrire comme un produit de nombres premiers. Cette décomposition en facteurs premiers est unique à l'ordre près.

(L'unicité de la décomposition en facteurs premiers est admise)
Démonstration :
Soit n un entier naturel strictement supérieur à 1 donc n admet un diviseur premier p_1 :
$n = p_1 . a_1$ *avec* $1 \leq a_1 < n$.
Si $a_1 = 1$ *la démonstration est terminée.*
Sinon a_1 *admet un diviseur premier* p_2 *et* $a_1 = p_2 . a_2$. *tel que* $1 \leq a_2 < a_1$.
Ainsi $n = p_1 . p_2 . a_2$.
Si $a_2 = 1$ *la démonstration est terminée.*
Sinon a_2 *admet un diviseur premier* p_3 *et* $a_2 = p_3 . a_3$. *tel que* $1 \leq a_3 < a_2$.
Et ainsi de suite... on fabrique deux suites d'entiers naturels (p_i) *et* (a_i) *telles que*

$$n = p_1 . p_2 . p_3 \ldots a_k$$

La suite d'entiers naturels (a_i) *étant strictement décroissante est finie donc le processus s'arrête pour un entier k tel que* $a_k = 1$.
Les termes de la suite des entiers naturels (p_i) *ne sont pas tous nécessairement distincts.*
En regroupant les éléments égaux, on obtient une décomposition du type :

$$n = p_1^{\alpha_1} . p_2^{\alpha_2} . p_3^{\alpha_3} \ldots p_j^{\alpha_j}$$ ***où*** $p_1, p_2, \ldots, p_j$ ***sont des nombres premiers distincts***

et $\alpha_1, \alpha_2, \ldots, \alpha_j$ ***des entiers naturels.***

Exemples : $60 = 2^2 . 3 . 5$. [Sur TI92 : mode «exact » et factor(60)]
$4896 = 17 . 3^2 . 2^5$.
méthode «manuelle » :

60	2
30	2
15	3
5	5
1	1

Attention : la TI92 ne cherche pas les facteurs premiers lorsqu'ils sont **tous** plus grands que 65 521.

Utilisations de la décomposition en produit de facteurs premiers :

a) *Trouver tous les diviseurs d'un nombre.*
b) *Reconnaître si un nombre est un carré, un cube, etc…*
c) *Calculer un PGCD.*
d) *Calculer un PPCM.*
e) *Calculer la somme de tous les diviseurs d'un nombre.*

Quelques curiosités :

*Les nombres de **Mersenne** (1588-1648) de la forme 2^p-1 où p est premier comme par exemple $2^{19\,937}$-1, $2^{21\,701}$-1, $2^{132\,049}$-1, $2^{216\,091}$-, $2^{859\,433}$-1 sont premiers mais il faut de gros ordinateurs pour l'établir.*

***Fermat** affirme en 1640 que «tous » les nombres du type $F_n = 2^{2^n}+1$ sont premiers. Mais si ceci est vrai pour n = 0, 1, 2, 3, 4, Euler démontre que c'est faux pour n = 5. D'après TI 92 : $2^{2^5}+1 = (641).(6700417)$.*

Actuellement, on sait que ces nombres sont composés pour $5 \le n \le 20$. Pour le reste...

*Le plus grand nombre de Mersenne connu est 3*2^303093+1 (91241 chiffres), Jeffrey Young en 1998*

*Le plus grand nombre premier connu est **2^3021377 - 1 (909526 chiffres)** trouvé par GIMPS en Janvier 1998*

Annexe 1 :

Crible d'Eratosthène ((-284) – (-192) av JC) :

Le crible d'Eratosthène est un algorithme permettant de déterminer la liste de tous les nombres premiers inférieurs à un entier N donné (N > 1)
Description :
On construit une grille comportant tous les entiers de 1 à N.
On raye le 1.
On raye ensuite tous les multiples de 2 autres que 2.
Le premier nombre à rayer est $2\times2 = 2^2$.
Le premier nombre non rayé après 2 est un nombre premier car il n'est multiple d'aucun nombre entier strictement compris entre 1 et lui-même. C'est 3.

On raye tous les multiples de 3 autres que 3. Le premier nombre à rayer est $3\times3 = 3^2$ car 2×3 est déjà rayé.
Le premier nombre non rayé après 3 est un nombre premier car il n'est multiple d'aucun nombre entier strictement compris entre 1 et lui-même. C'est 5.

On raye tous les multiples de 5 autres que 5. Le premier nombre à rayer est $5\times5 = 5^2$ car 2×5, 3×5 et 4×5 ont déjà été rayés comme multiples de 2 et de 3.
Le premier nombre non rayé après 5 est un nombre premier car il n'est multiple d'aucun nombre entier strictement compris entre 1 et lui-même. C'est 7.
Et on continue ainsi de suite …
L'algorithme se termine lorsqu'on a obtenu par ce procédé un nombre premier dont le carré dépasse N. (le premier nombre à rayer serait alors en dehors de la grille !)
Les nombres qui n'ont pas été rayés sont les nombres premiers compris entre 1 et N.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320
321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340
341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360

Annexe 2 :
Systèmes de numération

Il ne faut pas confondre les nombres et leurs désignations. Les nombres préexistent indépendamment de leur nom et la façon de les désigner dépend du langage, de codes choisis.

L'ensemble $\mathbb{N}$ des entiers naturels

La notion de nombre entier naturel se présente à l'intuition sous deux aspects principaux :

- l'aspect cardinal.

Intuitivement, il s'agit de « compter » le nombre d'éléments de divers « ensembles finis »

Deux ensembles sont dits **équipotents** si on peut établir une correspondance terme à terme (une bijection) entre eux. On dit alors qu'ils ont *autant* d'éléments l'un et l'autre. Il s'agit d'une notion très élémentaire, car on peut voir si deux ensembles sont équipotents sans savoir compter.
Ainsi, les bergers de l'Antiquité utilisaient des cailloux (d'où le nom de «calcul») pour faire rentrer le soir *autant* de moutons qu'ils en avaient fait sortir le matin; de même, lorsqu'on voit de nombreux couples danser sur une scène, malgré l'animation et sans compter, on sait immédiatement qu'il y a *autant* d'hommes que de femmes; remarquons enfin que, dès l'école maternelle, les enfants savent qu'ils ont *autant* de doigts à une main qu'à l'autre, aux mains qu'aux pieds, qu'il y a autant de tasses que de soucoupes, etc., et cela parce qu'ils savent réaliser les bijections correspondantes.
On peut définir le **nombre d'éléments** d'un ensemble fini donné comme étant la propriété commune à tous les ensembles qui lui sont équipotents. Par exemple, « deux » est la propriété commune à toutes les collections comportant une paire d'éléments.

- l'aspect ordinal

Intuitivement, il s'agit de « numéroter » (les pages d'un livre, les jours, les abonnés, etc.)

Le nombre peut être défini comme étant un élément d'une suite organisée ayant les propriétés suivantes :
- chaque élément a un successeur unique ;
- deux éléments différents ont des successeurs différents ;
- l'élément 0 n'est le successeur d'aucun nombre.

Le fait de mémoriser les éléments de cette suite (la comptine numérique) permet de garder ou de transmettre la mémoire d'une quantité.

On peut sans danger confondre ces deux définitions, mais selon les situations, c'est l'aspect ordinal ou l'aspect cardinal du nombre considéré qui intervient.

<u>Désignations des nombres</u>

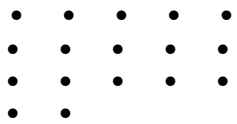
Les hommes ont de tous temps cherchés des moyens pour désigner des quantités de plus en plus grandes avec le moins de signes possibles. Chaque civilisation s'est donné un répertoire de signes et des règles permettant d'écrire et d'énoncer les nombres ; c'est ce que l'on appelle un **système de numération**.

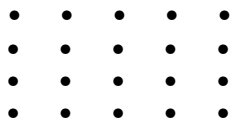
On peut citer les systèmes de numération Egyptien, Maya, Babylonien et Romain qui ont tous leur lot de symboles et de règles propres. L'étude de ces systèmes permet de mieux prendre conscience de l'ingéniosité de notre système de numération usuel actuel dit positionnel à base dix.

Principe de la numération de position à base constante :

L'idée : pour dénombrer une quantité, on choisit une base, par exemple dix (les doigts des mains) puis on fait des regroupements par paquets de dix ; on groupe ensuite les paquets obtenus par dix et ainsi de suite …Les groupements successifs correspondent à de puissances de dix d'unités. On note de droite à gauche les signes désignant les quantités de chaque groupement dans l'ordre des puissances croissantes en utilisant le signe zéro pour marquer l'absence de groupement d'une unité. De sorte qu'une unité de chaque ordre vaut dix unités de l'ordre précédent.

Exercice : utiliser ce procédé pour écrire en base trois les nombres de points

a) 

b) 

Soit b un entier naturel fixé ($b \geq 2$).
Par suite de l'unicité du quotient et du reste dans la division euclidienne, tout entier naturel a s'écrit d'une manière et d'une seule sous la forme :

$a = a_n b^n + a_{n-1} b^{n-1} + \ \ldots + a_1 b + a_0$

où les a_0 , a_1, ..., a_n sont des entiers naturels strictement inférieurs à b et où a_n est non nul.

On dit alors que l'écriture $\overline{a_n a_{n-1} \ldots a_0}^{\,b}$ est l'écriture de a en base b, et on exprime pratiquement chaque nombre a_i par un symbole (ou chiffre) d'une liste donnée de b symboles.

Plus généralement, lorsque aucune confusion n'est possible, on omet l'indication de la base, et on écrit $\overline{a_n a_{n-1} \ldots a_0}$ et même sans surligner $a_n a_{n-1} \ldots a_0$.

Attention : il faut se garder de lire «mille un» pour $\overline{1001}^{\,2}$; on doit lire la suite des chiffres écrits de gauche à droite dès que le nombre est écrit dans une base différente de dix.

Le *système décimal* est le système de numération de position où la base est dix, par exemple, 8345 signifie $8\times10^3 + 3\times10^2 + 4\times10 + 5$

Le *système binaire* est le système de numération de position où la base est deux: l'alphabet est composé des deux seuls chiffres 0 et 1. Ce système est très utilisé, car les machines à deux états (machines électriques ou électroniques, par exemple) peuvent réaliser une représentation des nombres entiers par leur désignation binaire, les deux états de la machine étant, dans le code, la traduction du 0 et du 1. Ainsi, «neuf» peut être codé par un top suivi de deux blancs puis d'un autre top.
Lorsque la base est supérieure à dix, il est nécessaire d'adjoindre aux chiffres habituels de nouveaux symboles. Par exemple, en base douze, on utilisera : « 0 », « 1 », « 2 », « 3 », « 4 », « 5 », « 6 », « 7 », « 8 », « 9 », « α », « β ».