Ecole Nationale des Sciences Appliquées

Chapitre II

Arithmetique dans Z

ENSAH AL Hoceima

2020-2021

Plan

Divisibilité dans $\mathbb{Z}$

Plan

Plan

Divisibilité dans $\mathbb{Z}$

Éléments premiers entre eux

Le plus grand diviseur commun (pgcd)

Plan

Plan

Plan

Definition 1

Soient $a; b \in \mathbb{Z}$. On dit que b divise a et on note b/a s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Exemples 2

$7/21$; $6/48$; a *est pair si et seulement si* $2/a$.
Pour tout a $a \in \mathbb{Z}$, *on a* $a/0$ *et aussi* $1/a$.

Remarque 1

Si $a/1$ *alors* $a = +1$ *ou* $a = -1$.
$(a/b \text{ et } b/a) \Rightarrow b = a$
$(a/b \text{ et } b/c) \Rightarrow a/c$
$(a/b \text{ et } a/c) \Rightarrow a/(b + c)$

Definition 3

(couple d'entiers associés)
On dit que deux entiers a et b sont associés si et seulement si $a|b$ et $b|a$, c'est-à-dire $a\mathbb{Z} = b\mathbb{Z}$.

Proposition 1

(Caractérisation des entiers associés)
Les entiers a et b sont associés si et seulement si il existe $\epsilon \in \{-1, 1\}$ tel que $a = \epsilon b$.

Théorème 4

(Théorème de la division euclidienne)

Theorem 5

Soit $(a, b) \in \mathbb{Z}^2$, $b \neq 0$.
Il existe un unique couple $(q, r) \in \mathbb{Z} \times \ \mathbb{N}$ *tel que :* $a = bq + r$ *et* $0 \leq r < |b|$

-
- L'entier q est appelé quotient de la division euclidienne de a par b.
- L'entier r est appelé reste de la division euclidienne de a par b.

Remarque 1

b *peut être négatif.*

Exemple

$27 = 6 \times 4 + 3 = 6 \times 3 + 9 = 6 \times 6 - 3.$
$27 = (-6) \times \ (-4) + 3 = (-6) \times \ (-5) - 3.$

Ainsi, des identités $a = bq + r$, il y en a beaucoup, mais une seule vérifie la condition imposée sur r.
Ici, le quotient de la division de 27 par 6 est 4, et son reste est 3.

Definition 6

Anneau euclidien
Soit A un anneau. On dit que A est euclidien s'il est intègre, et muni d'une application $v : A\backslash\{0\} \to \mathbb{N}$ telle que :
$\forall a \in A, \forall b \in A\backslash\{0\}, \exists (q, r) \in A^2, \ a = bq + r$ et $(r = 0$ ou $v(r) < v(n))$

Théorème 7

* $b/a \Leftrightarrow a \in b\mathbb{Z}$.
* Si $a\#0$, alors $b/a \Rightarrow |b| \leq |a|$
* $(a/b$ et $b/a) \Leftrightarrow a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \lambda b$ avec $\lambda = \pm 1$ [on dit que a et b sont associés].
* Si b/a et b/c alors $u, v \in \mathbb{Z}$, $b/(au + cv)$.
* Si nb/na et si $n\#0$, alors b/a

Definition 8

(**Congruences d'entiers**)
Soit $n \in \mathbb{N}^*$, et $(a, b) \in \mathbb{Z}^2$. On dit que a et b sont congrus modulo n, et on écrit $a \equiv b[n]$, SSI
n divise $b - a$, ou encore si les divisions euclidiennes de a et b par n ont même reste.

Remarque 2

On trouve aussi assez souvent la notation $a \equiv b \mod n$, ou un mélange des 2 : $a \equiv b[\mathrm{mod}\ n]$.

Remarque 3

On dit que la relation de congruence est compatible avec les opérations.

Théorème 9

La relation de congruence modulo n est une relation d'équivalence.

Théorème 10

La relation de congruence modulo n est compatible avec le produit et la somme : soit $(a, a', b, b') \in \mathbb{Z}^4$ tels que $a \equiv a'[n]$ et $b \equiv b'[n]$ Alors $a + b \equiv a' + b'\ [n]$ et $ab \equiv a'b'[n]$

En d'autre terme, c'est une congruence sur les monoïdes $(\mathbb{Z}, +)$ et $(\mathbb{Z}, \times)$

Plan

Definitions 11

Soit $p \in \mathbb{N}^*$. On dit que p est un nombre premier si p admet exactement 2 diviseurs positifs
distincts (à savoir 1 et p lui-même)

Remarquez que l'existence de deux diviseurs distincts exclut d'office 1 de l'ensemble des nombres premiers, puisqu'il n'a qu'un diviseur.

Definition 12

Soit $n \in \mathbb{N}^*$. On dit que n est un nombre composé si n possède au moins 3 diviseurs positifs distincts,
ou en d'autres termes, si n possède un diviseur positif distinct de 1 et de n.

Proposition 2

Tout nombre composé admet un diviseur strict premier.

Lemme 13

(Euclide)
Soit a *et* b *deux entiers et* p *un entier premier tel que* $p|ab$.
Alors $p|a$ *ou* $p|b$.

Remarque 4

Cette propriété se retraduit sur les idéaux par $ab \in p\mathbb{Z} \Rightarrow$
$a \in p\mathbb{Z}$ *ou* $bvp\mathbb{Z}$, *ou encore,*
dans $\mathbb{Z}/p\mathbb{Z}$: $\quad ab = 0 \Rightarrow a = 0$ *ou* $b = 0$
Ainsi, le lemme d'Euclide traduit le fait que $\mathbb{Z}/p\mathbb{Z}$ *est intègre.*

Definition 14

Soit A un anneau commutatif, et I un idéal de A. On dit que I est un idéal premier de A si et seulement si A/I est intègre.

Remarque 5

Il y a une infinité de nombres premiers.

Definition 15

Pour $a \in \mathbb{Z}$, on note Da l'ensemble des diviseurs de a. Si a, b $\in \mathbb{Z}$, on note Da, b l'ensemble des diviseurs
communs à a et b, on a donc $Da, b = Da \cap Db$, cet ensemble contient toujours ± 1.

Théorème 16

Soient $a, b, q, r \in \mathbb{Z}$, *si* $a = bq + r$, *alors* Da, b $= Db, r$

Exemple

Exemple : Cherchons les diviseurs communs à $a = 336$ *et* $b = 210$

– *on effectue la division de a par b :* $336 = 1 \times 210 + 126$, *donc* $Da, b = D_{210,126}$.

– *on effectue la division de 210 par 126 :* $210 = 1 \times 126 + 84$, *donc* $Da, b = D_{210,126} = D_{126,84}$.

– *on effectue la division de 126 par 84 :* $126 = 1 \times 84 + 42$, *donc* $Da, b = D_{84,42}$.

– *on effectue la division de 84 par 42 :* $84 = 2 \times 42 + 0$, *donc* $Da, b = D_{42,0} = D_{42}$, *c'est à dire :*

$$D_{336,210} = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}.$$

Remarque 6

– *Pour tout élément* $a \in \mathbb{Z}$, *on a* $\pm 1/a$
– *Si* $a \# 0$, *alors* Da *est un ensemble fini, plus précisément* $Da \subset [-|a|; |a|]$
– $D_0 = \mathbb{Z}, \quad D_{\pm 1} = \{\pm 1\}$.

Théorème 17

Décomposition primaire

Tout entier strictement positif n *s'écrit de façon unique sous la forme*

$$n = p1 \times \cdots \times pk$$

où $p1 \leq \cdots \leq pk$ *sont des nombres premiers, ce produit étant éventuellement vide si* $n = 1$.

Definition 18

Soient $a, b \in \mathbb{Z}$
On dit que a et b sont premiers entre eux (ou a est premier avec b) lorsque le seul diviseur commun positif est 1.

Remarque 7

– *Dire que a est premier avec b revient à dire que le dernier reste non nul dans l'algorithme d'Euclide est 1.*
– *Si a est premier avec b, alors au moins un des deux est non nul (sinon l'ensemble des diviseurs communs est $\mathbb{Z}$).*

Théorème 19

Théorème de Bézout
Soient $a, b \in \mathbb{Z}$, *alors* a *et* b *sont premiers entre eux si et seulement si il existe* $u, v \in \mathbb{Z}$ *tels que* $au + bv = 1$.
Les entiers u *et* v *sont appelés coefficients de Bézout.*

Preuve 1

Supposons que u *et* v *existent et soit* d *un diviseur commun à* a *et* b, *alors* d/a *et* d/b, *donc* $d/au + bv$
i.e. $d/1$, *donc* $d = \pm 1$ *ce qui prouve que* a *et* b *sont premiers entre eux.*
Réciproquement *: si* a *est premier avec* b. *En appliquant l'algorithme d'Euclide on vérifie qu'à chaque étape le reste* r_k *peut se mettre sous la forme* $r_k = a.u_k + b.v_k$

Plan

Definition 20

Soient $a, b \in \mathbb{Z}$ non tous deux non nuls. on appelle $pgcd$ de a et de b le plus grand diviseur commun.
Notation : $pgcd(a, b)$ ou $a \Lambda b$, c'est le dernier reste non nul dans l'algorithme d'Euclide.

Lemma 21

En découle que deux éléments a et b de $\mathbb{Z}$, non tous deux nuls, sont premiers entre eux si et seulement si $pgcd(a, b) = 1$.

Exemples 22

- *pgcd(21, 14) = 7, pgcd(12, 32) = 4, pgcd(21, 26) = 1.*
- *pgcd(a, ka) = a, pour tout k 2 Z et a $>$ 0.*
- *Cas particuliers. Pour tout a $>$ 0 : pgcd(a, 0) = a et pgcd(a, 1) = 1.*

Lemme 23

Soient $a, b \in \mathbb{N}^*$. *Écrivons la division euclidienne* $a = bq + r$.
Alors $pgcd(a, b) = pgcd(b, r)$

On calcule des divisions euclidiennes successives.
• division de a par b, $a = bq_1 + r_1$. Par le lemme 1, $pgcd(a, b) = pgcd(b, r_1)$ et si $r_1 = 0$ alors $pgcd(a, b) = b$ sinon on continue :
• $b = r_1 q_2 + r_2$, $pgcd(a, b) = pgcd(b, r_1) = pgcd(r_1, r_2)$,
• $r_1 = r_2 q_3 + r_3$, $pgcd(a, b) = pgcd(r_2, r_3)$,
• ....
• $r_{k-2} = r_{k-1} q_k + rk$, $pgcd(a, b) = pgcd(r_{k-1} q_k, r_k)$,
• $r_{k-1} q = r_k q_k + 0$. $pgcd(a, b) = pgcd(r_k, 0) = r_k$.
On a $0 \leq r_{i+1} < r_i$ .Les restes formant une suite décroissante d'entiers positifs ou nuls : $b > r_1 > r_2 > .....> 0$.

Exemple

Calcule les coefficients de Bézout pour $a = 600$ et $b = 124$.

$$
\begin{array}{rcrcrcr}
600 & = & 124 & \times & 4 & + & 104 \\
124 & = & 104 & \times & 1 & + & 20 \\
104 & = & 20 & \times & 5 & + & 4 \\
20 & = & 4 & \times & 5 & + & 0
\end{array}
$$

$$
4 = \left[\begin{array}{l} 600 \times 6 + 124 \times (-29) \\ 124 \times (-5) + (600 - 124 \times 4) \times 6 \end{array} \right.
$$

$$
4 = \left[\begin{array}{l} 124 \times (-5) + 104 \times 6 \\ 104 - (124 - 104 \times 1) \times 5 \end{array} \right.
$$

$$
4 = \left[\, 104 - 20 \times 5 \right.
$$

Ainsi pour $u = 6$ et $v = -29$ alors $600 * 6 + 124 * (-29) = 4$.
Donc le pgcd$(600, 124) = 4$.

Exemple

Calculez les coefficients de Bézout correspondant à pgcd(9945, 3003) = 39.

les coefficients de Bézout correspondant à pgcd$(9945, 3003) = 39$.

$$\begin{array}{rcrcrcr} 9945 &=& 3003 &\times& 3 &+& 936 \\ 3003 &=& 936 &\times& 3 &+& 195 \\ 936 &=& 195 &\times& 4 &+& 156 \\ 195 &=& 156 &\times& 1 &+& 39 \\ 156 &=& 39 &\times& 4 &+& 0 \end{array} \qquad \begin{array}{rcc} 39 &=& 9945\times(-16)+3003\times 53 \\ 39 &=& \cdots \\ 39 &=& \cdots \\ 39 &=& 195-156\times 1 \end{array}$$

On obtient $9945 * (-16) + 3003 * 53 = 39$.

Corollaire 1

Si a est premier avec b et si a est premier avec c, alors a est premier avec le produit bc.
On en déduit que si a est premier avec $c1, ..., cn$, alors a est premier avec le produit $c1 \times ... \times cn$.

Preuve 2

Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$, il existe $p, q \in \mathbb{Z}$ tels que $ap + cq = 1$.
On effectue le produit de ces deux relations, ce qui donne
$a(ucq + uap + pbv) + bc(vq) = 1$,
d'après le théorème de Bézout, a et bc sont premiers entre eux.

Théorème 24

Si a *est premier avec* c, *si* a/b *et si* c/b, *alors* $ac \,/\, b$.

Remarque 8

Ce théorème est faux lorsque a *et* c *ne sont pas premiers entre eux, par exemple :* $2/12$ *et* $4/12$ *mais* $2 \times 4 = 8$ *ne divise pas* 12.

Théorème 25

Théorème de Gauss

Si a/bc *et si* a *est premier avec* c, *alors* a/b.

Preuve 3

Il existe $u, v \in \mathbb{Z}$ *tels que* $au + cv = 1$, *on multiplie par* b, *ce qui donne* $bau + bvc = b$, *or* a/bc *donc* $a/(bau + bcv)$, *i.e.* a/b.

Proposition 3

Considérons l'équation (E) : $ax + by = c$ *où* $a, b, c \in \mathbb{Z}$.
1. L'équation (E) possède des solutions $(x, y) \in \mathbb{Z}^2$ *si et seulement si* $pgcd(a, b)/c$.
2. Si $pgcd(a, b)/c$ *, alors il existe même une infinité de solutions entières et elles sont exactement les* $(x, y) = (x_0 + \alpha k, y_0 + \beta k)$ *avec* x_0, y_0, α, $\beta \in \mathbb{Z}$ *fixés et* k *parcourant* $\in \mathbb{Z}$.

Exemple

Trouver les solutions entières de (E) : $161x + 368y = 115$

Solution 26

Première étape *: On effectue l'algorithme d'Euclide pour calculer le pgcd de* $a = 161$ *et* $b = 368$.

368	=	161	×	2	+	46
161	=	46	×	3	+	23
46	=	23	×	2	+	0

Donc $pgcd(368, 161) = 23$. *Comme* $115 = 5 * 23$ *alors* $pgcd(368, 161)/115$. *Par le théorème de Bézout, l'équation (E) admet des solutions entières.*

Solution 27

Deuxième étape *: Trouver une solution particulière : la remontée de l'algorithme d'Euclide.*

$$\begin{array}{rcrcrcr} 368 & = & 161 & \times & 2 & + & 46 \\ 161 & = & 46 & \times & 3 & + & 23 \\ 46 & = & 23 & \times & 2 & + & 0 \end{array} \qquad \begin{array}{rcl} 23 & = & \left| \begin{array}{l} 161 \times 7 + 368 \times (-3) \\ 161 + (368 - 2 \times 161) \times (-3) \end{array} \right. \\ 23 & = & 161 - 3 \times 46 \end{array}$$

On trouve donc $161 * 7 + 368 * (-3) = 23$.
Comme $115 = 5 * 23$ *en multipliant par 5 on obtient :*
$161 * 35 + 368 * (-15) = 115$
Ainsi $(x_0, y_0) = (35, -15)$ *est une solution particulière de (E).*

Solution 28

Troisième étape *: Recherche de toutes les solutions. Nous savons que* (x_0, y_0) *est aussi solution. Ainsi :*
$161x + 368y = 115$ *et* $161x_0 + 368y_0 = 115$
La différence de ces deux égalités conduit à

$$\begin{aligned} & 161 \times (x - x_0) + 368 \times (y - y_0) = 0 \\ \Longrightarrow \quad & 23 \times 7 \times (x - x_0) + 23 \times 16 \times (y - y_0) = 0 \\ \Longrightarrow \quad & 7(x - x_0) = -16(y - y_0) \qquad (*) \end{aligned}$$

Nous avons simplifié par 23 qui est le pgcd de 161 et 368. (Attention, n'oubliez surtout pas cette simplification, sinon la suite du raisonnement serait fausse.)

Solution 29

Ainsi $7/16(y - y_0)$, *or* $pgcd(7,16) = 1$ *donc par le lemme de Gauss* $7/y - y_0$. *Il existe donc* $k \in \mathbb{Z}$ *tel que* $y - y_0 = 7k$.
Repartant de l'équation ( ) : $7(x - x_0) = -16(y - y_0)$. *On obtient maintenant* $7(x - x_0) = -16 \times 7k$.
D'où $x - x_0 = -16k$. *(C'est le même* k *pour* x *et pour* y*).*
Nous avons donc $(x, y) = (x_0 - 16k, y_0 + 7k)$. *Il n'est pas dur de voir que tout couple de cette forme est solution de l'équation (E). Il reste donc juste à substituer (x0, y0) par sa valeur et nous obtenons :*
Les solutions entières de 161x + 368y = 115 sont les $(x, y) = (35 - 16k, -15 + 7k)$, $k \in \mathbb{Z}$.

Exemple

Montere que les solutions de l'équation (E) : $37x + 23y = 1$ *sont* $(5 - 23k\ ; -8 + 37k)$ *tel* $k \in \mathbb{Z}$

Plan

Definition 30

Le $ppcm(a, b)$ (plus petit multiple commun) est le plus petit entier > 0 divisible par a et par b.

Par exemple $ppcm(12, 9) = 36$.

Proposition 4

Si a, b sont des entiers (non tous les deux nuls) alors $pgcd(a, b)\times\ ppcm(a, b) = |ab|$

Proposition 5

Si a/c et b/c alors $ppcm(a, b)/c$.

Théorème 31

Soit $n \succeq 2$ *un entier. Il existe des nombres premiers* $p_1 < p_2 < ..... < p_r$ *et des exposants entiers* $\alpha_1, \alpha_2, ..., \alpha_r > 1$ *tels que :* $\quad n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times .... \times p_r^{\alpha_r}$
De plus les pi et les $\alpha_1 (i = 1, ..., r)$ *sont uniques.*

Exemple

$24 = 2^3 \times 3$ *est la décomposition en facteurs premiers.*
Par contre $36 = 2^2 \times 9$ *n'est pas la décomposition en facteurs premiers, c'est* $36 = 2^2 \times 3^2$.

Exemple

$504 = 2^3 \times 3^2 \times 7$ *et* $300 = 2^2 \times 3 \times 5^2$.

Pour calculer le pgcd on réécrit ces décompositions :

$504 = 2^3 \times 3^2 \times 5^0 \times 7$, $300 = 2^2 \times 3 \times 5^2 \times 7^0$.

Le pgcd est le nombre obtenu en prenant le plus petit exposant de chaque facteur premier :

$pgcd(504, 300) = 2^2 \times 3^2 \times 5^0 \times 7^0 = 12.$

Pour le ppcm on prend le plus grand exposant de chaque facteur premier :

$ppcm(504, 300) = 2^3 \times 3^2 \times 5^2 \times 7^1 = 12600$