Chapitre 3: Arithmétique dans Z

1.1 Multiples et diviseurs d'un entier

Définition:

Soit a ∈ Z* et b ∈ Z.   On dit que a divise b et on écrit "alb", s'il existe k ∈ Z tel que b = ka. On dit aussi que b est un multiple de a.

Exemples:

3I12, 7|168

Remarques:

1. Pour tout a ∈ Z*, 1, -1, a et -a sont des diviseurs de a.
2. La relation "/" est une relation d'ordre non total dans N.

1.1.1 Propriétés

Soit a ∈ Z* , b,c ∈ Z.

1. Si a divise b et b divise a alors, a = ±b.
2. Si a divise b et a divise c alors a divise b + c.
3. Si a divise b et α divise β alors aα divise bβ.
4. Si a divise b alors a^n divise b^n où n ∈ N*.

Notation

On note par D(a), l'ensemble des diviseurs de a et par aZ l'ensemble d es multiples de a. Ainsi,

$$aZ = \{ ka, k \in Z\}$$

1.2 Division euclidienne dans Z

Théorème 1

Soit (a, b) ∈ Z^2 tel que b≠0.

Il existe un couple unique (q, r) ∈ Z^2, tel que

$$a = bq + r \text{ et } 0 \leq r \prec |b|$$

q est appelé quotient et r reste de la division de a par b.

Preuve

Existence : Premier cas : $b \in \mathbb{N}^*$. Pour $a \in \mathbb{Z}$, on pose $q = [\frac{a}{b}]$. On a,

$$q \leq \frac{a}{b} < q+1 \quad eq \quad qb \leq a < qb+b \quad eq \quad 0 \leq a-qb < b$$

On pose, $r = a - bq$. On a bien $0 \leq r < b$.

Deuxième cas : $b \in \mathbb{Z}_-$. On divise a par -b, on a d'après le premier cas,

$q = [\frac{a}{-b}]$ et $r = a - q(-b)$ vérifiant

$$0 \leq r < -b.$$

Unicité Supposons que $a = bq + r = bq' + r'$, avec $0 \leq r < |b|$ et $0 \leq r' < |b|$

On a $b(q - q') = r' - r$; $r' - r$ est donc un multiple de b. Comme il est strictement compris entre $-|b|$ et $|b|$, il ne peut être que nul. Donc $r' = r$ et par suite $q' = q$. Le couple (q, r) est donc unique.

Remarque : Il est immédiat que b divise a si, et seulement si, $r = 0$.

Exemple

1) Soit $a= -5$ et $b = 2$, on a:

$$-5 = (-3)(2) + 1,\ q = -3 \text{ et } r = 1.$$

2. Soit $a = -127$ et $b = -11$, on a,

$$-127 = -11(12) + 5.$$

1.3 Congruences

Définition 1: On dit que a et $b \in \mathbb{Z}$ sont congrus modulo $n \in \mathbb{N}^*$ et on écrit $a \equiv b(n)$ ou encore $a \equiv b[n]$ ssi $a - b$ est un multiple de n. Ainsi,

$$a \equiv b(\ n) \iff \exists k \in \mathbb{Z}^* ,\ a - b = kn$$

1.4. Diviseurs communs de deux entiers

Exemple 1: 3 ≡ 1(2), 25 ≡ 0(5), 31 ≡ 4(3).

Proposition 1: Soit n ∈ N* 1 a, b, c, d ∈ Z tels que u ≡ b(n) et c ≡ d(n) Alors a+ c ≡ b + d(n) et ac ≡ bd(n).
En particulier si a ≡ b(n) alors $a^m \equiv b^m$(n) pour tout m ∈ N.

Preuve: Soit k et k' ∈ Z tels que a = b + nk et c = d + nk' alors a + c = b + d + n(k + k') et ac = bd+ n(kd + k' b + nkk'). Ce qui prouve le résultat.

Proposition 2: La congruence modulo n est une relation d'équivalence sur Z.

Proposition 3: Soit R la relation congru mod n. La classe d'un entier a ∈ Z est la classe de son reste dans la division de a par n. et on note par

Z/nZ = $\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$

Exemple 2:

a,b ∈ Z
aRb <=> a≡b(3)
Déterminons la classe de a.
cl(a) = {b ∈ Z, b ≡ a(3)} = {b ∈ Z, b = a.+ 3k, k E Z} = {b = r + 3q, 0 ≤ r < 3} = cl(r)
Ainsi,
cl(0) = 3Z, cl(1) = 3Z + 1 et cl(2) = 3Z + 2.
cl(3) = cl(0) = cl(9) = cl(-3)
Z/3Z = $\{\overline{0},\overline{1},\overline{2}\}$

1.4 Diviseurs communs de deux entiers

Définition 2: Soit (a, b) ∈ Z^2 . On appelle plus grand commun diviseur du couple (a, b) et on note P.G.C.D. de a et b: noté encore a /\ b, tout entier d ∈ N vérifiant

1. d/a et d/b
2. Si δ / a et δ / b donc δ / d

Exemple 3: pgcd(21, 14) = 7, pgcd(12, 32) = 4
En particulier pgcd(a, 0) = |a|
Définition 3: Deux entiers a et b sont premiers entre eux si pgcd(a, b) = 1.

1.4.1 Algorithme d'euclide:

Proposition 4: Soit a, b ∈ N*. On a:
pgcd(a, b) = pgcd(b, r)
où r est le reste de la division de a par b.

Preuve: Si d/a et d/b alors d/a-bq = r. Ainsi, d/b et d/r donc d/pgcd(b, r) = δ. D'autre part, si δ/b et δ/r = a-bq alors δ/b et δ/a donc δ/d. En conclusion, d/δ et δ/d donc d = δ. ■
On peut supposer, sans nuire à la généralité, que a et b sont positifs.
De même on peut supposer, quitte à les échanger, que a > b. On a donc $0 \leq b \leq a$.
• Si b = 0, les diviseurs communs de a et b sont ceux de a. Ainsi,

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

• Si b > 0, effectuons la division euclidienne de a par b : a = bq + r avec $0 \leq r < b$.
On a,

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

• Si r= 0, on a donc

$$\text{pgcd}(b, r) = b$$

• Si r > 0, on divise b par r : b = $rq_1 + r_1$ avec $0 \leq r1 < r$ et on a
pgcd(a , b) = pgcd(b, r) = pgcd(r, r_1).
On peut poursuivre ce raisonnement tant que le reste obtenu est non nul :
pgcd(a,b) = pgcd(b,r) =pgcd(r,r_1) =pgcd (r_1, r_2)= … =pgcd(r_{k-1},r_k)
La suite (b,r,r_1, ... , r_k) est une suite d'entiers naturels strictement décroissante: elle est nécessairement finie. On aboutit donc en un nombre fini d'étapes à un reste nul. Supposons que $r_k \neq 0$ et r_{k+1}= 0; on a alors :
pgcd(a , b) = pgcd(b,r) =pgcd(r,r_1) =pgcd(r_1,r_2)= … = pgcd(r_{k-1},r_k) = pgcd(r_k,0)= r_k

r_k est un diviseur commun de a et b et tout diviseur commun de a et b est un diviseur de r_k. C'est le plus grand diviseur commun de a et b. On peut rassembler toutes ses opérations sur un tableau:

	q	q_1	q_2	$\ldots q_{k-1}$	q_k
a	b	r	r_1	$\ldots r_{k-1}$	r_k
r	r_1	r_2		$\ldots r_k$	0

Ainsi le P.G.C.D. de deux entiers non nuls est le dernier reste non nul de l' Algorithme d'Euclide.

Exemple

Calculons 9100 /\ 1848

	4	1	12	5	
9100	1848	1708	140	28	
1708	140	28	0		

Ainsi 9100 /\ 11848 = 28.

Théorème de Bezout:

Soit (a, b) ∈ Z^2. Ils existent (u, v) ∈ Z^2 tels que

$$au + bv = pgcd(a, b)$$

Preuve

L'algorithme d'Euclide nous permet d'obtenir u et v en remontant l'algorithme

Exemple:

A partir de l'exemple précédent, on peut écrire:

28 = 1708 - (140 X 12)

=1708 - (1848 - 1708) X 12
=-11.1708 - 1848.12
=-11.(9100 - 4.1848) - 12.1848
=(-11)(9100) + 32.18482

Ainsi 28 est bien la somme d'un multiple de (9100) et d'un multiple de (18482).

1.5. Entiers premiers entre eux:

Caractérisons simplement deux entiers premiers entre eux.

Théorème de Bezout

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

Preuve

- Si $a \wedge b = 1$, alors il existe $(u, v) \in Z^2$ tel que $1 = au + bv$
- Soit $d = a \wedge b$. Alors, d/a et d/b donc d/au + bv. Ainsi d/1 => d = 1.

Corollaire: Théorème de Gauss

Si un entier divise un produit et qu 'il est premier avec l'un des facteurs il divise l'autre:

$$a|bc \text{ et } a\wedge b=1 \Rightarrow a|c$$

Preuve

Comme $a\wedge b = 1 \Leftrightarrow \exists\ (u, v) \in Z^2$ tel que
$au + bv = 1 \Rightarrow acu + bcv = c$.
Comme a divise bc, alors, $\exists\ k \in Z$ tel que $bc = ka$ et par suite $a(cu+kv) = c$.
Ainsi, a divise c.

Corollaire

Si un entier est divisible par deux entiers premiers entre eux, il est divisible par leur produit

$$a|c \text{ , } b|c \text{ et } a\wedge b=1 \Rightarrow ab|c$$

Preuve

Comme a divise c et b divise c, il existe k, k' ∈ Z tel que c = ka = k'b. Ainsi b divise ka et a et b premiers entre eux implique, que b divise k, c'est à dire, il existe k' ∈ Z tel que k = k'b. Ainsi c = ka = k'ba et par suite a^b divise c.

Corollaire

Si un entier est premier avec deux autres, il est premier avec leur produit. Ainsi,

$$a \wedge c = 1 \text{ et } b \wedge c = 1 \Rightarrow ab \wedge c = 1$$

Preuve

Comme a et c sont premiers entre eux, alors, ∃ (u, v) ∈ Z^2 tel que au+cv = 1. De même, Comme b et c sont premiers entre eux, alors, ∃ (u', v') ∈ Z^2 tel que bu'+ cv' = 1. Ainsi abuu' + acuv' + bcu'²vv' = 1. D'où, ab(uu') + c(auv' + bu'v + cvv') = 1. D'après le théorème de Bezout, on en déduit que ab et c sont premiers entre eux.

Conséquence

Soit (a, b) ∈ Z^2

Si a∧b = 1 => $a^n \wedge b^m$ = 1 , n , m ∈ N*

Caractérisation de P.G.C.D.

Théorème

Soit (a, b) ∈ Z^2

Un entier positif d est le P.G.C.D. de a et b si, et seulement si,

∃ (a’,b’) ∈ Z^2 tel que a = a’d et b = b’d et a’∧b’ = 1

Preuve

• Si d = a ∧ b est un diviseur de a et b, il existe donc a' et b’ tels que a = a' d et b = b' d. Par ailleurs, il existe (u, v) ∈ Z^2 tel que au +bc= d; d'ou par simplification par d . On aura a'u + b'v = 1 et ceci nous donne d'après Bezout que a' ∧ b' = 1.

• Si a = a' d et b = b' d, d est un diviseur de a et b, donc de a ∧ b.

Par ailleurs, si a'∧b' = 1, il existe (u, v) $\in Z^2$ tel que a'u + b'v = 1, d'où au+ bv = d, ce qui signifie que d est un multiple de a ∧ b.

• Comme d|a ∧ b et a ∧ bld, et qu'ils sont tous les deux positifs, on en déduit d = a ∧ b.

Multiples communs de deux entiers

Définition 4: Soient a, b ∈ Z*. On appelle plus petit commun multiple ou ppcm de a et b et on note a V b le plus petit élément de l'ensemble des multiples communs strictement positif de a et b. Ainsi, si a/m et b/m alors ppe,m(a, b)/m.

Exemple

1. ppcm(12, 9) = 36
2. a V 0 = 0, a V b = lal V lbl

Théorème 5: Soient a et b des entiers non tous les deux nuls alors

pgcd(a, b) x ppcm(a, b) = labl

Preuve

(On peut supposer que a et b positifs)

Posons d =a ∧ b et a= a'd, b = b'd avec a' ∧ b' = 1 Soit m = da'b'. m est un multiple commun de a et de b. Tout multiple de m est un multiple commun de a et b.

Réciproquement soit M un multiple commun de a et de b, il existe (p: q) $\in Z^2$ tel que M = ap = bq. On a a'dp = b'dq, d'où a'p = b'q comme a' divise b'q et qu'il est premier avec b', il divise q. Donc il existe r ∈ Z tel que q = ra'

Ainsi M = ra'b = rm

Ainsi m.d = a'b'd² = ab. D'où

(a V b).(a ∧ b) = labl.

Nombres premiers

Définition Un entier naturel p ≥ 2 est dit premier s'il possède exactement deux diviseurs positifs 1 et lui même.

Remarque

1 est un nombre non premier.

Exemple

2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 31, 41, 43, 47 ... sont des nombres premiers.

Théorème d'Euclide

Il existe une infinité de nombre premiers.

Preuve

Dans le cas contraire, il n'y aurait qu'un nombre fini p_1, p_2, ... , p_n de nombres premiers. Soit m = $p_1 p_2 ... p_n$ + 1 et soit q son plus petit diviseur autre que 1. Alors q est premier et donc q est l'un des p_i. Ce qui est absurde car q|m et q † (m - 1).

Proposition

Si n n'est pas premier, alors il existe nombre premier, tel que p|n et on a p≤$\sqrt{n}$.

Preuve

Si n n'est pas premier alors n possède un diviseur premier p. Ainsi, n = pq avec 2 ≤ p ≤ q < n. Ainsi, n = pq ≥ p² ceci implique que p ≤ $\sqrt{n}$

Exemple:

n = 271 est-il premier?

Comme 16 < $\sqrt{271}$ < 17 il suffit de s'intéresser aux nombres premiers inférieurs ou égaux à 16 qui sont 2, 3, 5, 7, 11, 13 et aucun d'entre eux ne divise 271. Ainsi 271 est un nombre premier.

Remarque

1. Si p est un nombre premier et p ne divise pas n alors p∧ n = 1.
2. Si p est un nombre premier et si pl$a_1 a_2$ ... a_n alors p l un des a_i.

En effet : Raisonnons par récurrence.

- Pour n = 1, c'est clair.
- Pour n = 2, pl$a_1 a_2$ et p† a_1 => pla_2 .(d'après le théorème de Gauss).

Supposons le résultat vrai à l'ordre n et soit a_1, a_2, .. ,a_{n+1} tel que pl$a_1 a_2$, .. a_{n+1} avec p†a_1 => pl$a_2 a_3$, …$a_n a_{n+1}$
et d'après l'hypothèse de récurrence p divisera l'un d'eux.

Théorème fondamental

Tout entier supérieur ou égal à 2 s'écrit d'une manière unique sous la forme d'un produit de facteurs premiers (à l'ordre près) c'est à dire : ∀ n > 2, $\exists! p_1, p_2 \ldots p_m$ des nombres premiers distincts et $\alpha_1, \alpha_2 \ldots \alpha_m \in$ N*, tels que

$$n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$$

C'est la décomposition de l' entier n en produit de facteurs premiers.

Exemples

1. $43200 = 2^6 \times 3^3 \times 5^2$
2. $407 = 114 \times 37$
3. $300 = 2^2 \times 3 \times 5^2$

Preuve

Soit n > 1 tel que tout entier inférieur ou égal à n soit un produit de facteurs premiers. On a, n + 1 possède un diviseur premier p. Posons n + 1 = pq.

• Si q = 1, n + 1 = p, c'est donc le produit d'un seul facteur premier.
• Si q > 1, alors q ≤ n, d'après l'hypothèse de récurrence, q est un produit de k facteurs premiers. Donc (n+1) est le produit de (k+1) facteurs premiers.

Unicité : En regroupant les facteurs premiers égaux on peut écrire

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

les p_i étant des nombres premiers distincts deux à deux. Supposons qu'un certain nombre premier p apparaisse avec l'exposant $\alpha \geq 1$ dans une décomposition de n et l'exposant $\beta \geq 1$ dans une autre (on envisage $\beta = 0$ pour le cas où p ne figurant dans la deuxième décomposition). On a $p^{\alpha} a = p^{\beta} b$.

a et b sont des produits de nombres premiers distincts de p, ils sont donc premiers avec p :

• Si $\alpha > \beta$, $p^{\alpha-\beta} a = b$, ce qui contredit $p \wedge a = 1$.
• Si $\alpha < \beta$, $a = p^{\beta-\alpha} b$, ce qui contredit $p \wedge a = 1$, donc $\alpha = \beta$. Tous les facteurs premiers out le même exposant dans deux décompositions de n qui ne permet donc différer que par l'ordre des facteurs.