Chapitre II : Arithmétique dan Z

I- Relation de divisibilité, division euclidienne

1- Relation de divisibilité

Définition: Divisibilité

Soient deux entiers relatifs (a, b) $\in Z^2$. On dit que a divise b, ou que a est un diviseur de b, ou que b est un multiple de a si et seulement si $\exists\ k \in Z\ tq\ b = a$. On notera a | b (se lit « a divise b ») le fait que l'entier a divise l'entier b.

Théorème : Propriétés de la relation de divisibilité

Soient $a, b, c, d \in Z$

- **Réflexivité :** La relation « divise » est réflexive : $\forall\ a \in Z\ a \mid a$.
- **Transitivité :** La relation « divise » est transitive : $\forall\ a, b, c \in Z$ [a | b et b |c] $\Rightarrow a \mid c$.
- **Symétrie / antisymétrie :** La relation « divise » n'est ni symétrique, ni antisymétrique. Donc ce n'est ni une relation d''équivalence, ni une relation d'ordre sur Z). Par contre : [a | b et b | a] $\Rightarrow$ a = $\pm$ b.
- **Combinaison linéaire :** Si [d | a et d |b] $\Rightarrow d \mid k_1 a + k_2 b\ \ \forall k_1, k_2 \in Z$
- **Produit :** Si [a | b et c |d] $alors\ ac \mid bd$. En particulier si $a \mid b$ alors $a^k | b^k \quad \forall k, \in N$
- **Multiplication / division par un entier :** si $d \neq 0;\ a \mid b \ \Leftrightarrow\ ad \mid bd$

2- Relation de congruence

Définition:

Soient n $\in N$ et a, b$\in Z$. On dit que a est congru à b modulo n si n | (b-a), i.e. si $\exists\ k \in Z\ tq\ b = a + kn$. On notera a $\equiv$ b.

Remarque : La relation de congruence est une généralisation de la relation de divisibilité ; il faut en effet avoir en tête le cas particulier n | a $\Leftrightarrow$ a $\equiv$ 0 modulo n.

Théorème : Propriétés de la relation de congruence

Soient $a, a', b, b' \in Z\ \ et\ m, n \in N$

- La relation . $\equiv$. mod n est réflexive, symétrique et transitive
- **Somme :** Si $a \equiv$ b mod n et a' $\equiv$ b'$mod\ n\ \ alors\ a + a' \equiv$ b + b' mod n
- **Produit :** Si $a \equiv$ b mod n et a' $\equiv$ b'$mod\ n\ \ alors\ a.a' \equiv$ b. b' mod n . En particulier si $a \equiv b\ mod\ n$ alors $a^k \equiv b^k\ \ mod\ n\ \forall k, \in N$
- **Multiplication / division par un entier :** si $m \neq 0;\ a \equiv b\ mod\ n \ \Leftrightarrow\ am \equiv bm\ mod\ mn$

3- Division euclidienne

Soient deux entiers (a, b) $\in$ Z ×N avec b $\neq$ 0. Alors il existe un unique couple (q, r) $\in$ Z ×N tel que :

a = bq + r et 0 ≤ r ≤ b-1 ; ou encore 0 ≤ r < b

On appelle a le dividende, b le diviseur, q le quotient et r le reste de la division euclidienne de a par b.

On a $q = \left[\frac{a}{b}\right]\ \ et\ r \equiv$ a mod b

II- Diviseur et Multiple Communs

Définition: soit $a, b \in Z$

- On appelle un diviseur commun de a et b tout entier $d \in Z$ qui à la fois est un diviseur de a et un diviseur de b.
- On appelle un multiple commun de a et b tout entier $m \in Z$ qui à la fois est un multiple de a et un multiple de b.

1. PGCD, théorèmes d'Euclide et de Bezout

Définition:

Soient deux entiers non tous deux nuls (a, b) ∈ Z².

On appelle plus grand commun diviseur de PGCD de a et b tout entier $d \in Z$ tel que :

- d est diviseur commun de a et b : $d \mid a$ et $d \mid b$;
- d est un multiple de tout diviseur commun de a et b $\forall\delta \in Z, (\ \delta|a$ et $\delta|b) \Rightarrow\ \delta|d$

Le plus grand commun diviseur de a et b est noté PGCD (a, b) ou a ∧ b .

Théorème: Théorème d'Euclide

Soient deux entiers (a ,b) ∈ N^{*2}. Effectuons la division euclidienne de l'entier a par l'entier b :

∃! (q, r) ∈ N² : a = bq + r et 0 ≤ r < b Alors : a ∧ b = b ∧ r

Exemple : Déterminons le pgcd des entiers 366 et 43 en utilisant l'algorithme d'Euclide :

366 = 43 ×8+ 22
43 = 22 ×1+ 21
22 = 21 ×1+ 1
21 = 1 ×21+0
Donc PGCD (366, 431) = 1

1542 = 26 x 58 + 34
58 = 1 x 34 + 24
34 = 1 x 24 +10
24 = 2 x 10 + 4
10 = 2 x 4 + 2
4 = 2 x 2 + 0
Donc PGCD (1542, 58) = 2

Théorème: Existence et unicité du PGCD

Soient deux entiers a, b ∈ Z il existe un et un seul PGCD positif de a et b, appelé le PGCD de a et b.
Le seul autre PGCD de a et b est alors -PGCD (a, b)

Théorème: Propriétés du PGCD

Soient deux entiers a, b ∈ Z

(i) pour tout $k \in Z$ PGCD (ak, bk) = $|k|$PGCD (a, b)

(ii) pour tout diviseur commun $d \neq 0$ de a et b $PGCD\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{PGCD(a,b)}{|d|}$

Théorème: Coefficients de Bezout

Soient deux entiers non nuls (a, b) ∈ Z². Il existe (u, v) ∈ Z² tels que au + bv = a ∧ b.
Un tel couple (u, v) est appelé couple de coefficients de Bezout pour a et b.

Remarques : les entiers (u, v) ne sont pas uniques

Pour trouver un couple de coefficients de Bézout de deux entiers strictement positifs a et b, il suffit de « remonter les calculs » dans l'algorithme d'Euclide

Exemple :

Donner le PGCD de a et b et un couple de coefficients de Bezout avec avec a = 14938 et b = 9471

$14938 = 1 \cdot 9471 + 5467$	$77 = 385 - 308$
$9471 = 1 \cdot 5467 + 4004$	$77 = 385 - (1078 - 2 \cdot 385) = 3 \cdot 385 - 1078$
$5467 = 1 \cdot 4004 + 1463$	$77 = 3(1463 - 1078) - 1078 = -4 \cdot 1078 + 3 \cdot 1463$
$4004 = 2 \cdot 1463 + 1078$	$77 = -4 \cdot (4004 - 2 \cdot 1463) + 3 \cdot 1463 = 11 \cdot 1463 - 4 \cdot 4004$
$1463 = 1 \cdot 1078 + 385$	$77 = 11 \cdot (5467 - 4004) - 4 \cdot 4004 = -15 \cdot 4004 + 11 \cdot 5467$
$1078 = 2 \cdot 385 + 308$	$77 = -15 \cdot (9471 - 5467) + 11 \cdot 5467 = 26 \cdot 5467 - 15 \cdot 9471$
$385 = 1 \cdot 308 + 77$	$77 = 26 \cdot (14938 - 9471) - 15 \cdot 9471 = 26 \cdot 14938 - 41 \cdot 9471$

Les calculs de la colonne 1 donnent a ^ b = 77, puis ceux de la colonne 2 donnent 26a – 41b = 77

Exo : reprendre les questions de l'exemple précédant avec a= 3080 et b= 525

2. Nombres premiers entre eux

Définition:

Soit a, b ∈ Z. On dit que a et b sont premiers entre eux (ou encore étrangers) si leurs seuls diviseurs communs sont 1 et -1 ou encore a ^ b = 1.

Exemple : 28 et 15 sont premiers entre eux

Théorème : Théorème de Bezout

Soient deux entiers non nuls (a, b) ∈ Z². Les deux propositions suivantes sont équivalentes

- Les entiers a et b sont premiers entre eux : a ∧ b = 1
- ∃(u, v) ∈ Z² tel que 1 = au + bv

Théorème : Théorème de Gauss

Soient trois entiers non nuls (a, b, c) $\in Z^{*3}$ si [a | bc et a ∧ b = 1] ⇒ a | c

Corollaire : Forme irréductible d'un nombre rationnel

Soit $\boldsymbol{r} \in \boldsymbol{Q}$. Il existe un unique couple $(p, q) \in Z \times N^*$ $tel\ que$ $r = \frac{p}{q}$ et tel que p et q soient premiers entre eux. Cette écriture $r = \frac{p}{q}$ est appelée la forme irréductible de r.

3. PPCM

Définition:

Soient deux entiers non tous deux nuls (a, b) ∈ Z².

On appelle plus petit commun multiple PPCM de a et b tout entier $m \in Z$ tel que :

- m est multiple commun de a et b : $a \mid m$ et $b \mid m$;
- m est un diviseur de tout multiple commun de a et b $\forall \mu \in Z, (\ a|\mu$ et $b|\mu) \Rightarrow\ m|\mu$

Le plus petit commun multiple de a et b est noté PPCM (a, b) ou a ∨ b .

Théorème: Existence et unicité du PPCM

Soient deux entiers a, b ∈ Z il existe un et un seul PPCM positif de a et d, appelé le PPCM de a et b.

Le seul autre PPCM de a et b est alors - PPCM (a, b)

On a l'égalité $|ab| = PGCD(a, b) \times PPCM(a, b)$

Exemple :

PPCM (1542, 58) = 44718 en effet PPCM $(1542, 58) = \frac{1542 \times 58}{\text{PGCD } (1542,58)} = \frac{1542 \times 58}{2} = 44718$

III- Nombres premiers

Définition :

Soit p un entier naturel. On dit que p est premier si p > 2 et si ses seuls diviseurs dans N sont 1 et p. On dit que p est composé si p n'est pas premier.

L'ensemble des nombres premiers est noté $\mathbb{p}$

Exemple : La liste des nombres premiers contient 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43…

Proposition : L'ensemble des nombres premiers est infini.

Lemme :

Soit $r \in N^*$. On considère r nombre premiers $p_1, p_2, \ldots . . p_r \in \mathbb{p}$, distincts deux à deux et des entiers naturels non nuls $\alpha_1, \alpha_2, \ldots . . \alpha_r$. Alors tout diviseur premier $p_1^{\alpha_1} p_2^{\alpha_2} \ldots \ldots p_r^{\alpha_r}$ est l'un des $p_{i\ ou\ i \in [\![1,\ r]\!]}$

Théorème: Existence et unicité de la décomposition en facteurs premiers

Soit un entier $n \in N, n \geq 2$. il existe un unique entier $r \in N^*$, une unique famille $(p_1, p_2, \ldots\ldots p_r)$ de nombres premiers rangés dans l'ordre $p_1 < p_2 < \ldots\ldots < p_r$ et une unique famille $(\alpha_1, \alpha_2, \ldots\ldots \alpha_r)$ d'entiers naturels non nuls tels que : $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$

Les entiers $p_1, p_2, \ldots\ldots p_r$ sont tous les nombres premiers qui divisent n

Pour tout $i \in [\![1, \ r]\!]$ $p_i^{\alpha_i}$ est la plus grande puissance de p_i qui divise n

α_i est appelé l'ordre de multiplicité de p_i dans n.

Théorème: Expression du PGCD et du PPCM à l'aide des facteurs premiers

Soient deux entiers non-nuls $a, b \in N^*$. Leur décomposition en facteurs premiers s'écrit :

$$a = \prod_{p \in \mathbb{P}} p^{\alpha_p} \quad et \quad b = \prod_{p \in \mathbb{P}} p^{\beta_p}$$

Alors PGCD $(a, b) = \prod_{p \in \mathbb{P}} p^{\min(\alpha_p, \beta_p)}$ $\quad et \quad$ $PPCM\ (a, b) = \prod_{p \in \mathbb{P}} p^{\max(\alpha_p, \beta_p)}$