ARITHMETIQUE

DIVISIBILITE DANS $\mathbb{Z}$

Pour bien préciser les notations $\mathbb{N}$ et $\mathbb{Z}$

N s'appelle l'ensemble des entiers naturels ; il est constitué des entiers positifs ou nul ; si on enlève zéro, l'ensemble obtenu est noté N*.

$\mathbb{Z}$ s'appelle l'ensemble des entiers relatifs ; il est constitué de tous les entiers, c'est-à-dire des entiers strictement négatifs, de zéro et aussi des entiers strictement positifs ; si on enlève zéro, l'ensemble obtenu est noté $\mathbb{Z}$*.

$\mathbb{N} = \{0 ; 1 ; 2 ; 3 ; ...\}$ $\quad$ $\mathbb{N} \setminus \{0\} = \{1 ; 2 ; 3 ; ...\}$

$\mathbb{Z} = \{... ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; ..\}$ $\quad$ $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$

$\mathbb{N} = \mathbb{Z}^+$ $\quad$ $\mathbb{N} \subset \mathbb{Z}$

Multiples et diviseurs d'un entier relatif

Quelques exemples

$28 = 14 \times 2$ donc : 28 est un multiple de 14 et aussi un multiple de 2 ; on dit aussi que 14 et 2 sont des diviseurs de 28.

$28 = (-7) \times (-4)$ donc : 28 est un multiple de – 7 et aussi un multiple de – 4 ; on dit aussi que – 7 et – 4 sont des diviseurs de 28.

$-27 = 3 \times (-9)$ donc : – 27 est un multiple de 3 et aussi un multiple de – 9 ; on dit aussi que 3 et– 9 sont des diviseurs de 27.

$-27 = -2 \times 13{,}5$ mais 13,5 n'est pas un entier. – 27 n'est pas un multiple de – 2 car il n'est pas possible de trouver un entier qui, multiplié par – 2, fasse – 27 ; – 2 n'est donc pas un diviseur de – 27.

Multiples d'un entier relatif

Définition 1 Soient a et b deux entiers relatifs quelconques. S'il existe un entier relatif k tel que $a = b\,k$, alors a est un multiple de b ou que b est un diviseur de a.

L'ensemble de tous les multiples de 3 est :

$\{... -12 ; -9 ; -6 ; -3 ; 0 ; 3 ;...\} = \{3\,k ; k \text{ décrit } \mathbb{Z}\}$.

On notera parfois cet ensemble : $3\,\mathbb{Z}$.

L'ensemble de tous les multiples de b est de façon générale $\{... ; b \times (-3) ; b \times (-2) ; b \times (-1) ; b \times 0 ; b \times 1 ; b \times 2 ; b \times 3 ; ...\}$

Si $b \neq 0$, c'est un ensemble ayant une infinité d'éléments ; il contient zéro qui est un multiple de n'importe quel entier relatif b puisque $0 = b \times 0$.

On pourra noter $b\,\mathbb{Z}$ l'ensemble de tous les entiers relatifs multiples de b.

$b\,\mathbb{Z}$ est l'ensemble de tous les multiples entiers relatifs de b.

pour $b \neq 0$, $b\,\mathbb{Z}$ possède une infinité d'éléments.

Exemples : $1\,\mathbb{Z}$ est l'ensemble de tous les multiples de 1 donc $1\,\mathbb{Z} = \mathbb{Z}$.

$2\,\mathbb{Z}$ est l'ensemble de tous les multiples de 2 : c'est l'ensemble de tous les entiers relatifs pairs.

$0\,\mathbb{Z}$ est l'ensemble des multiples de 0 : il n'y en a qu'un seul, c'est zéro lui-même ; donc $0\,\mathbb{Z} = \{0\}$.

$b\,\mathbb{Z} = (-b)\,\mathbb{Z}$ car l'ensemble de tous les entiers relatifs multiples de b coïncide avec l'ensemble de tous les entiers relatifs multiples de $-b$.

Démonstration

a multiple de $b \Leftrightarrow$ il existe k de $\mathbb{Z}$ tel que $a = b \times k \Leftrightarrow$ il existe $-k$ de $\mathbb{Z}$ tel que $a = (-b) \times (-k) \Leftrightarrow a$ multiple de $-b$.

On note $b\,\mathbb{Z}$ l'ensemble des multiples de b.

Définition 2 Soit $n \in \mathbb{Z}$, $d \in \mathbb{Z}^*$, d est un diviseur de n s'il existe un entier relatif $q \in \mathbb{Z}$ tel que $n = q\,d$.

m multiple de $n \Leftrightarrow n$ diviseur de m

On note alors $d \mid n$.

Remarque 1 L'ensemble des diviseurs de 0 est $\mathbb{Z}$

Propriétés de la divisibilité
n et d sont des entiers relatifs

1. d divise n est équivalent à $-d$ divise n
2. si d divise n $(n \neq 0)$ alors $|d| \leq n$.
   donc tout entier non nul admet un nombre fini de diviseurs.
3. Si d et n sont des entiers naturels, si d divise n alors $d \leq n$.
4. si d divise n et n divise d alors $n = d$ ou $n = -d$
5. si d divise n et n divise m alors d divise m
6. a divise b et divise c alors a divise $b\,x + c\,y$ pour tout $(x, y) \in \mathbb{Z}^2$.
   En particulier, a divise $b + c$ et a divise $b - c$.
7. d divise n donc pour tout c de $\mathbb{Z}$ * : $d\,c$ divise $n\,c$.

Nombres premiers

Définition : un entier naturel est premier si et seulement s'il admet uniquement deux diviseurs positifs distincts 1 et lui-même.

Exemples :

1 n'a qu'un seul diviseur donc 1 n'est pas un nombre premier.

– 3 n'est pas un entier naturel donc n'est pas un nombre premier.

24 est divisible par 3 donc n'est pas un nombre premier.

13 a pour seuls diviseurs positifs 1 et 13 donc est un nombre premier.

Propriété : tout entier naturel n supérieur ou égal à 2 admet au moins un diviseur premier. Si cet entier n'est pas premier, il admet un diviseur premier compris entre 2 et $\sqrt{n}$.

Remarque : on utilise souvent la contraposée de cette propriété :

Si un entier n n'admet aucun diviseur premier compris entre 2 et $\sqrt{n}$ alors cet entier n est premier.

Démonstration :

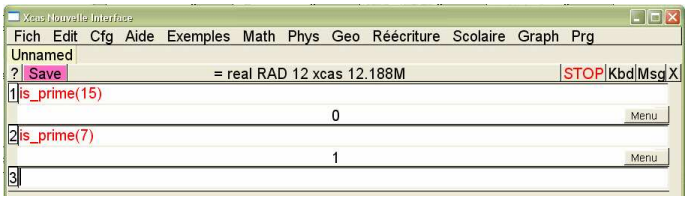
Si n est premier, la propriété est vérifiée

Si n n'est pas premier, alors il admet au moins un diviseur différent de 1 et de n.
Soit p le plus petit diviseur de n différent de 1 et de n.
Montrons que p est un nombre premier, pour cela supposons que ce nombre p n'est pas premier, il admet alors un diviseur p' différent de 1 et de p.
p' est donc encore un diviseur de n différent de 1 et de n et $1 < p' < p < n$, ce qui est en contradiction avec le fait que p est le plus petit diviseur de n différent de 1 et de n. L'hypothèse est donc fausse, p est un nombre premier.
Donc tout entier naturel n supérieur ou égal à 2 admet au moins un diviseur premier.

p est un diviseur de n, il existe donc un entier q tel que $n = p\,q$
p est le plus petit diviseur de n différent de 1 et de n, donc $1 < p \leq q < n$ donc $p^2 \leq p\,q$ soit $p^2 \leq n$ donc $1 < p \leq \sqrt{n}$ soit $2 \leq p \leq \sqrt{n}$

Reconnaître un nombre premier :
Avec un logiciel à calcul formel :
Avec XCas : Choisir le menu Math, Entier,

is_prime(15) puis ENTREE
la réponse 0 correspond à Non
is_prime(7) puis ENTREE
la réponse 1 correspond à Oui



Crible d'Eratosthène
On écrit les nombres entiers de 1 à 100 (par exemple) et on élimine successivement les multiples stricts de 2,

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

on élimine ensuite successivement les multiples stricts de 3,

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

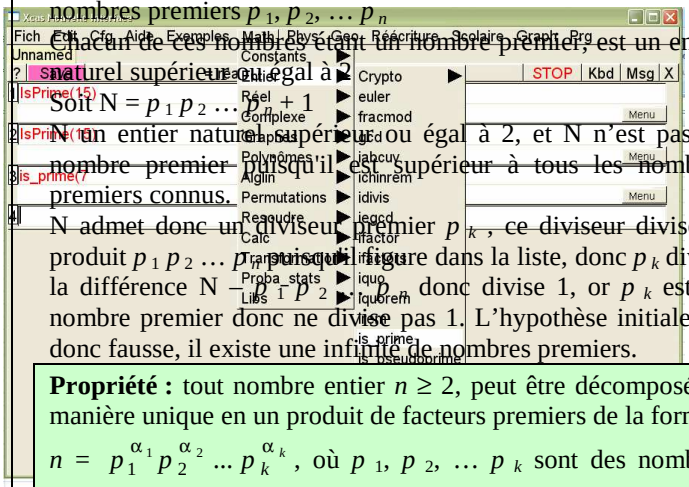
etc. jusqu'à obtenir le tableau suivant :

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

Les cases grisées contiennent les nombres premiers inférieurs ou égaux à 100.

Propriété : il existe une infinité de nombres premiers.

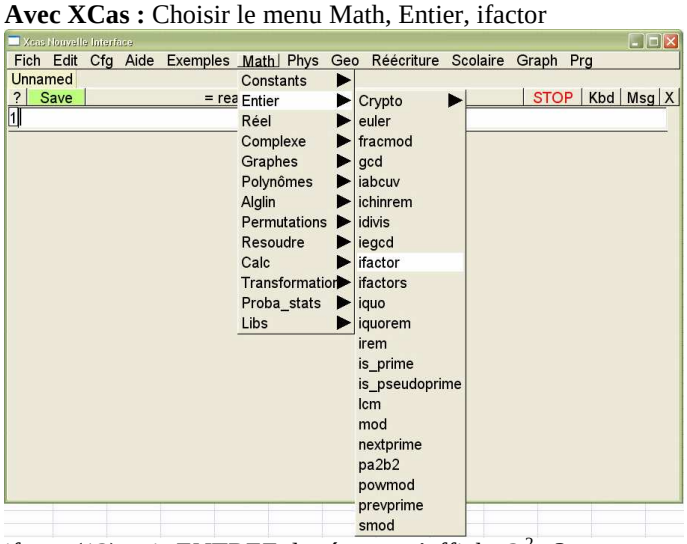
Démonstration : supposons qu'il existe un nombre fini de nombres premiers $p_1, p_2, \ldots p_n$
Chacun de ces nombres étant un nombre premier, est un entier naturel supérieur ou égal à 2.
Soit $N = p_1 p_2 \ldots p_n + 1$
N un entier naturel supérieur ou égal à 2, et N n'est pas un nombre premier puisqu'il est supérieur à tous les nombres premiers connus.
N admet donc un diviseur premier p_k, ce diviseur divise le produit $p_1 p_2 \ldots p_n$ puisqu'il figure dans la liste, donc p_k divise la différence $N - p_1 p_2 \ldots p_n$ donc divise 1, or p_k est un nombre premier donc ne divise pas 1. L'hypothèse initiale est donc fausse, il existe une infinité de nombres premiers.



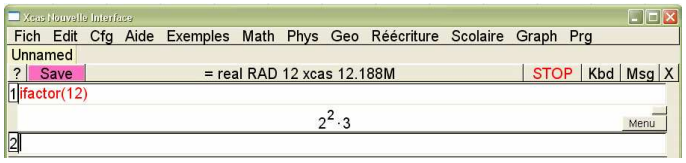
Propriété : tout nombre entier $n \geq 2$, peut être décomposé de manière unique en un produit de facteurs premiers de la forme : $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, où $p_1, p_2, \ldots p_k$ sont des nombres premiers avec $p_1 < p_2 < \ldots < p_k$ et $\alpha_1, \alpha_2, \ldots \alpha_k$ des entiers naturels non nuls. $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ est alors la décomposition de n en produits de facteurs premiers.

Démonstration
$n \geq 2$, donc n admet au moins un diviseur premier q_1, et alors $n = q_1 n_1$
Comme d'une part $n_1 \neq 0$, et d'autre part $q_1 \geq 2$ on a : $1 \leq n_1 < n$
Si $n_1 = 1$, la décomposition est terminée
Si $n_1 \geq 2$, on recommence le même raisonnement avec n_1
n_1 admet un diviseur premier q_2 (éventuellement égal à q_1) et $n_1 = q_2 n_2$
D'une part $n_2 \neq 0$, et d'autre part, comme $q_2 \geq 2$ on a $1 \leq n_2 < n_1 < n$
Les différents nombres $n_1, n_2 \ldots$ forment une suite strictement décroissante de nombres entiers donc il existe un entier naturel r tel que $n_r = 1$
en reconstituant n : $n = q_1 q_2 \ldots q_r$ avec q_i nombres premiers donc en regroupant les nombres premiers identiques :
$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, où $p_1, p_2, \ldots p_k$ sont des nombres premiers avec $p_1 < p_2 < \ldots < p_k$

Décomposer un nombre en produit de facteurs premier
Avec un logiciel à calcul formel :
Avec XCas : Choisir le menu Math, Entier, ifactor



ifactor(12) puis ENTREE, la réponse s'affiche $2^2 . 3$
donc $12 = 2^2 \times 3$



A la main
On divise le nombre par les différents nombres premiers connus

16 758	2
8 379	3
2 793	3
931	7
133	7
19	19
1	

donc $16\,758 = 2 \times 3^2 \times 7^2 \times 19$

Propriété : Soit n un entier naturel admettant pour décomposition en facteurs premiers : $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$
Les diviseurs positifs de n sont les entiers d de la forme $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $0 \le \beta_i \le \alpha_i$ pour tout i compris entre 1 et k

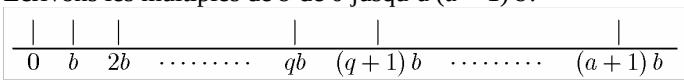
Application :
Nombres de diviseurs de 18 144
$18\,144 = 2^5 \times 3^4 \times 7$ donc les diviseurs positifs de 18 144 sont les entiers d de la forme $d = 2^x \times 3^y \times 7^z$ avec $0 \le x \le 5$, $0 \le y \le 4$ et $0 \le z \le 1$
On a donc $6 \times 5 \times 2 = 60$ multiples différents possibles.

Liste des diviseurs de 3 381
$3\,381 = 3 \times 7^2 \times 23$ donc les diviseurs positifs de 3 381 sont les entiers d de la forme $d = 3^x \times 7^y \times 23^z$ avec $0 \le x \le 1$, $0 \le y \le 2$ et $0 \le z \le 1$ donc on a $2 \times 3 \times 2$ diviseurs possibles de 3 381.
$3^0 \times 7^0 \times 23^0$; $3^0 \times 7^1 \times 23^0$; $3^0 \times 7^2 \times 23^0$;
$3^0 \times 7^0 \times 23^1$; $3^0 \times 7^1 \times 23^1$; $3^0 \times 7^2 \times 23^1$
$3^1 \times 7^0 \times 23^0$; $3^1 \times 7^1 \times 23^0$; $3^1 \times 7^2 \times 23^0$;
$3^1 \times 7^0 \times 23^1$; $3^1 \times 7^1 \times 23^1$; $3^1 \times 7^2 \times 23^1$;

Division euclidienne dans $\mathbb{N}$

Propriété : Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}$, il existe un couple unique (q, r) de $\mathbb{N}^2$ tel que $a = b\,q + r$ avec $0 \le r < b$

Démonstration.
Existence
$b > 0$ donc les multiples positifs de b forment une suite strictement croissante.
Ecrivons les multiples de b de 0 jusqu'à $(a + 1)\,b$.

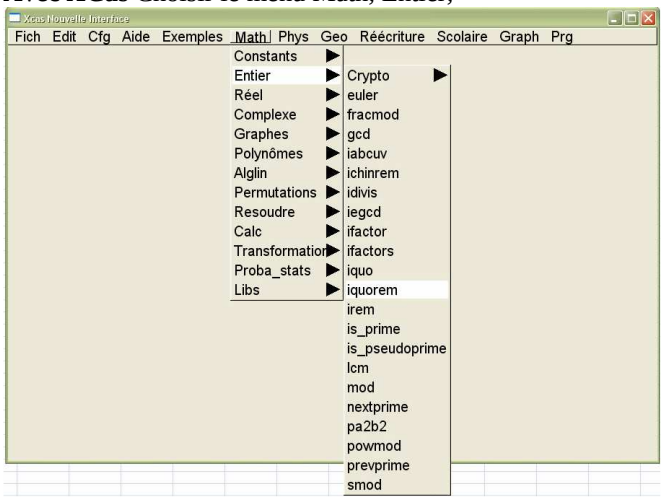


$(a + 1)\,b = a\,b + b$ donc $(a+ 1)\,b > a\,b \ge a$ (car $b \ge 1$).
Donc a est nécessairement, soit l'un des multiples écrits, soit compris entre deux multiples consécutifs, c'est à dire qu'il existe q unique tel que $a \in [q\,b\ ;\ (q + 1)\,b\ [$.
Soit $r = a - b\,q$ (r est donc unique). $b\,q \le a < b\,(q + 1)$ donc $0 \le r < b$
Donc $a = b\,q + r$ avec $0 \le r < b$

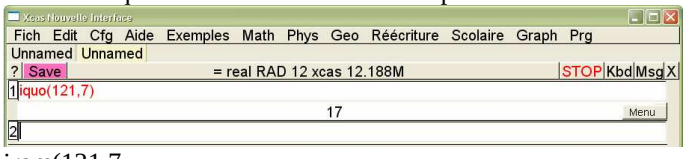
Unicité
Supposons qu'il existe deux couples d'entiers relatifs $(q\ ;\ r)$ et $(q'\ ;\ r')$ tels que $a = b\,q + r$ et $a = b\,q' + r'$ avec $0 \le r < b$ et $0 \le r' < b$
Par soustraction : $b\,(q - q') + r - r' = 0$
$q - q' \in \mathbb{Z}$ donc $r - r'$ est un multiple de b or $-b < r - r' < b$
Le seul multiple qui convient est 0 donc $r - r' = 0$ donc $r = r'$, $b \ne 0$ on a donc $q = q'$

Comment obtenir le reste et le quotient d'une division euclidienne ?
Avec une calculatrice :
Si $b > 0$, $q = \text{Int}(a/b)$ et $r = a - b\,\text{Int}(a/b)$

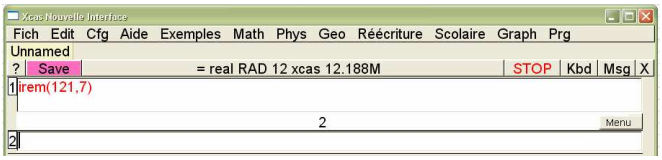
Avec XCas Choisir le menu Math, Entier,



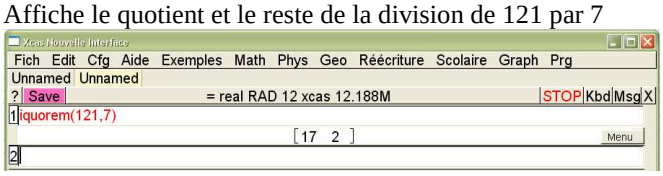
iquot(121,7
Affiche le quotient de la division de 121 par 7



irem(121,7
Affiche le reste de la division de 121 par 7



iquorem(121,7
Affiche le quotient et le reste de la division de 121 par 7



Écriture d'un entier naturel en base *b*, *b* dans $\mathbb{N} \setminus \{0 , 1\}$

Soit *b* un entier naturel donné
- si $b = 0$ alors $b^1 = b^2 = b^3 = ... = 0$
- si $b = 1$ alors $b^1 = b^2 = b^3 = ... = 1$
- si $b \neq 0$ et $b \neq 1$ alors pour 2 exposants distincts i et j : $b^i \neq b^j$.

C'est ce cas qui sera utilisé car il est important de pouvoir distinguer les différentes puissances de *b*.
Nous allons travailler dans un système de numération ayant *b* chiffres 0, 1, 2, ... et $b - 1$.

Propriété

Soit *b* élément de $\mathbb{N} \setminus \{0 , 1\}$, *b* donné.

Tout entier naturel *x* peut s'écrire d'une manière unique :

$$X = x_p \times b^p + x_{p-1} \times b^{p-1} + ... + x_1 \times b^1 + x_0 \times b^0$$

avec $x_p \neq 0$ et pour tout i de $\{0 , ... p\}$, $0 \leq x_i < b$.
Ces nombres x_i sont les chiffres de *x* en base *b*.
On écrit $x = \overline{x_p \, x_{p-1} ... x_1 \, x_0}^{(b)}$.

La démonstration de cette propriété repose sur des divisions euclidiennes successives.
Remarque : La barre que l'on met au-dessus n'a qu'un seul rôle : c'est celui de faire comprendre que les chiffres sont écrits côte à côte dans l'ordre donné. Sans la barre, on pourrait croire que les *x*; se multiplient entre eux, et ici ce n'est pas le cas.

Exemples : $x = \overline{402}^{(Sept)} = 4 \times 7^2 + 0 \times 7^1 + 2 \times 7^0$

$\overline{402}^{(Sept)} = 4 \times 49 + 2 = \overline{198}^{(dix)}$

$y = \overline{3210}^{(quatre)} = 3 \times 4^3 + 2 \times 4^2 + 1 \times 4^1 + 0 \times 4^0$

$\overline{3210}^{(quatre)} = 192 + 32 + 4 = \overline{228}^{(dix)}$

Quelques remarques générales
Tout entier naturel *b* différent de 0 et 1 peut être une base : il y aura alors *b* chiffres dans ce système de numération.
La représentation de « zéro » est 0 dans n'importe quelle base car : $0 = 0 \times b^0$ et $0 < b$
La représentation de « un » est 1 dans n'importe quelle base car : $1 = 1 \times b^0$ et $1 < b$ La représentation de « *b* » ($b > 1$) dans la *b* est : $\overline{10}^{(b)}$ car : $b = 1 \times b^1 + 0 \times b^0$
Dans le système décimal (dix) les chiffres sont : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Dans le système binaire (deux) les chiffres sont : 0, 1
Dans le système de base onze les onze chiffres sont : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, α,
Dans le système de douze (duodécimal) les douze chiffres sont : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, α, β
On complète par d'autres symboles pour avoir le nombre de « chiffres » voulus.

Soit le nombre : $\overline{12\alpha\beta}^{(douze)}$; l'écrire en base 10.

Soit le nombre : $\overline{44\,910}^{(dix)}$; l'écrire en base 12.

Puissances de 12	$12^3 = 1\,728$	$12^2 = 144$	$12^1 = 12$	$12^0 = 1$
Chiffres	1	2	α	β
Produits :	$1 \times 1\,728$	2×144	10×12	11×1

$\overline{12\alpha\beta}^{(douze)} = 1\,728 + 288 + 120 + 11 = \overline{2\,147}^{(dix)}$.

Pour écrire en base douze ; on va donner deux méthodes.
Méthode 1
Écrivons les puissances de 12 inférieures à 44 910. On a successivement $12^2 = 144$; $12^3 = 1\,728$; $12^4 = 20\,736$.

$\overline{44\,910}^{(dix)} = 2 \times 20\,736 + 3\,438$

$\overline{44\,910}^{(dix)} = 2 \times 12^4 + 1 \times 1\,728 + 1\,710$

$\overline{44\,910}^{(dix)} = 2 \times 12^4 + 1 \times 12^3 + 11 \times 144 + 126$

$\overline{44\,910}^{(dix)} = 2 \times 12^4 + 1 \times 12^3 + 11 \times 12^2 + 10 \times 12 + 6$

$\overline{44\,910}^{(dix)} = \overline{21\beta\alpha6}^{(douze)}$

α est le chiffre qui désigne 10, β est le chiffre qui désigne 11

Méthode 2
En utilisant les divisions euclidiennes successives par 12 : les restes obtenus à partir de la gauche seront les chiffres à écrire à partir de la droite.

44 910	12				
8 9	3 742	12			
51	14	311	12		
30	22	071	25	12	
6	**10**	**11**	**1**	2	12
	C'est α	C'est β		**2**	0

D'où $\overline{44\,910}^{(dix)} = \overline{21\beta\alpha6}^{(douze)}$

Voici les explications de la disposition pratique utilisée :
$44910 = 12 \times 3742 + 6$
$= 12\,(12 \times 311 + 10) + 6$
$= 12^2 \times 311 + 12 \times 10 + 6$
$= 12^2 \times (12 \times 25 + 11) + 12 \times 10 + 6$
$= 12^3 \times 25 + 12^2 \times 11 + 12 \times 10 + 6$
$= 12^3 \times (12 \times 2 + 1) + 12^2 \times 11 + 12 \times 10 + 6$
$= 12^4 \times 25 + 12^3 \times 1 + 12^2 \times 11 + 12 \times 10 + 6$

Congruences

Définition : Soient *a* et *b* deux entiers relatifs et *n* un entier naturel supérieur ou égal à 2
a* est congru à *b modulo *n* si et seulement si *a* et *b* ont le même reste dans la division euclidienne par *n*. On note $a \equiv b \; [n]$

On utilise aussi les notations $a \equiv b \bmod(n)$ et $a \equiv b \; (n)$

Exemple : $86 = 7 \times 12 + 2$ et $23 = 7 \times 3 + 2$ donc 86 et 23 ont le même reste dans la division euclidienne par 7 donc $83 \equiv 23 \; [7]$

Propriété : *a* est congru à *b* modulo *n* si et seulement *n* divise $a - b$ ou encore $a - b$ est un multiple de *n*

Démonstration :
Dans la division euclidienne par *n*, il existe deux couple d'entiers relatifs $(q ; r)$ et $(q' ; r')$ avec $0 \leq r < n$ et $0 \leq r' < n$ tels que : $a = n\,q + r$ et $b = n\,q' + r'$

a est congru à b modulo n donc a et b ont le même reste dans la division euclidienne par n donc $r = r'$
soit $a = n\,q + r$ et $b = n\,q' + r$ donc $a - b = n\,(q - q')$ donc n divise $a - b$ ou $a - b$ est un multiple de n.

Réciproquement
si $a - b$ est un multiple de n alors il existe un entier relatif Q tel que $a - b = n$ Q or $b = n\,q' + r'$ donc $a = n\,(Q + q') + r'$ avec $0 \leq r' < n$ donc r' est le reste dans la division euclidienne de a par n donc a et b ont le même reste dans la division euclidienne par n donc $a \equiv b\ [n]$.

Exemples :
$86 - 23 = 63$ or 7 divise 63 donc $86 \equiv 23\ [7]$
$86 - (-5) = 91$ or 7 divise 91 ($91 = 7 \times 13$) donc $83 \equiv -5\ [7]$

Remarques : si r est le reste dans la division euclidienne de a par n alors $a \equiv r\ [n]$ mais la réciproque est fausse : $86 \equiv 23\ [7]$.
0 est un multiple de n donc pour tout entier relatif a, $a \equiv a\ [n]$.

Propriété : On a le droit d'effectuer sur les congruences les mêmes opérations qu'avec les égalités EXCEPTE la division par un entier des deux termes de la congruence
Soit n un entier naturel ($n \geq 2$) et a, b, c, a' , b' des entiers relatifs
1. Si $a \equiv b\ [n]$ alors $a\,c \equiv b\,c\ [n]$
2. Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$
3. Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors $a + a' \equiv b + b'\ [n]$ et $a - a' \equiv b - b'\ [n]$ et $a\,a' \equiv b\,b'\ [n]$
4. Si $a \equiv b\ [n]$ alors pour tout entier naturel p non nul, $a^p \equiv b^p\ [n]$

Démonstration :
1. Si $a \equiv b\ [n]$ alors $a - b$ est un multiple de n donc il existe un entier relatif q tel que $a - b = n\,q$
donc pour tout entier relatif c : $c\,(a - b) = n\,c\,q$
donc $a\,c - b\,c = n\,c\,q$
donc $a\,c - b\,c$ est un multiple de n alors $a\,c \equiv b\,c\ [n]$

2. Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors :
$a - b$ est un multiple de n donc il existe un entier relatif q tel que $a - b = n\,q$
et $b - c$ est un multiple de n donc il existe un entier relatif q' tel que $b - c = n\,q'$
par addition : $a - b + b - c = n\,q + n\,q'$
$a - c = n\,(q + q')$ avec $q + q'$ entier relatif donc $a - c$ est un multiple de n alors $a \equiv c\ [n]$

3. Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors
$a - b$ est un multiple de n donc il existe un entier relatif q tel que $a - b = n\,q$
$a' - b'$ est un multiple de n donc il existe un entier relatif q' tel que $a' - b' = n\,q'$
en additionnant terme à terme :
$a + a' - (b + b') = n\,(q + q')$ avec $q + q'$ entier relatif donc $a + a' - (b + b')$ est un multiple de n alors $a + a' \equiv b + b'\ [n]$
de même en soustrayant membre à membre :
$a - a' - (b - b') = n\,(q - q')$ avec $q - q'$ entier relatif donc :
$a - a' - (b + b')$ est un multiple de n alors $a - a' \equiv b - b'\ [n]$

$a\,a' = (b + n\,q)\,(b' + n\,q')$
donc $a\,a' = b\,b' + n\,(q\,b' + q'\,b + q\,q')$
$q\,b' + q'\,b + q\,q'$ entier relatif donc $a\,a' - b\,b'$ est un multiple de n alors $a\,a' \equiv b\,b'\ [n]$

4. Récurrence :
La propriété si $a \equiv b\ [n]$ alors pour tout entier naturel p non nul, $a^p \equiv b^p\ [n]$ est vraie pour $p = 1$
Supposons que la propriété Si $a \equiv b\ [n]$ alors pour tout entier naturel p non nul , $a^p \equiv b^p\ [n]$ soit vraie pour l'entier et démontrons qu'elle est vraie pour $p + 1$
$a^p \equiv b^p\ [n]$ et $a \equiv b\ [n]$ donc d'après la propriété précédente :
$a^p \times a \equiv b^p \times b\ [n]$ soit $a^{p+1} \equiv b^{p+1}\ [n]$

Applications des congruences
Recherche de restes
Exemple 1
Etudier selon les valeurs de l'entier relatif n, les restes de la division de $n^8 - 5\,n$ par 3.
On factorise : $n^8 - 5\,n = n\,(n^7 - 5)$
Les restes dans la division d'un nombre par 3, sont 0, 1 ou 2 donc on 3 cas :
$n \equiv 0\ [3]$ donc $n\,(n^7 - 5) \equiv 0\ (n^7 - 5)\ [3]$ soit $n\,(n^7 - 5) \equiv 0\ [3]$
$n \equiv 1\ [3]$ donc $n^7 \equiv 1\ [3]$ et $n^7 - 5 \equiv -4\ [3]$ or $2 \equiv -4\ [3]$
ou encore $n^7 - 5 \equiv 2\ [3]$ donc $n^8 - 5\,n \equiv 2\ [3]$
$n \equiv 2\ [3]$ soit $n \equiv -1\ [3]$ donc $n^7 \equiv -1\ [3]$ et $n^7 - 5 \equiv -6\ [3]$ or $-6 \equiv 0\ [3]$ donc $n^7 - 5 \equiv 0\ [3]$ donc $n^8 - 5\,n \equiv 0\ [3]$
Si $n \equiv 1\ [3]$ ou encore n de la forme $3\,k + 1$ avec $k \in \mathbb{Z}$, alors le reste de la division de $n^8 - 5\,n$ par 3 est 2
Si $n \equiv 0\ [3]$ ou , $\equiv 2\ [3]$ ou encore n de la forme $3\,k$ ou $3\,k + 2$ avec $k \in \mathbb{Z}$, alors le reste de la division de $n^8 - 5\,n$ par 3 est 0

Exemple 2
Reste de la division de 2008^n par 15 suivant les valeurs de n
$2008 \equiv 13\ [15]$ ou $2008 \equiv -2\ [15]$
$2008^2 \equiv (-2)^2\ [15]$ soit $2008^2 \equiv 4\ [15]$
$2008^3 \equiv 4 \times (-2)\ [15]$ donc $2008^3 \equiv 7\ [15]$
$2008^4 \equiv 4^2\ [15]$ or $4^2 \equiv 1\ [15]$ donc $2008^{4k} \equiv 1\ [15]$

En remarquant que $2008^{4k+1} = 2008^{4k} \times 2008$
$2008^{4k+1} \equiv 2008\ [15]$ donc $2008^{4k+1} \equiv 13\ [15]$
$2008^{4k+2} \equiv 2008^2\ [15]$ donc $2008^{4k+2} \equiv 4\ [15]$
$2008^{4k+3} \equiv 2008^3\ [15]$ donc $2008^{4k+3} \equiv 7\ [15]$

si n est de la forme $4\,k$ ($k \in \mathbb{Z}$) alors $2008^n \equiv 1\ [15]$

si n est de la forme $4\,k + 1$ ($k \in \mathbb{Z}$) alors $2008^n \equiv 13\ [15]$

si n est de la forme $4\,k + 2$ ($k \in \mathbb{Z}$) alors $2008^n \equiv 4\ [15]$

si n est de la forme $4\,k + 3$ ($k \in \mathbb{Z}$) alors $2008^n \equiv 7\ [15]$

Critère de divisibilité
Dans le système décimal, un entier naturel est divisible :
- par **10** si et seulement si il se termine par zéro
- par $\mathbf{10^2}$ si et seulement si il se termine par deux zéros
- par $\mathbf{10^k}$ si et seulement si il se termine par k zéros
- par **2** si et seulement si il est pair (se termine par 0, 2, 4, 6 ou 8)
- par **5** si et seulement si il se termine par 0 ou 5
- par **4** si et seulement si le nombre formé des deux derniers chiffres (à droite) est divisible par 4
- par **25** si et seulement si il se termine par 00, 25, 50 ou 75
- par **3** si et seulement si la somme de ses chiffres est divisible par 3
- par **9** si et seulement si la somme de ses chiffres est divisible par 9.
- par **11** si et seulement si la différence de la somme de ses chiffres de rang pair et de la somme de ses chiffres de rang impair est divisible par 11.

Exemple
44 319 n'est divisible ni par 2 ni par 5
4 + 4 + 3 + 1 + 9 = 21 et 21 est divisible par 3 donc 44 319 est divisible par 3 mais pas par 9 car 21 n'est pas divisible par 9.

Rang	4	3	2	1	0
Chiffre	4	4	3	1	9

La somme des chiffres de rang pair est 9 + 3 + 4 = 16
La somme des chiffres de rang impair est 1 + 4 = 5
16 – 5 = 11 qui est divisible par 11 donc 44 319 est divisible par 11

PGCD de deux entiers naturels

Diviseurs communs à deux entiers naturels
Soient a et b deux entiers naturels non tous les deux nuls.
L'ensemble des diviseurs communs à a et b est une partie de $\mathbb{Z}$ non vide (elle contient 1) et ses éléments sont tous inférieurs ou égaux à a et à b. donc cet ensemble possède un plus grand élément.

Définition Soient a et b deux entiers non tous nuls. Le plus grand diviseur commun à a et b est le PGCD de a et b.
On le note PGCD (a ; b) ou $a \wedge b$.

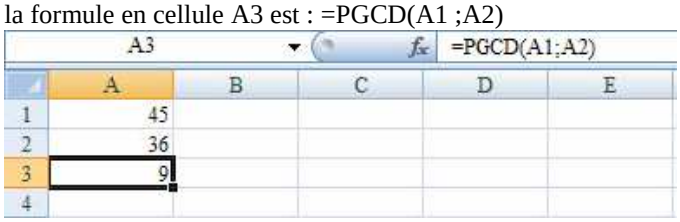
Exemple : Les diviseurs de 36 sont :
– 36 ; – 18 ; – 12 ; – 9 ; – 6 ; – 4 ; – 3 ; – 2 ; – 1 ; 1 ; 2 ; 3 ; 4 ; 6 ; 12 ; 18 ; 36
Les diviseurs de 45 sont :
– 45 ; – 15 ; – 9 ; – 5 ; – 3 ; – 1 ; 1 ; 3 ; 5 ; 9 ; 15 ; 45
Les diviseurs communs à 36 et 45 sont – 9 ; – 3 ; – 1 ; 1 ; 3 ; 9
donc PGCD(36 ; 45) = 9

Remarque : Le PGCD de deux entiers relatifs est un entier supérieur ou égal à 1.
Deux entiers opposés ont les mêmes diviseurs donc
PGCD(a ; b) = PGCD(– a ; b) = PGCD(– a ; – b)

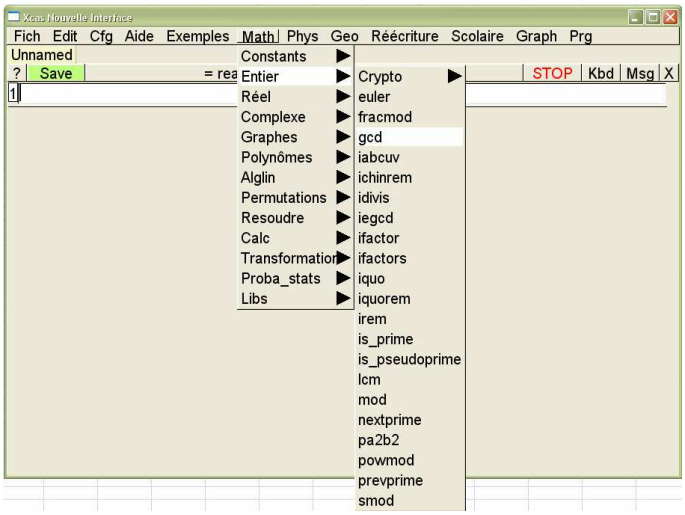
Propriété Pour tout entier naturel c, l'ensemble des diviseurs communs à c et 0 est l'ensemble des diviseurs de c.

Propriété Si a divise b, alors PGCD(a ; b) = a.

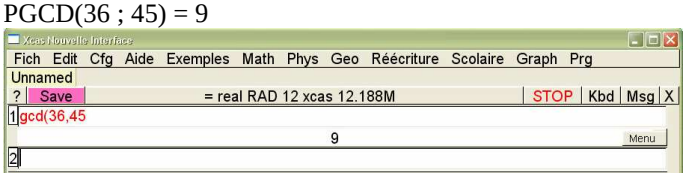
Détermination du PGCD de 2 entiers naturels :
Avec Excel :
la formule en cellule A3 est : =PGCD(A1 ;A2)



Avec XCas Choisir le menu Math, Entier,



La commande gcd(36 , 45 permet d'obtenir que PGCD(36 ; 45) = 9



A la main
Utiliser la décomposition en produit de facteurs premiers (démonstration après)

Algorithme d'Euclide
(démonstration après)

Algorithme d'Euclide

Propriété : Soit a, b, c et q des entiers relatifs tels que $a = b\,q + c$.
Les diviseurs communs à a et b sont les diviseurs communs à b et c.

Démonstration
Notation : D(a , b) est l'ensemble des diviseurs communs à a et b
Soit d un diviseur commun à a et b, d divise $a - b\,q$ donc d divise c, donc D(a , b) (D (b , c)
Soit (un diviseur commun à b et c, (divise b q + c donc (divise a donc D(b , c) (D (a , b) d'où D(a , b) = D (b , c)
Notation : D(a , b) est l'ensemble des diviseurs communs à a et b
Soit d un diviseur commun à a et b, d divise $a - b\,q$ donc d divise c, donc D(a , b) $\subset$ D (b , c)
Soit δ un diviseur commun à b et c, δ divise $b\,q + c$ donc δ divise a donc D(b , c) $\subset$ D (a , b)
d'où D(a , b) = D (b , c)

Remarque :
dans la division euclidienne de a par b, il existe un entier r ($0 \leq r < b$) tel que $a = b\,q + r$ donc D(a , b) = D (b , r)

Propriété : Soit a et b deux entiers relatifs non nuls.
Soit la suite d'entiers définie par $r_0 = |\,b\,|$
r_1 est le reste de la division euclidienne de a par b
si $r_1 \neq 0$, r_2 est le reste de la division euclidienne de b par r_1
si $r_2 \neq 0$, r_3 est le reste de la division euclidienne de r_1 par r_2
…
si $r_{n-1} \neq 0$, r_n est le reste de la division euclidienne de r_{n-2} par r_{n-1} etc.
La suite des restes est finie et le dernier terme non nul de cette suite est le PGCD(a ; b)

Exemple
Calcul de PGCD (4095 ; 98)
$4095 = 98 \times 41 + 77$
$98 = 77 \times 1 + 21$
$77 = 21 \times 3 + 14$
$21 = 14 \times 1 + 7$
$14 = 7 \times 2$
Le dernier reste non nul est 7 donc PGCD (4095 ; 98) = 7

Démonstration : Par définition du reste de la division euclidienne : $0 \leq r_n < \ldots < r_2 < r_1 < |b|$
La suite (r_n) est strictement décroissante, à termes positifs donc contient au plus $|b| + 1$ éléments donc il existe un entier k tel que $r_k \neq 0$ et $r_{k+1} = 0$.
Par définition de la suite, il existe un entier relatif q_k tel que : $r_{k-1} = q_k r_k$ donc r_k divise r_{k-1}
$D(a ; b) = D(b ; r_1) = \ldots = D(r_{k-1} ; r_k)$
r_k divise r_{k-1} donc $D(r_{k-1} ; r_k) = D(r_k)$
Les diviseurs communs à a et b sont donc les diviseurs de r_k donc $PGCD(a ; b) = r_k$

Propriété : Soit a et b deux entiers non nuls,
- tout diviseur commun à a et b est un diviseur de leur PGCD
- Soit k un entier relatif,
$$PGCD(k\,a ; k\,b) = |k|\,PGCD(a ; b)$$

Démonstration
Propriété 1 : $D(r_{k-1} ; r_k) = D(r_k)$ donc tout diviseur commun à a et b est un diviseur de leur PGCD
Propriété 2 : deux cas :
Si $k > 0$, reprendre l'algorithme d'Euclide en multipliant chaque ligne par k.
Si $k < 0$, $PGCD(k\,a ; k\,b) = PGCD(-k\,a ; -k\,b)$
$PGCD(k\,a ; k\,b) = -k\,PGCD(a ; b)$
$PGCD(k\,a ; k\,b) = |k|\,PGCD(a ; b)$

Application : $-26 = -2 \times 13$ et $39 = 3 \times 13$
donc $PGCD(-26 ; 39) = 13$ $PGCD(2 ; 3) = 13$

Propriété : Le PGCD de deux entiers non nuls est égal au produit de leurs diviseurs premiers communs chacun d'eux étant affecté de son plus petit exposant.

Exemple : $116\,375 = 5^3 \times 7^2 \times 19^1$
$410\,571 = 3^2 \times 7^4 \times 19^1$
Les diviseurs premiers (d'exposant non nul) communs aux deux décomposition sont 7 et 19.
donc $PGCD(116\,375 ; 410\,571) = 7^2 \times 19 = 931$

Nombres premiers entre eux

Définition : Deux entiers naturels a et b sont dits premiers entre eux lorsque leur PGCD est 1.

Propriété : Soit a et b deux entiers relatifs
d est leur PGCD si et seulement s'il existe deux entiers relatifs a' et b' tels que $a = d\,a'$, $b = d\,b'$ et $PGCD(a' ; b') = 1$

Démonstration :
Soit $d = PGCD(a ; b)$, d divise a et b donc il existe deux entiers relatifs a' et b' tels que $a = d\,a'$, $b = d\,b'$
$PGCD(a ; b) = PGCD(d\,a' ; d\,b') = d\,PGCD(a' ; b')$
or $d = PGCD(a ; b)$, donc $d = d\,PGCD(a' ; b')$ donc $PGCD(a' ; b') = 1$
Réciproquement
Supposons qu'il existe deux entiers relatifs a' et b' tels que $a = d\,a'$, $b = d\,b'$ et $PGCD(a' ; b') = 1$
$PGCD(a ; b) = PGCD(d\,a' ; d\,b') = d\,PGCD(a' ; b') = d \times 1$
donc $PGCD(a ; b) = d$

Applications :
Diviseurs communs à deux entiers
PGCD (4095 ; 98) = 7 donc les diviseurs communs à 4 095 et 98 sont les diviseurs de 7 soit – 7 ; – 1 ; 1 ; 7.

Simplification de fractions
Avec l'algorithme d'Euclide : PGCD(50 960 ; 43 472) = 208
donc $50\,960 = 208 \times 245$ et $43\,472 = 208 \times 209$ et 245 et 209 sont premiers entre eux donc $\frac{50\,960}{43\,472} = \frac{245}{209}$ (fraction irréductible).

Théorème de Bezout :
a et b sont deux entiers, $PGCD(a ; b) = d$ **alors** il existe deux entiers relatifs u et v tels que : $a\,u + b\,v = d$
a et b sont deux entiers premiers entre eux **si et seulement s'il** existe deux entiers relatifs u et v tels que : $a\,u + b\,v = 1$

Démonstration :
Soient a et b deux entiers premiers entre eux
Supposons $a > 0$ et $b > 0$
Soit la suite d'entiers définie par $r_0 = a$
$r_1 = b$
r_2 est le reste de la division euclidienne de r_0 par r_1
donc $r_0 = r_1 q_1 + r_2$ donc $r_0 - r_1 q_1 = r_2$
soit $a - b\,q_1 = r_2$
de la forme $a\,u_2 + b\,v_2 = r_3$ avec u_2 et v_2 entiers relatifs

r_3 est le reste de la division euclidienne de r_1 par r_2
donc $r_1 = r_2 q_2 + r_3$ donc $r_1 - r_2 q_2 = r_3$
soit $b - (a - b\,q_1)\,q_2 = r_3$
de la forme $a\,u_3 + b\,v_3 = r_3$ avec u_3 et v_3 entiers relatifs

r_4 est le reste de la division euclidienne de r_2 par r_3
donc $r_2 = r_3 q_3 + r_4$ donc $r_2 - r_3 q_3 = r_4$
$a - b\,q_1 - q_3\,(a\,u_3 + b\,v_3) = r_4$
de la forme $a\,u_4 + b\,v_4 = r_4$ avec u_4 et v_4 entiers relatifs
…
r_{n-1} est le reste de la division euclidienne de r_{n-2} par r_{n-3}.
$r_{n-1} = r_{n-2} \times q_{n-2} + r_{n-3}$

Montrons que pour tout $n \geq 2$, si la propriété est vraie aux rangs $n-2$ et $n-1$ alors elle est vraie au rang n :
au rang $n-2$: $r_{n-2} = a\,u_{n-2} + b\,v_{n-2}$ avec u_{n-2} et v_{n-2} entiers relatifs
au rang $n-1$: $r_{n-1} = a\,u_{n-1} + b\,v_{n-1}$ avec u_{n-1} et v_{n-1} entiers relatifs
Montrons que la propriété est vraie au rang $n+1$
r_n est le reste de la division euclidienne de r_{n-2} par r_{n-1}.
$r_n = r_{n-1} \times q_{n-1} + r_{n-2}$
$r_n = (a\,u_{n-1} + b\,v_{n-1}) \times q_{n-1} + a\,u_{n-2} + b\,v_{n-2}$
de la forme : $r_n = a\,u_n + b\,v_n$ avec u_n et v_n entiers relatifs
La propriété est héréditaire donc la suite (r_n) vérifie : pour tout n de $\mathbb{N}$, il existe deux entiers relatifs u et v tels que :
$$r_n = a\,u_n + b\,v_n.$$
cette suite est telle qu'il existe un rang k tel que $r_k = PGCD(a , b) = d$
donc il existe deux entiers relatifs u et v tels que : $a\,u + b\,v = d$
Si a et b sont des entiers relatifs tels que $PGCD(a , b) = d$, alors $PGCD(-a , b) = PGCD(a , -b) = PGCD(-a , -b) = d$

Si $a > 0$ et $b < 0$, $PGCD(a , -b) = d$ avec a et $-b$ positifs donc il existe deux entiers relatifs u et v tels que :

$a\ u + (-b)\ v = 1$ soit $a\ u + b\ (-v) = 1$, u et $-v$ étant deux entiers relatifs
Même démonstration pour $a < 0$ et $b > 0$ ou $a < 0$ et $b < 0$.

Cas particulier $d = 1$
Si a et b sont premiers entre eux, il existe deux entiers u et v tels que $a\ u + b\ v = 1$ (démonstration précédente)

Réciproquement :
S'il existe deux entiers relatifs u et v tels que : $a\ u + b\ v = 1$,
soit d = PGCD(a ; b), d divise $a\ u + b\ v$ donc d divise 1, or $d > 0$ donc $d = 1$
a et b sont premiers entre eux.

Remarque : attention si $a\ u + b\ v = d$, alors on a uniquement que PGCD (a ; b) divise d
Exemple :
Déterminer u et v tels que $2\,244\ u + 780\ v$ = PGCD(a ; b)
$2\,244 = 780 \times 2 + 684$ soit $684 = 2\,244 - 780 \times 2$
$780 = 684 \times 1 + 96$ soit $96 = 780 - 684 \times 1$
donc $96 = 780 - (2\,244 - 2 \times 780)$
$96 = 3 \times 780 - 2\,244$

$684 = 96 \times 7 + 12$
donc $12 = 2\,244 - 780 \times 2 - 7 \times (3 \times 780 - 2\,244)$
soit $12 = 8 \times 2\,244 - 23 \times 780$

$96 = 12 \times 8$ donc PGCD(a ; b) = 12 ; $u = 8$ et $v = -23$

Théorème de Gauss : Si a, b et c sont des entiers tels que a divise le produit $b\ c$ et si a est premier avec b, alors a divise c.
Sous forme plus symbolique : Si a / $b\ c$ et si PGCD(a ; b) = 1 alors a / c.

Démonstration
D'après le théorème de Bézout, il existe deux entiers u et v tels que : $a\ u + b\ v = 1$ d'où : $a\ c\ u + b\ c\ v = c$.
Puisque a / a et a / $b\ c$, alors a / $a\ c\ u + b\ c\ v$, c'est-à-dire a / c.

Conséquences :
a, b et c sont des entiers strictement positifs.
1. Si a et b divisent un entier c, et si a et b sont premiers entre eux, alors $a\ b$ divise c.
2. Si un nombre premier p divise un produit $a\ b$, alors p divise a ou b.
3. Si un nombre premier divise un produit de nombres premiers, alors il est égal à l'un d'entre eux.
4. La décomposition en facteurs premiers d'un entier est unique (à l'ordre près).

Démonstration
1. Si a divise c, il existe un entier relatif k tel que $c = k\ a$.
Si de plus b divise $c = k\ a$, a et b sont premiers entre eux, donc d'après le théorème de Gauss, b doit diviser k, d'où $k = b\ k_0$ et $c = a\ b\ k_0$ soit $a\ b$ divise c.

2. Si p ne divise pas a, le PGCD de p et a n'étant pas p est donc 1.
p et a sont premiers entre eux, donc d'après le théorème de Gauss, p doit diviser b.

3. C'est une conséquence de 2.
4. Pourrait être démontré en utilisant 3.
Exemples :
Montrer qu'un entier est divisible par un autre :
Pour montrer qu'un entier est divisible par 60, il suffit de démontrer qu'il est divisible par 3 et 5 donc, 3 et 5 étant premiers entre eux,
par 3×5 puis qu'il est divisible par 4
15 et 4 étant premiers entre eux, l'entier est divisible par 4 (15 donc par 60.

Montrer que si a et b sont premiers entre eux, alors $a + b$ et $a\ b$ sont premiers entre eux.
Soit p un diviseur premier commun à $a + b$ et à $a\ b$.
p divise $a\ b$ donc d'après la conséquence 2 du théorème de Gauss, p divise soit a soit b.
si p divise a alors p divise $(a + b) - a$ donc p divise b
si p divise b alors p divise $(a + b) - b$ donc p divise a
dans les deux cas, on aboutit à une contradiction puisque a et b sont premiers entre eux donc $a + b$ et $a\ b$ sont premiers entre eux

Déterminer tous les couples d'entiers naturels (x ; y) vérifiant : $32\ x = 45\ y$.
$32 = 2^5$ et $45 = 3^2$ (5 donc 32 et 45 sont premiers entre eux
32 divise 45 y donc 32 divise y donc il existe un entier relatif k tel que $y = 32\ k$
en remplaçant : $32\ x = 45\ y$ donc $32\ x = 45$ ($32\ k$ soit $x = 45\ k$
les couples d'entiers naturels (x ; y) vérifiant : $32\ x = 45\ y$ sont de la forme ($45\ k$; $32\ k$) avec k ($\mathbb{Z}$

Vérification : $32 \times 45\ k = 45 \times 32\ k$

n est un entier naturel. Prouver que $(n^2 - 1)\ n^2\ (n^2 + 1)$ est divisible par 60.
$60 = 2^2 \times 3 \times 5$
$N = (n - 1)\ n\ (n + 1)\ n\ (n^2 + 1)$
$n \equiv 0\ (4)$ donc $N \equiv 0\ (4)$
$n \equiv 1\ (4)$ donc $(n - 1) \equiv 0\ (4)$ donc $N \equiv 0\ (4)$
$n \equiv 2\ (4)$ donc $n^2 \equiv 0\ (4)$ donc $N \equiv 0\ (4)$
$n \equiv 3\ (4)$ donc $n + 1 \equiv 0\ (4)$ donc $N \equiv 0\ (4)$

$n \equiv 0\ (3)$ donc $N \equiv 0\ (3)$
$n \equiv 1\ (3)$ donc $(n - 1) \equiv 0\ (3)$ donc $N \equiv 0\ (3)$
$n \equiv 2\ (3)$ donc $n + 1 \equiv 0\ (3)$ donc $N \equiv 0\ (3)$

$n \equiv 0\ (5)$ donc $N \equiv 0\ (5)$
$n \equiv 1\ (5)$ donc $(n - 1) \equiv 0\ (5)$ donc $N \equiv 0\ (5)$
$n \equiv 2\ (5)$ donc $n\ 2 + 1 \equiv 0\ (5)$ donc $N \equiv 0\ (5)$
$n \equiv 3\ (5)$ donc $n\ 2 + 1 \equiv 0\ (5)$ donc $N \equiv 0\ (5)$
$n \equiv 4\ (5)$ donc $n + 1 \equiv 0\ (5)$ donc $N \equiv 0\ (5)$
donc 3, 4, 5 divisent N.
Ces nombres étant premiers entre eux, $4 \times 3 \times 5$ divise N donc 60 divise N.

Méthode de résolution de l'équation a $x + b\ y = c$.
1) On détermine d = PGCD(a ; b).

2) Si c n'est pas un multiple de d, l'équation n'a pas de solutions entières.
Sinon, on divise a, b et c par d. On obtient alors une équation de la forme $A\ x + B\ y = C$, avec A et B premiers entre eux.

3) On détermine à l'aide de l'algorithme d'Euclide une solution particulière (u ; v) de l'équation.

4) On écrit $\begin{cases} A\ x + B\ y = C \\ A\ u + B\ v = C \end{cases}$.
En soustrayant membre à membre, on voit que l'équation est équivalente à : $A\ (x - u) = -B\ (y - v)$.
A et B étant premiers entre eux, A divise $-B\ (y - v)$ donc d'après le théorème de Gauss, A divise $(y - v)$ donc il existe un entier relatif
k tel que $y - v = k\ A$ d'où par substitution $x - u = -k\ B$

5) Vérification
Si $x = u - k\,B$ et $y = v + k\,A$, alors $A\,x + B\,y = A\,u + B\,v = C$
Finalement l'ensemble des solutions est l'ensemble des couples de la forme : $(u - k\,B\,;\ v + k\,A)$, où k désigne un entier relatif arbitraire.

Exemple :
x et y désignent des entiers relatifs.
a. **Montrer que l'équation (E) $65\,x - 40\,y = 1$ n'a pas de solution.**
$65\,x - 40\,y = 5\,(13\,x - 8\,y)$ or x et y sont des entiers relatifs donc $65\,x - 40\,y$ est un multiple de 5
1 n'est pas un multiple de 5 donc l'équation (E) $65\,x - 40\,y = 1$ n'a pas de solution.

b. **Montrer que l'équation (E') $17\,x - 40\,y = 1$ admet au moins une solution.**
40 et 17 sont premiers entre eux donc d'après le théorème de Bezout l'équation (E') $17\,x - 40\,y = 1$ admet au moins une solution.

c. **Déterminer à l'aide de l'algorithme d'Euclide un couple d'entiers relatifs solution de l'équation (E').**
L_1 $\quad 40 = 17 \times 2 + 6$
L_2 $\quad 17 = 6 \times 2 + 5$
L_3 $\quad 6 = 5 \times 1 + 1$
donc $1 = 6 - 5 \times 1$
or $5 = 17 - 6 \times 2$ en remplaçant $1 = 6 - (17 - 6 \times 2)$ soit $1 = 3 \times 6 - 17$
or $6 = 40 - 17 \times 2$ en remplaçant $1 = 3 \times (40 - 17 \times 2) - 17$
soit $40 \times 3 - 17 \times 7 = 1$ ou encore $17 \times (-7) - 40 \times (-3) = 1$
$(-7\,;-3)$ est solution de (E').

d. **Résoudre l'équation (E').**
$$\begin{cases} 17\,x - 40\,y = 1 \\ -17 \times 7 + 40 \times 3 = 1 \end{cases}$$
En soustrayant membre à membre, on voit que l'équation est équivalente à : $17\,(x + 7) - 40\,(y + 3) = 0$
40 et 17 étant premiers entre eux, 40 divise $-(x + 7)$ donc d'après le théorème de Gauss, 40 divise $(x + 7)$ donc il existe un entier
relatif k tel que $(x + 7) = 40\,k$ d'où par substitution :
$(y + 3) = 17\,k$
Vérification :
Si $x = -7 + 40\,k$ et $y = -3 + 17\,k$, alors :
$17\,x - 40\,y = 17 \times (-7 + 40\,k) - 40 \times (-3 + 17\,k) = 1$
donc l'ensemble des solutions est l'ensemble des couples de la forme : $(-7 + 40\,k\,;\ -3 + 17\,k)$, où k désigne un entier relatif arbitraire.

La recherche de la solution particulière peut se faire à l'aide d'un tableau :
$a = 40$ et $b = 17$ (inutile de s'occuper des signes)

	u	v	$a\,u + b\,v$	Quotient
Ligne L_1	1	0	40	
Ligne L_2	0	1	17	
$L_3 = L_2 - q_1\,L_1$	1	-2	6	$q_1 = 2$ quotient de 40 par 17
$L_4 = L_3 - q_2\,L_2$	-2	5	5	$q_2 = 2$ quotient de 17 par 6
$L_5 = L_4 - q_3\,L_3$	3	-7	1	$q_3 = 1$ quotient de 6 par 5
$L_6 = L_5 - q_4\,L_4$	-17	40	0	

donc si $u = 3$ et $v = -7$ on a :
$3 \times 40 - 7 \times 17 = 1$ soit $(-7) \times 17 - 40 \times (-3) = 1$
$(-7\,;-3)$ est solution de (E'). La suite est identique

Petit théorème de Fermat : Soit a un entier relatif et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1 \quad [p]$

Démonstration
soit a un entier relatif
soit r le reste de la division euclidienne de a par p ; alors $a \equiv r$ $[p]$ donc $a^{p-1} \equiv r^{p-1} \quad [p]$
or $r \equiv 0$ donc il suffit de démontrer le théorème dans le cas où a est un entier positif.
Soit p un nombre premier et a un entier naturel.
On sait que :
$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ldots + \binom{p}{p-1} a + 1$$
Soit k un entier est telle que $1 \le k \le p - 1$.
k est un entier avec ; $\binom{p}{k} = \dfrac{p\,(p-1)\ldots(p-k+1)}{k\,!}$
donc $k\,!\binom{p}{k} = p\,(p-1)\ldots(p-k+1)$ donc p divise $k\,!\binom{p}{k}$.
Or p est un nombre premier, dont il est premier avec tous les entiers naturels qui lui sont inférieurs en particulier avec k !
On en déduit, d'après le théorème de Gauss, que p divise $\binom{p}{k}$.
On vient de prouver que : pour tout entier naturel k tel que
$1 \le k \le p - 1$, $\binom{p}{k} \equiv 0 \quad [p]$.
$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ldots + \binom{p}{p-1} a + 1$$
donc $(a+1)^p \equiv a^p + 1 \quad [p]$

Démontrons par récurrence sur a que : $a^p \equiv a \quad [p]$.
On vérifie que la propriété est vraie au rang 0 :
$p > 0$ donc $0^p = 0$ donc $0^p \equiv 0\ [p]$
On vérifie que la propriété est héréditaire.
Montrons que pour tout a de $\mathbb{N}$, si la propriété est vraie pour un certain a ; alors elle est vraie pour $a + 1$

La propriété est vraie pour un certain a on a donc : $a^p \equiv a\ [p]$.
Or on a démontré à l'étape précédente que :
$$(a+1)^p \equiv a^p + 1\ [p]$$
en utilisant l'hypothèse de récurrence, on obtient :
$$(a+1)^p \equiv a + 1\ [p]$$
la propriété est donc vraie au rang $n + 1$.

Conclusion : Si p est un nombre premier, pour tout entier naturel a, $a^p \equiv a\ [p]$ ou encore $a^p - a$ est un multiple de p.
Si p ne divise pas a, p étant un nombre premier, il est premier avec a.
p divise $a^p - a = a\,(a^{p-1} - 1)$, donc d'après le théorème de Gauss p divise $a^{p-1} - 1$, soit : $a^{p-1} \equiv 1\ [p]$.

Applications :
Etudier les restes de la division euclidienne de 12^n par un nombre premier 5.
5 est un nombre premier, et 5 ne divise pas 12 alors d'après le petit théorème de Fermat : $12^{5-1} \equiv 1\ [5]$ soit $12^4 \equiv 1\ [5]$
Or pour tout entier naturel k, $(12^4)^k = 12^{4k}$
donc $12^{4k} \equiv 1\ [5]$, il s'ensuit donc que pour tout entier r : $12^{4k+r} \equiv 12^r\ [5]$
il suffit donc de réaliser une étude de cas suivant le reste de la division euclidienne de n par 4.

Si $n = 4k$, (où $k \in \mathbb{N}$) alors $12^n = 12^{4k}$ or $12^{4k} \equiv 1$ [5] donc $12^n \equiv 1$ [5]

Si $n = 4k + 1$, (où $k \in \mathbb{N}$) alors $12^n = 12^{4k+1}$
or $12^{4k+1} \equiv 12$ [5] et $12 \equiv 2$ [5] donc $12^n \equiv 2$ [5]

Si $n = 4k + 2$, (où $k \in \mathbb{N}$) alors $12^n = 12^{4k+2}$
or $12^{4k+2} \equiv 12^2$ [5] et $12^2 \equiv 4$ [5] donc $12^n \equiv 4$ [5]

Si $n = 4k + 3$, (où $k \in \mathbb{N}$) alors $12\ n = 12\ 4k + 3$
or $12\ 4k + 3$ ($12\ 3$ [5] et $12\ 3$ (3 [5] donc $12\ n$ (3 [5]
Dans une division euclidienne par 4, les restes possibles sont 0, 1, 2 ou 3. Tous les cas ont donc été envisagés.

PPCM

Propriété : soit a et b deux entiers relatifs non nuls.
L'ensemble des multiples strictement positifs communs à a et b admet un plus petit élément M. On note M = PPCM(a ; b).

Démonstration :
L'ensemble des multiples strictement positifs communs à a et b et non vide : il contient $|a|\,|b|$.

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément, donc

l'ensemble des multiples strictement positifs communs à a et b admet un plus petit élément M.

Exemple
les multiples strictement positifs de 24 sont : 24, 48, 72, 96, ...
Les multiples strictement positifs de 16 sont : 16, 32, 48, 64, ...
Donc PPCM(24 ; 16) = 48.

Remarque :
Deux entiers opposés ont les mêmes multiples donc
PPCM(a ; b) = PPCM($-a$; b) = PPCM(a ; $-b$)
et PPCM(a ; b) = PPCM($-a$; $-b$)

Propriété : soit a et b deux entiers relatifs non nuls.
1. PGCD(a ; b) × PPCM(a ; b) = $|a\,b|$
2. L'ensemble des multiples communs à a et b est l'ensemble des multiples de leur PPCM.
3. Soit k un entier relatif non nul, PPCM($k\,a$; $k\,b$) = $|k|$ PPCM(a ; b)

Démonstration :
1. Soit a et b deux entiers relatifs
d est leur PGCD donc il existe deux entiers relatifs a' et b' tels que $a = d\,a'$, $b = d\,b'$ et PGCD(a' ; b') = 1
Soit m un multiple commun à a et b, il existe deux entiers relatifs x et y tels que $m = a\,x = b\,y$
donc $m = d\,a'\,x = d\,b'\,y$ donc $a'\,x = b'\,y$ donc a' divise $b'\,y$
or PGCD(a' ; b') = 1 donc, d'après le théorème de Gauss, a' divise y, il existe donc un entier relatif n tel que $y = a'n$
donc $m = d\,a'\,b'\,n$
Les multiples positifs communs à a et b sont donc les entiers de la forme : $|a'\,b'|\,d\,n$ lorsque $n \in \mathbb{N}^*$.

PPCM(a ; b) est le plus petit élément de l'ensemble des multiples strictement positifs communs à a et b, donc PPCM(a ; b) est obtenu pour $n = 1$
soit PPCM(a ; b) = $|a'\,b'|\,d = |d\,a'\,b'| = |a\,b'|$
PGCD(a ; b) × PPCM(a ; b) = $d\,|a\,b'| = |a\,d\,b'| = |a\,b|$

2. Les multiples positifs communs à a et b sont donc les entiers de la forme : $|a'\,b'|\,d\,n$ lorsque n ($\mathbb{N}^*$ donc de la forme n PPCM (a ; b)
L'ensemble des multiples communs à a et b est l'ensemble des multiples de leur PPCM.

3. Soit k un entier relatif non nul,
PGCD($k\,a$; $k\,b$) × PPCM($k\,a$; $k\,b$) = $|k\,a\,k\,b| = |k|^2\,|a\,b|$
$|k|$ PGCD(a ; b) × PPCM($k\,a$; $k\,b$) = $|k|^2$ PGCD(a ; b) × PPCM(a ; b)
$k \neq 0$ et PGCD(a ; b) $\neq 0$ donc PPCM($k\,a$; $k\,b$) = $|k|$ PPCM(a ; b)

Applications :
Calculer PPCM(a ; b) connaissant PGCD(a ; b)

Résoudre certaines équations :
Déterminer tous les entiers naturels non nuls a et b ($a > b$) tels que :
2 PGCD(a ; b) + PPCM(a ; b) = 38
Soit a et b deux entiers naturels non nuls
d est leur PGCD donc il existe deux entiers relatifs a' et b' tels que $a = d\,a'$, $b = d\,b'$ et PGCD(a' ; b') = 1
Soit m = PPCM(a ; b)
PGCD(a ; b) × PPCM(a ; b) = $a\,b$ donc $m = d\,a'\,b'$
en remplaçant dans l'équation : d ($2 + a'\,b'$) = 38 donc d divise 38

Les diviseurs de 38 sont 1 ; 2 ; 19 ; 38
si d = 1 alors $2 + a'\,b' = 38$ donc $a'\,b' = 36$ d'où les possibilités :

$a = a'$	1	~~2~~	~~3~~	4	~~6~~	9	~~12~~	~~18~~	36
$b = b'$	36	~~18~~	~~12~~	9	~~6~~	4	~~3~~	~~2~~	1

Les cases rayées ne conviennent pas car les nombres ne sont pas premiers entre eux
$a > b$ donc les seules solutions sont les couples :
(a ; b) = (36 ; 1) ou (a ; b) = (9 ; 4)
Si d = 2 alors $2 + a'\,b' = 19$ donc $a'\,b' = 17$ d'où les possibilités :

a'	1	17
b'	17	1

$a = 2\,a'$	34	2
$b = 2\,b'$	2	34

$a > b$ donc la seule solution est le couple (a ; b) = (34 ; 2)
si d = 19 alors $2 + a'\,b' = 2$ donc $a'\,b' = 0$ ce qui est impossibles a et b n'étant pas nuls
si d = 38 alors $2 + a'\,b' = 1$ donc $a'\,b' = -1$ ce qui est impossibles a et b étant positifs.
Les seules solutions sont les couples :
(36 ; 1) ou (34 ; 2) ou (9 ; 4)

Propriété : Le PPCM de deux entiers non nuls est égal au produit de leurs diviseurs premiers apparaissant dans au moins une des
décompositions en produit de facteurs premiers, chacun d'eux étant affecté de son plus grand exposant.

Démonstration :
Soit $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots p_k^{\beta_k}$ où,
pour tout i compris entre 1 et k : p_i est un nombre premier qui apparait dans la décomposition en produit de facteurs premiers soit de a soit de b
α_i et β_i sont des entiers éventuellement nuls,

$\alpha_i = 0$ (respectivement $\beta_i = 0$) si p_i n'apparaît pas dans la décomposition en produit de facteurs premiers de a (resp. b)

PGCD (a ; b) = $p_1^{d_1} \times p_2^{d_2} \times \ldots p_k^{d_k}$ où d_i est le plus petit des entiers α_i et β_i

PGCD(a ; b) × PPCM(a ; b) = $a\,b$

donc PPCM(a ; b) = $\dfrac{p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots p_k^{\alpha_k} \times p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots p_k^{\beta_k}}{p_1^{d_1} \times p_2^{d_2} \times \ldots p_k^{d_k}}$

or d_i est égal soit à α_i soit à β_i donc $\alpha_i + \beta_i = d_i + m_i$

d_i est le plus petit des entiers α_i et β_i et m_i est le plus grand des entiers α_i et β_i, après simplification on obtient donc que

PPCM(a ; b) = $p_1^{m_1} \times p_2^{m_2} \times \ldots p_k^{m_k}$

Exemple :

$116\,375 = 5^3 \times 7^2 \times 19$

$410\,571 = 3^2 \times 7^4 \times 19$

donc PPCM(116 375 ; 410 571) = $3^2 \times 5^3 \times 7^4 \times 19$ = 51 321 375