1 Divisibilité, nombres premiers, division euclidienne et congruences

DIVISIBILITÉ DANS Z

Définition

Soient a et b deux entiers relatifs. On dit que a divise b (ou que a est un diviseur de b, ou que b est un multiple de a) lorsqu'il existe un entier k tel que $b = ka$ (a divise b se note alors a / b).

Exemples

15 divise 45 puisque : $45 = 3 \times 15$.

48 est un multiple de 12 puisque : $48 = 4 \times 12$.

Propriétés

1. $a / b \Leftrightarrow -a / b \Leftrightarrow -a / -b \Leftrightarrow a / -b$.

2. Tout diviseur positif a de b (avec $b \geq 0$) vérifie : $1 \leq a \leq b$.

3. Tout entier positif (non nul) a un nombre fini de diviseurs.

Exemple

1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60 sont les diviseurs positifs de 60 (il en possède douze).

Propriétés

Si a / b et b / c alors a / c.

Si a / b et a / c alors $a / (bu + cv)$ pour tous entiers u et v (et en particulier : $a / b + c$ et $a / b - c$).

Exemples

15 divise 30 et 30 divise 120 donc 15 divise 120.

12 divise 24 et 12 divise 60 donc 12 divise 228 (puisque $228 = 2 \times 24 + 3 \times 60$).

NOMBRES PREMIERS

Définition

Soit p un entier strictement positif. On dit que p est premier lorsqu'il ne possède que deux diviseurs : 1 et lui-même (c'est-à-dire p).

Exemples

2, 3, 5, 7, 11, 13, 19, 23, 29 sont tous des nombres premiers (2 est le seul nombre premier pair). Attention : l'entier 1 n'est pas un nombre premier !

Définition
Un nombre strictement positif, différent de 1, qui n'est pas premier est dit composé.

Théorème fondamental de l'Arithmétique
Tout nombre entier supérieur strictement à 1 admet au moins un diviseur premier.

Propriétés
1. Tout nombre composé n admet un diviseur premier inférieur ou égal à $\sqrt{n}$.

2. Si aucun des entiers compris entre 2 et $\sqrt{n}$ ne divise n, alors n est premier.

L'algorithme qui teste si un nombre est premier

L'algorithme ci-dessous permet de tester si un entier est premier. Il utilise la propriété précédente (propriété **2.**).

```
VARIABLES
    n EST_DU_TYPE NOMBRE
    k EST_DU_TYPE NOMBRE
    Premier EST_DU_TYPE CHAINE
DEBUT_ALGORITHME
    LIRE n
    k PREND_LA_VALEUR 1
    Premier PREND_LA_VALEUR "Vrai"
    TANT_QUE (k<=sqrt(n) ET Premier!="Faux") FAIRE
        DEBUT_TANT_QUE
        k PREND_LA_VALEUR k+1
        SI (n%k==0) ALORS
            DEBUT_SI
            Premier PREND_LA_VALEUR "Faux"
            AFFICHER n
            AFFICHER " est divisible par : "
            AFFICHER k
            FIN_SI
        FIN_TANT_QUE
    SI (Premier=="Vrai") ALORS
        DEBUT_SI
        AFFICHER n
        AFFICHER " est premier."
        FIN_SI
FIN_ALGORITHME
```

Propriété
Il y a une infinité de nombres premiers (Euclide (325-265 av. J.-C.)).

Théorème de décomposition en facteurs premiers
Tout entier n strictement supérieur à 2 se décompose de manière unique (à l'ordre près) en produit de facteurs premiers, c'est-à-dire que pour tout

n, il existe des nombres premiers p_1, p_2, … p_r et des entiers non nuls k_1, k_2, … k_r tels que $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$.

Exemples

1. On a : $360 = 2^3 \times 3^2 \times 5$.

2. On a : $952560 = 2^4 \times 3^5 \times 5 \times 7^2$.

Remarques

1. Pour trouver la décomposition en facteurs premiers d'un entier, on divise autant de fois qu'il est possible par 2, puis par 3, 5, 7, etc.

2. L'instruction ifactor() (sous Xcas) permet d'obtenir la décomposition en facteurs premiers d'un entier.

Propriété

a divise b si et seulement si les facteurs premiers intervenant dans la décomposition de a interviennent dans la décomposition de b avec un exposant inférieur. Ainsi tous les diviseurs de l'entier $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ sont de la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$,

avec $0 \le \alpha_1 \le k_1$, $0 \le \alpha_2 \le k_2$, $0 \le \alpha_r \le k_r$.

Exemples

1. $60 = 2^2 \times 3 \times 5$ divise $9000 = 2^3 \times 3^2 \times 5^3$.

2. $252 = 2^2 \times 3^2 \times 7$ divise $952560 = 2^4 \times 3^5 \times 5 \times 7^2$.

Propriété

Le nombre de diviseurs positifs de l'entier $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ est égal au produit $(k_1 + 1)(k_2 + 1)...(k_r + 1)$.

Exemple

$60 = 2^2 \times 3 \times 5$ possède $(2+1)(1+1)(1+1) = 3 \times 2 \times 2 = 12$ diviseurs strictement positifs (c'est vrai, on l'a déjà vu, il s'agit de : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60).

DIVISION EUCLIDIENNE

Définition (dans N)

Soient a et b deux entiers positifs $(b \neq 0)$. Il existe un unique entier q (quotient) positif et un unique entier r (reste) positif vérifiant $a = bq + r$ et $0 \le r < b$. Effectuer la division euclidienne de a par b consiste à trouver ces nombres q et r. q s'appelle le quotient et r le reste dans la division euclidienne de a par b.

Exemple

La division euclidienne de :

$a = 57$ par $b = 15$ donne : $57 = 15 \times 3 + 12$ ($q = 3$ et $r = 12$).

$a = 349$ par $b = 25$ donne : $349 = 25 \times 13 + 24$ ($q = 13$ et $r = 24$).

Remarque

L'instruction iquorem() (sous Xcas) permet d'avoir le quotient q et le reste r d'une division euclidienne.

```
iquorem(57,15)
                    [3, 12]
```

Propriété

Dans la division euclidienne $a = bq + r$, on a : $q = E\left(\frac{a}{b}\right)$ où E désigne la partie entière (« floor » sous Algobox) et $r = a - bq$.

Algorithme de la division euclidienne

Voici l'algorithme de division euclidienne (dans N) de a par b :

```
VARIABLES
  a EST_DU_TYPE NOMBRE
  b EST_DU_TYPE NOMBRE
  q EST_DU_TYPE NOMBRE
  r EST_DU_TYPE NOMBRE
DEBUT_ALGORITHME
  LIRE a
  LIRE b
  q PREND_LA_VALEUR floor(a/b)
  r PREND_LA_VALEUR a-b*q
  AFFICHER a
  AFFICHER " = "
  AFFICHER b
  AFFICHER "*"
  AFFICHER q
  AFFICHER "+"
  AFFICHER r
FIN_ALGORITHME
```

Définition (dans Z)

Soient a et b deux entiers relatifs $(b \neq 0)$. Il existe un unique entier q relatif et un unique entier r positif vérifiant : $a = bq + r$ et $0 \leq r < |b|$.

Exemples

La division euclidienne de :

$a = -49$ par $b = -4$ donne : $-49 = -4 \times 13 + 3$ ($q = 13$ et $r = 3$).

$a = -28$ par $b = 3$ donne : $-28 = 3 \times (-10) + 2$ ($q = -10$ et $r = 2$).

$a = 34$ par $b = -5$ donne : $34 = -5 \times (-6) + 4$ ($q = -6$ et $r = 4$).

Propriété

$b / a \Leftrightarrow r = 0$ (dans la division euclidienne $a = bq + r$).

Propriétés

Parmi k entiers consécutifs, l'un est multiple de k. Plus précisément,

1. L'un des 2 entiers (consécutifs) n ou $n+1$ est divisible par 2.

2. L'un des 3 entiers (consécutifs) n, $n+1$, $n+2$ est divisible par 3.

3. L'un des 4 entiers (consécutifs) n, $n+1$, $n+2$, $n+3$ est divisible par 4. Etc.

Propriétés

1. Tout entier n est nécessairement de la forme $2k$ ou $2k+1$, avec k entier.

2. Tout entier n est nécessairement de la forme $3k$ ou $3k+1$ ou $3k+2$, avec k entier

3. Tout entier n est nécessairement de la forme $4k$ ou $4k+1$ ou $4k+2$, ou $4k+3$, avec k entier. Etc.

CONGRUENCES

Définition

Soient a et b deux entiers relatifs et n un entier strictement positif. On dit que a est congru à b modulo n lorsque $a-b$ est un multiple de n (ou lorsque n divise $a-b$).

Notation

Lorsque a est congru à b modulo n, on écrit : $a \equiv b[n]$.

Exemples

$5 \equiv 1[2]$ car $5-1$ est un multiple de 2.

$16 \equiv 1[3]$ car $16-1$ est un multiple de 3.

De même $17 \equiv 1[4]$, $60 \equiv 0[4]$, $81 \equiv 1[4]$, $15 \equiv 0[5]$, $17 \equiv 2[5]$, $25 \equiv 1[6]$, $35 \equiv 5[6]$, $27 \equiv 6[7]$, $49 \equiv 0[7]$, $73 \equiv 3[7]$, $155 \equiv 11[12]$, etc.

Propriété

Modulo n, a est toujours congru à son reste r dans la division euclidienne de a par n.

Exemples

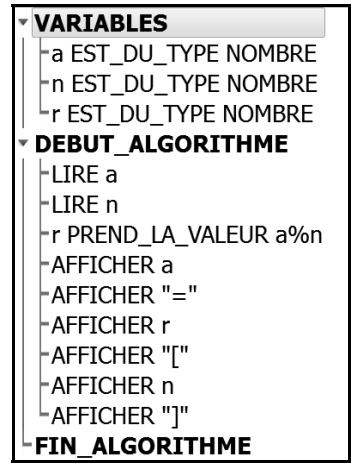
1. $17 = 5 \times 3 + 2$ donc : $17 \equiv 2[5]$.

2. $255 = 7 \times 36 + 3$ donc : $255 \equiv 3[7]$.

3. $1079 = 11 \times 98 + 1$ donc : $1079 \equiv 1[11]$.

4. $42 = 14 \times 3 + 0$ donc : $42 \equiv 0[14]$ (14 divise 42).

Algorithme (calculant le reste modulo n d'un entier a)
L'algorithme suivant calcule le reste r modulo n d'un entier a (positif). On utilise a%n, qui désigne le reste modulo n de l'entier a.



Propriétés

Soit n un entier strictement positif.

1. $a \equiv a\left[n\right]$.

2. Si $a \equiv b\left[n\right]$ et $b \equiv c\left[n\right]$ alors $a \equiv c\left[n\right]$.

3. $a \equiv 0\left[n\right] \Leftrightarrow n / a$.

4. Si $a \equiv b\left[n\right]$ et $a' \equiv b'\left[n\right]$ alors $a + a' \equiv b + b'\left[n\right]$.

5. Si $a \equiv b\left[n\right]$ alors pour tout entier k, $ka \equiv kb\left[n\right]$.

6. Si $a \equiv b\left[n\right]$ et $a' \equiv b'\left[n\right]$ alors $a \times a' \equiv b \times b'\left[n\right]$.

7. Si $a \equiv b\left[n\right]$, alors pour tout entier p de N, $a^p \equiv b^p\left[n\right]$.

Exemple

$5 \equiv 1\left[4\right]$ donc pour tout entier $n \geq 0$, $5^n \equiv 1^n \equiv 1\left[4\right] \Leftrightarrow 5^n - 1 \equiv 0\left[4\right]$.

Ainsi pour tout entier $n \geq 0$, 4 divise $5^n - 1$.

Propriétés (critères de divisibilité)

Les critères qui suivent sont des applications directes des congruences :

1. Un entier est pair si son chiffre des unités est pair (comme 28 ou 300).

2. Un entier est divisible par 3 si la somme de ses chiffres l'est (comme 627).

3. Un entier est divisible par 4 si ses deux derniers chiffres forment un entier qui l'est (comme 31**32**).

4. Un entier est divisible par 5 si son chiffre des unités est 0 ou 5 (comme 70 ou 155).

5. Un entier est divisible par 9 si la somme de ses chiffres l'est (comme 927).

Raisonnement par disjonction de cas

Les congruences permettent ce type de raisonnement car si x est un entier, alors modulo 2 on a $x \equiv 0[2]$ et $x \equiv 1[2]$.

Modulo 3, on a $x \equiv 0[3]$, $x \equiv 1[3]$, $x \equiv 2[3]$. Etc. Ces congruences réduisant fortement le nombre de cas à étudier sont particulièrement utiles dans l'étude de certaines équations diophantiennes.

Exemple

L'équation diophantienne $x^2 - 3y^2 = 2$ n'admet pas de couples-solutions. Démontrons-le par l'absurde : supposons qu'il y en ait un notée (x_0, y_0). Alors on aurait $x_0^2 - 3y_0^2 = 2$, ce qui modulo 3 donne $x_0^2 - 3y_0^2 \equiv 2[3]$ soit $x_0^2 \equiv 2[3]$. Mais pour tout entier x, modulo 3, on a :

– soit $x \equiv 0[3]$ (qui donne $x^2 \equiv 0[3]$), soit $x \equiv 1[3]$ (qui donne $x^2 \equiv 1^2 \equiv 1[3]$),

– soit $x \equiv 2[3]$ (qui donne $x^2 \equiv 4 \equiv 1[3]$).

On voit par disjonction de cas (3 cas en tout), que l'égalité $x_0^2 \equiv 2[3]$ est impossible. Contradiction ! Conclusion : l'équation $x^2 - 3y^2 = 2$ n'admet pas de solutions entières.

✸ Exercice 1

10 min

1. Montrer que si a divise b et b divise c, alors a divise c.
2. Montrer que si d divise e et d divise f, alors d divise $e + f$.
3. Montrer que si un nombre premier p divise un autre nombre premier q, alors $p = q$.

✸✸ Exercice 2

30 min

1. a) Vérifier à l'aide d'un algorithme que la somme de trois entiers consécutifs strictement positifs est toujours divisible par 3 (on étudiera les mille premiers cas).
b) Démontrer algébriquement ce résultat.
2. a) Vérifier à l'aide d'un algorithme que la somme de trois cubes d'entiers consécutifs strictement positifs est toujours divisible par 9 (on étudiera les mille premier cas).
b) Démontrer algébriquement ce résultat.

✸✸ Exercice 3

10 min

Esprit ROC : Démontrer que si $a \equiv b\left[n\right]$ alors $a^p \equiv b^p\left[n\right]$ pour tout entier p strictement positif. (On effectuera un raisonnement par récurrence sur p.)

✸✸ Exercice 4

30 min

Dans l'annexe du *Traité du triangle arithmétique* de Blaise Pascal (1623-1662), on trouve la règle suivante : *« Pour qu'un nombre soit divisible par 8, il faut et il suffit que la somme formée du chiffre des unités, du double de celui des dizaines et du quadruple de celui des centaines soit multiple de 8 ».*

Démontrer ce résultat énoncé par Blaise Pascal (on pourra utiliser les congruences).

✸✸ Exercice 5

30 min

1. Rechercher à l'aide d'un algorithme, des couples (x, y) de solutions entières positives de l'équation : $2yx = 21 + x^2$.

2. Résoudre algébriquement, pour x et y entiers positifs, cette équation (on utilisera les factorisations possibles de 21 en produit de deux entiers positifs).

✸✸ Exercice 6

30 min

1. Écrire un algorithme permettant la recherche de solutions entières positives de l'équation $4y^2 = x^2 + 12$.

2. Résoudre algébriquement cette équation. (on utilisera les factorisations possibles de 12 en produit de deux entiers positifs).

✸✸ Exercice 7

10 min

Démontrer que $492^{2015} + 1048^{2015}$ est divisible par 7 (on pourra utiliser les congruences modulo 7).