1
Divisibilité, nombres premiers, division euclidienne, congruences

1. DIVISIBILITE

1.1. Diviseur

Définition

Soient a et b (b non nul) deux entiers. S'il existe un entier k tel que $b = ka$, alors on dit que a divise b (ou que a est un diviseur de b, ou encore que b est un multiple de a).

Exemples

- 4 est un diviseur de 12 (ou 12 est un multiple de 4) puisque : $12 = 3 \times 4$.
- 8 est un diviseur de 72 (puisque : $72 = 9 \times 8$).
- -12 est un diviseur de 48 (puisque : $48 = -4 \times (-12)$).

✍ Exercice d'application 1

1. Déterminer tous les diviseurs positifs de 60.
2. Déterminer la forme des multiples de 2.
3. Démontrer que pour tout entier n, $n(n+1)$ est divisible par 2.

Corrigé

1. On en trouve douze, à savoir : 1, 2, 3, 4, 5, 6, 10, 12,15, 20, 30, 60.
2. L'ensemble des multiples de 2 (c'est-à-dire des nombres pairs) sont les nombres de la forme $2k$ avec k entier.
3. 1er cas : supposons que n soit pair, alors n s'écrit sous la forme $n = 2k$ et on a $n(n+1) = 2k(2k+1)$ ce qui montre que 2 divise $n(n+1)$.
2e cas : supposons que n soit impair, alors $n+1$ est pair donc s'écrit sous la forme $n+1 = 2q$ et $n(n+1) = (2q-1)2q = 2q(2q-1)$ ce qui montre que 2 divise $n(n+1)$.

✍ Exercice d'application 2

Démontrer que pour tout entier n, 4 divise $(2n+1)^2 - 21$.

Corrigé

Pour tout n, $(2n+1)^2 - 21 = 4n^2 + 4n + 1 - 21 = 4n^2 + 4n - 20 = 4(n^2 + n - 5)$
Donc 4 divise $(2n+1)^2 - 21$.

✍ Exercice d'application 3

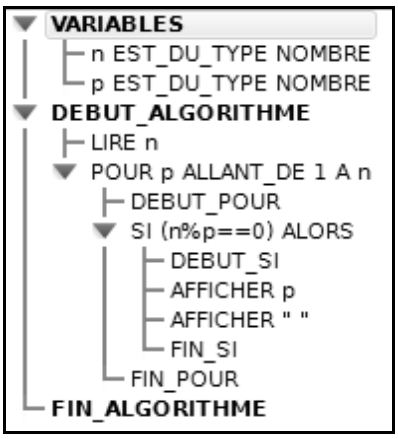
1. Ecrire un algorithme qui affiche la liste des diviseurs strictement positifs d'un entier positif donné n. (indication : avec Algobox, pour savoir si p est un diviseur d'un entier n, on utilise le test : n%p==0, si n%p==0 alors p divise n).

2. Modifier cet algorithme de manière à ce qu'il affiche le nombre de diviseurs strictement positifs d'un entier donné n.

3. Déterminer le nombre de diviseurs de 12, puis le nombre de diviseurs de 60 et de 360.

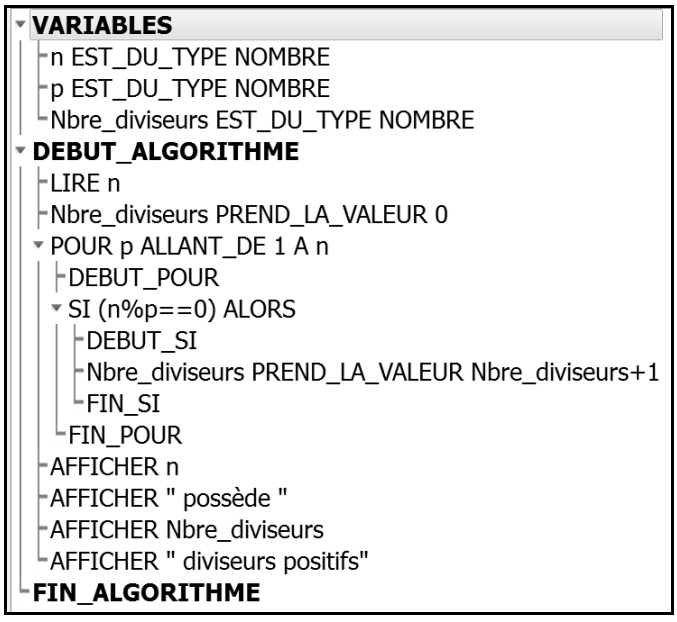
Corrigé

1. L'idée est d'utiliser une boucle « pour », combinée avec le test n%p==0 :



Par exemple, pour $n = 12$, l'algorithme nous affiche : 1, 2, 3, 4, 6, 12.

2. On va utiliser un compteur (Nbre_diviseurs), qui augmentera de 1 à chaque fois que la condition « SI » décèle un nouveau diviseur de n :



3. Si on fait fonctionner l'algorithme pour $n = 12$, ce dernier nous annonce 6 diviseurs positifs. Pour $n = 60$, il nous en annonce 12 et pour $n = 360$, il nous en annonce 24 !

Remarque

360 (comme 60 et 12) possède beaucoup de diviseurs (bien plus que 10, 20 et 100), c'est probablement la raison pour laquelle les mésopotamiens (dont l'activité scientifique connut un essor important vers 2250 av. J.-C.) avaient adopté ce système à base 12, (qu'on retrouve encore aujourd'hui dans la douzaine d'œufs ou dans les heures de chaque demi-journée), 60 (qu'on retrouve dans les minutes et les secondes) et 360 (qu'on retrouve dans les mesures d'angles en degrés) et qu'ils nous ont légués ! Avoir autant de diviseurs rend les divisions, les partages plus faciles : c'est très commode pour le commerce, la comptabilité, les sciences, etc.

✍ Exercice d'application 4

Soit q un entier impair. Démontrer que la somme de q entiers consécutifs est toujours divisible par q.

Corrigé

Puisque q est impair, on peut l'écrire sous la forme $q = 2k + 1$ (avec k entier).

On a $q = 2k + 1$ entiers consécutifs, appelons **n** celui qui se trouve au **centre**. Comme il y a k entiers à droite (et autant à gauche) de n, on peut donc tous les écrire sous la forme : $n - k$, $n - (k - 1)$, $n - (k - 2)$, …, $n - 2$, $n - 1$, **n**, $n + 1$, $n + 2$, …, $n + (k - 2)$, $n + (k - 1)$, $n + k$.

Déterminons leur somme S, en l'écrivant deux fois : une fois à l'endroit et une fois à l'envers puis en les ajoutant (comme l'a fait Gauss, voir programme de 1re S), on a :

$S = n - k + n - (k - 1) + ... + n + ... + n + (k - 1) + n + k$

$S = n + k + n + (k - 1) + ... + n + ... + n - (k - 1) + n - k$

Ce qui nous donne : $2S = 2n + 2n + ... + 2n + ... + 2n + 2n$

Soit : $S = \underbrace{n + n + ... + n + ... + n + n}_{2k+1 \text{ fois}}$

Soit : $S = n(2k + 1)$ soit : $S = nq$, ce qui montre que q divise S.

✍ Exercice d'application 5

1. Démontrer l'égalité $q^{n+1} - 1 = \left(1 + q + q^2 + ... + q^n\right)\left(q - 1\right)$ (E) (si $q \neq 1$).

2. Soit a un entier différent de 1.

a) Démontrer que $a^{18} - 1$ est divisible par $a - 1$.

b) Démontrer que $a^{18} - 1$ est divisible par $a^2 - 1$.

c) Démontrer que $a^{18} - 1$ est divisible par $a^6 - 1$.

3. Soit a un entier différent de 1, n un entier supérieur ou égal à 1, et d un diviseur de n. Démontrer que $a^n - 1$ est divisible par $a^d - 1$.

Corrigé

1. D'après le cours de 1re S sur les suites géométriques, on a :

$1 + q + q^2 + ... + q^n = \dfrac{1 - q^{n+1}}{1 - q}$ (si $q \neq 1$) soit (après produit en croix) :

$1 - q^{n+1} = \left(1 + q + q^2 + ... + q^n\right)\left(1 - q\right)$ soit :

$$q^{n+1} - 1 = \left(1 + q + q^2 + ... + q^n\right)\left(q - 1\right) \text{ (E)}$$

2. a) En appliquant l'égalité (E) à $q = a$ et $n = 17$, on obtient : $a^{18} - 1 = \left(1 + a + a^2 + ... + a^{17}\right)\left(a - 1\right)$, ce qui montre que $a^{18} - 1$ est divisible par $a - 1$.

b) On a : $a^{18} - 1 = \left(a^2\right)^9 - 1$. Or en appliquant l'égalité (E) à $q = a^2$ et $n = 8$, on obtient :

$\left(a^2\right)^9 - 1 = \left(1 + a^2 + \left(a^2\right)^2 + ... + \left(a^2\right)^8\right)\left(a^2 - 1\right)$ soit :

$a^{18} - 1 = \left(1 + a^2 + a^4 + ... + a^{16}\right)\left(a^2 - 1\right)$

ce qui montre que $a^{18} - 1$ est divisible par $a^2 - 1$.

c) On a : $a^{18} - 1 = \left(a^6\right)^3 - 1$. Or en appliquant l'égalité (E) à $q = a^6$ et $n = 2$, on obtient : $\left(a^6\right)^3 - 1 = \left(1 + a^6 + \left(a^6\right)^2\right)\left(a^6 - 1\right)$ soit :

$a^{18} - 1 = \left(1 + a^6 + a^{12}\right)\left(a^6 - 1\right)$

ce qui montre que $a^{18} - 1$ est divisible par $a^6 - 1$.

3. On a $q^{n+1} - 1 = \left(1 + q + q^2 + ... + q^n\right)(q - 1)$ (E) (valable pour tout n) donc aussi l'égalité : $q^k - 1 = \left(1 + q + q^2 + ... + q^{k-1}\right)(q - 1)$ (F).

Comme d divise n, il existe k tel que $n = kd$ et donc $a^n = a^{kd} = \left(a^d\right)^k$, on a donc , en utilisant l'égalité (F) avec $q = a^d$:

$\left(a^d\right)^k - 1 = \left(1 + a^d + \left(a^d\right)^2 + ... + \left(a^d\right)^{k-1}\right)\left(a^d - 1\right)$ soit :

$a^n - 1 = \left(1 + a^d + a^{2d} + ... + a^{(k-1)d}\right)\left(a^d - 1\right)$.

Cette dernière égalité prouve que $a^n - 1$ est divisible par $a^d - 1$.

1.2. Propriétés de la divisibilité

Notation

a divise b se note plus simplement : a / b.

Propriété

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

Théorème

1. Soit b un entier positif. Si a est positif et divise b, alors $1 \leq a \leq b$.
2. Un entier positif (non nul) admet un nombre fini de diviseurs.

Théorème (dit des combinaisons linéaires)

Si a divise b et si a divise c alors :

- a divise $b + c$.
- a divise $b - c$.
- a divise toute combinaison linéaire $k_1 b + k_2 c$ pour tous entiers k_1 et k_2.

Exemple

4 divise 12 et 4 divise 16 donc 4 divise $5 \times 12 + 2 \times 16 = 92$.

Théorème (dit de transitivité)

Si a divise b et que b divise c alors a divise c.

Exemples

- 16 divise 80 et 80 divise 2400 donc 16 divise 2400.
- 6 divise 12, 12 divise 120, 120 divise 480, 480 divise 4800 donc 6 divise 4800.

- Tous les multiples de 4 sont des multiples de 2 puisque 2 divise 4.

2. NOMBRES PREMIERS

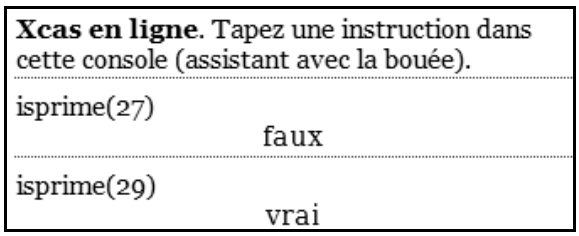
2.1. Définitions

Définition

Un entier strictement positif p est premier lorsqu'il admet exactement deux diviseurs entiers positifs distincts : 1 et p (c'est-à-dire 1 et lui-même).

Remarques

- 1 n'est pas premier (ne faites jamais cette erreur) car 1 n'admet qu'un seul diviseur : lui-même. 2 est le seul nombre premier qui soit pair. Ensuite, les nombres premiers sont 3, 5, 7, 11, 13, 17, 19, 23, etc.
- Le logiciel de calcul formel Xcas sait très bien tester si un entier est premier ou non, grâce à l'instruction isprime()



- Il y a une infinité de nombres premiers, et ça c'est Euclide (325-265 av. J.-C.) qui l'a démontré ! C'est même un très bel exemple de raisonnement par l'absurde qu'on vous invite à aller voir dans le Devoir 2.

✍ Exercice d'application 6

Démontrer que 3 est le seul nombre premier de la forme $n^2 - 1$.

Corrigé

- Donnons le début de la liste des entiers de la forme $n^2 - 1$ pour $n \geq 0$: -1, 0, 3 (premier), 8 (non premier), 15 (non premier), 24 (non premier), 35 (non premier), 48 (non premier)… Le résultat semble vrai, essayons de le prouver.
- On a l'identité remarquable $n^2 - 1 = (n-1)(n+1)$ qui montre que $n - 1$ est un diviseur de $n^2 - 1$. Intéressons-nous à ce diviseur : dès que $n > 2$, on a $n - 1 > 1$ et $n - 1 < n^2 - 1$ (car $n < n^2$ puisque $1 < n$).

Ainsi, dès que $n > 2$, $n^2 - 1$ possède un diviseur (à savoir : $n - 1$) différent de 1 et de lui-même. On en déduit que : si $n > 2$ alors $n^2 - 1$ n'est pas premier.

- Reste le cas $n = 1$ qui donne $n^2 - 1 = 3$ qui est bien premier.

Conclusion : 3 est le seul nombre premier de la forme $n^2 - 1$.

Définition

Un entier strictement supérieur à 1 qui n'est pas premier, est qualifié de nombre composé.

Théorème fondamental de l'Arithmétique

Tout entier strictement supérieur à 1 admet au moins un diviseur premier.

Théorème

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

Théorème

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