Divisibilité, Congruences, Bézout

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$, l'ensemble des entiers naturels

$\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$ relatifs

ou simplement entiers.

1 Divisibilité :

Soient a, b deux entiers ; on dit que b divise a. On le note $b | a$, s'il existe un entier k tel que : $a = kb$.

On dit que a est divisible par b ou encore a est un multiple de b.

et donc l'ensemble des $\mathbb{Z}b = \{nb, n \in \mathbb{Z}\}$ est donc l'ensemble des multiples de b.

Cas particulier : $b = 0$; $\mathbb{Z}0 = \{0\}$, i.e. On n'a qu'un seul multiple.

si $b \neq 0$, b a une infinité de multiples.

Soit $a \in \mathbb{Z}$, $D(a)$ est l'ensemble des diviseurs de a ;

<u>Proposition</u> : $a \in \mathbb{Z}^*$, entier non nul ; si $b \in D(a)$; $|b| \leq |a|$.

preuve : $a = kb$; $a \neq 0$, $b \neq 0$, $k \neq 0$; $|k| \geq 1$

$\Rightarrow |a| = |k||b| \geq |b|$.

si $a = 0$; 0 a une infinité de diviseurs !

$D(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.

$D(a)$ est un ensemble fini pour $a \neq 0$;
les diviseurs de a sont en nombre fini.

Proposition : (très utile) : On suppose que $a | b$ et $a | c$ alors $a | \alpha b + \beta c$; $(\alpha, \beta) \in \mathbb{Z}^2$.

preuve : ~~$\alpha b + \beta c =$~~

$a | b \Rightarrow b = ka$
$a | c \Rightarrow c = k' a$.

$$\alpha b + \beta c = \alpha k a + \beta k' a = \underbrace{(\alpha k + \beta k')}_{\in \mathbb{Z}} a$$

Application : On considère la question suivante :
On cherche tous les entiers n tel que :

$$n - 4 \mid 3n - 17.$$

On a : $n - 4 \mid n - 4$ $\Rightarrow (n-4) \mid 3n - 17 - 3(n-4)$

$n - 4 \mid 3n - 17$

i.e. $n - 4 \mid 3n - 17 - 3n + 12 = -5$ ou encore

$n - 4 \in D(-5) = \{-5, -1, 1, 5\}$

$n \in \{-1, 3, 5, 9\}$.

si $n = -1$; $n-4 = -5$, $3n-17 = -10$; $-5 \mid -20$

si $n = 3$, $n-4 = -1$, $3n-17 = -8$; $-1 \mid -8$

si $n = 5$, $n-4 = 1$; $3n-17 = -5$, $1 \mid -2$

si $n = 9$ $n-4 = 5$; $3n-17 = 10$; $5 \mid 20$

$n \in \{-1, 3, 5, 9\}$.

② Congruences : $n \neq 0$; $(a, b) \in \mathbb{Z}$.

On dit que a et b sont congrus modulo n ; si $n \mid a-b$; On note $a \equiv b\,[n]$.

Remarque : ① $a \equiv a\,[n]$.

② si $a \equiv b\,[n]$, alors $b \equiv a\,[n]$

(3) si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ $\Rightarrow$ $a \equiv c\,[n]$.

Cette propriété s'appelle relation d'équivalence.

Proposition : $n \in \mathbb{N}^*$, a, b, c, d des entiers $a \equiv b\,[n]$, $c \equiv d\,[n]$ alors

1) $a+c \equiv b+d\,[n]$.

2) $ac \equiv bd\,[n]$.

preuve : (1) $n \mid b-a$ et $n \mid c-d$

$\Rightarrow n \mid b-a+c-d = b+d-(a+c).$

$\Rightarrow$ ~~b~~. $a+c \equiv b+d\ [n].$

(2) : $bd-ac = bd-bc+bc-ac$

$= b(d-c)+c(b-a).$

$n \mid d-c$ et $n \mid b-a \Rightarrow n \mid bd-ac.$

Application : Critère de divisibilité par 3

$n = a_d a_{d-1} \cdots a_0$ = écriture décimale.

$= a_d 10^d + a_{d-1} 10^{d-1} + \cdots + a_1 \cdot 10 + a_0.$

$10 \equiv 1\ [3]$

$10^2 \equiv 1\times 1 = 1\ [3]$

$\vdots$

$10^d \equiv 1\ [3].$

$n \equiv a_d + a_{d-1} + \cdots + a_0\ [3]$

n est divisible par 3 $\Leftrightarrow$ $a_d + a_{d-1} + \cdots a_0$ est un multiple de 3.

division euclidienne:

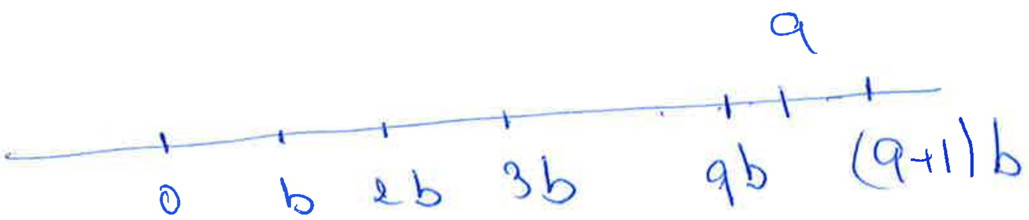
proposition

$a \in \mathbb{Z}$; b un entier ≥ 1 ; il existe un unique couple (q,r), $q \in \mathbb{Z}$; $r \in \mathbb{Z}$ tel

$$a = bq + r \; ; \quad 0 \leq r \leq b-1$$

q = le quotient, r le reste :

preuve : On suppose pour simplifier que $a \geq 0$



$A = \{$ multiple de $b \leq a \}$.

A est un ensemble fini ; il possède un plus grand élément, soit qb cet élément.

On pose : $r = a - qb$; $r \geq 0$ par définition de A ;

On a : $qb \leq a$ et $(q+1)b > a$.

$qb + b > a \Rightarrow qb - a > -b$ ou encore : $\underbrace{a - qb}_{r} < b$

Montrons l'unicité :

$a = bq + r$
$= bq' + r'$; $\Rightarrow r - r' = b(q' - q)$.

* $r - r'$ est un multiple de b:

si $r-r' \neq 0$; on peut supposer que $r - r' \geq 0$

On a : $r \leq b-1$ et $r - r' \leq b-1$

$r-r'$ ne peut etre un multiple de b.

$\Rightarrow r - r' = 0 \Rightarrow (q'-q)b = 0 \Rightarrow q = q'$.

Consequence de la division euclidienne:

Soit $a \in \mathbb{Z}$; $n \in \mathbb{N}'$, $n \geq 1$

$a = qn + r$; (division euclidienne de a par n)

$r \in \{0, 1, \dots, n-1\}$.

$a \equiv r\,[n]$

Application : 1 $n(n+1)(n+2)$ est un multiple de 3

On a trois cas:

a) $n \equiv 0\,[n]$; OK.

b) $n \equiv 1\,[n]$, $n+2 \equiv 0\,[n]$.

c) $n \equiv 2\,[n]$, $n+1 \equiv 0\,[n]$.

2 On suppose que $7 \mid a^2 + b^2$, montrer que $7 \mid a$ et $7 \mid b$.

preuve:

10

On utilise les congruences :

a	0	1	2	3	4	5	6
a^2	0	1	4	2	2	4	1

$a^2 \in \{0, 1, 2, 4\}$:

On voit donc que pour avoir $a^2 + b^2 \equiv 0 \, [7]$

$\iff a \equiv 0 \, [7]$ et $b \equiv 0 \, [7]$.

(4) PGCD. $a \neq 0$, $b \neq 0$

$D(a) \cap D(b)$ a un plus grand élément.

On l'appelle $\operatorname{pgcd}(a,b) = (a,b)$

Exemple : $a = 28$; $b = 16$

$(D(a) \cap D(b))^+ = \{2, 4\}$.

$\operatorname{pgcd}(a,b) = 4$.

ou encore : $28 = 4 \times 7 = 2^2 \times 7$

$16 = 2^4$

$\Rightarrow \operatorname{pgcd}(28, 16) = 2^2$.

④ Algorithme d'Euclide :

<u>proposition</u> : Soient a, b deux entiers, $a \neq 0$, $b \neq 0$.

$a = bq + r$ la division euclidienne de a par b

On a : $pgcd(a, b) = pgcd(b, r)$.

<u>preuve</u> : Soit d un diviseur de a et de b ;

$d \mid a$ et $d \mid b \Rightarrow d \mid a - bq = r$;

<u>Reciproquement</u> : si $d \mid b$ et et $d \mid r \Rightarrow$

$d \mid bq + r = a$; autrement dit.

$D(a) \cap D(b) = D(b) \cap D(r)$. ou encore

$pgcd(a, b) = pgcd(b, r)$

On va utiliser le résultat pour établir un algorithme (très efficace) pour calculer $pgcd(a, b)$:

<u>suivons</u> .. $a = b q_1 + r_1$; $0 \leq r_1 \leq b-1$; $(a, b) = (b, r_1)$

$b = r_1 q_2 + r_2$; $0 \leq r_2 < r_1$, $(b, r_1) = (r_1, r_2)$.

$r_1 = r_2 q_3 + r_3$;

⋮

$r_{n-2} = r_{n-1} q_n + r_n$ $(r_{n-2}, r_{n-1}) = (r_{n-1}, r_n)$.

$r_{n-1} = r_n q_{n+1} + 0$ $(r_{n-1}, r_n) = r_n$.

En résumé : $\text{pgcd}(a,b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$

$\dots = \text{pgcd}(r_{n-1}, r_n) = r_n$.

Le pgcd(a,b) est donc le dernier reste non nul des divisions successives.

Exemples : (1) $a = 120$, $b = 23$.

$$120 = 23 \times 5 + 5$$

$$23 = 5 \times 4 + 3.$$

$$5 = 3 \times 1 + 2.$$

$$3 = 2 \times 1 + 1$$

$$2 = 2 \times 1 + 0.$$

$\text{pgcd}(120, 23) = 1$, on dit qu'ils sont premiers entre eux.

(2) $a = 135$, $b = 101$

$$135 = 101 \times 1 + 34$$

$$101 = 34 \times 2 + 33$$

$$34 = 33 \times 1 + 1$$

$$33 = 33 \times 1 + 0.$$

$\text{pgcd}(135, 101) = 1$

(3) $\text{pgcd}(931, 513) = 19$ (à faire chez vous)

th de Bézout : Soient a, b deux entiers, $a \neq 0$, $b \neq 0$
il existe $(u, v) \in \mathbb{Z}^2$ tel que :

$\boxed{au + bv = pgcd(a, b)}$; identité de Bézout.

preuve. On pose : $D = \{ au + bv, (u, v) \in \mathbb{Z}^2 \}$

On veut donc montrer que $pgcd(a, b) \in D$.

Com. On fait d'abord une petite remarque.
prenons $n \in D$, $m \in D$; on effectue une division euclidienne de n par m.

$n = qm + r$; $n - qm = r \in D$.

i.e. le reste de la division euclidienne de deux élément de D reste dans D.

Reprenons l'Algorithme d'Euclide

$a = a \times 1 + 0 \times b \in D$.

$b = 0 \times a + 1 \times b \in D$

$\Rightarrow r_1 \in D$
de la même manière, $r_2 \in D$ ... , $r_n = pgcd(a, b)$
est un élément de D.

Remarque : le couple (u, v) n'est pas unique.

Comment trouver (u, v) ?

Algorithme d'Euclide étendu :

On reprend l'exemple précédent :

$$120 = 5 \times 23 + 5 \qquad (23, 5)$$

$$23 = 5 \times 4 + 3. \qquad (5, 3)$$

$$5 = 3 \times 1 + 2 \qquad (3, 2)$$

$$3 = 1 \times 2 + 1.$$

On part de la dernière ligne :

$$1 = 3 - 1 \times 2. = 3u + 2v;$$

$u = 1$, $v = -1$, c'est une identité de Bezout du couple $(3, 2)$: On remplace le 2 de ligne au dessus :

$$1 = 3 - 1 \times 2 = 3 - 1 \times (5 - 3 \times 1)$$

$$= 3 - 5 + 3 = 2 \times 3 - 5$$

$$= 3u + 5v;$$

Identité de Bezout du couple $(5, 3)$. On continue en remontant les lignes de la même manière ; On remplace les restes :

$$1 = 2 \times 3 - 5 = 2 \times (23 - 5 \times 4) - 5$$

$$= 2 \times 23 - 9 \times 5$$

$= 2\times 23 - 9\times(120 - 5\times 23)$

$= 2\times 23 - 9\times 120 + 45\times 23$

$= \underbrace{47}_{u}\times 23 \underbrace{- 9}_{v}\times 120$

dans l'autre exemple : $(135, 101)$.

on trouve : $1 = 3\times 135 - 4\times 101$

Remarque :

① Supposons qu'on a une identité de Bezout $au + bv = 1$; On peut conclure que $\text{pgcd}(a,b) = 1$;

② ⚠ Supposons qu'on a : $au + bv = d$; $\text{pgcd}(a,b)$ n'est pas égal à d forcément ; on peut toutefois conclure que : $\text{pgcd}(a,b)$ divise d. On peut facilement comprendre cette situation. Donnons un exemple : $1 = 3\times 135 - 4\times 101$

$2 = 3\times 270 - 8\times 101$

on a multiplié u et v par deux ; le $\text{pgcd}(135, 101) = 1$ et non 2 ⚠. (le couple (u,v) n'est pas unique)

(3) Supposons qu'on a :

$$au + bv = \mathrm{pgcd}(a,b).$$

Soit d un diviseur commun de a et de b ;
alors $d \mid \mathrm{pgcd}(a,b)$. Cette remarque est très importante. $\mathrm{pgcd}(a,b)$ est par définition le plus grand diviseur commun de a et de b ; et d'autre propriété ; il est multiple de tous les diviseurs communs de a et de b ;
connaître le $\mathrm{pgcd}(a,b)$ permet de connaître les diviseurs commun de a et de b !

(5) th de Gauss (ou lemme de Gauss)

th : On considère 3 entiers a, b, c, avec $\mathrm{pgcd}(a,b) = 1$, on suppose que $a \mid bc$ alors $a \mid c$.

<u>Remarque.</u> $12 \mid 24 = 6 \times 4$;

$(12,6) = 6$ et 12 ne divise ni 6, ni 4 !
$(12,4) = 4$

L'hypothèse $(a,b) = 1$ est primordiale.

<u>preuve</u> : D'après Bezout, on a une identité

$$au + bv = 1$$

On multiplie par c des deux côtés :

$$a u c + b v c = c.$$

On a : $a \mid auc$ et $a \mid bcv$. $\Rightarrow a \mid c$.

Corollaire (Lemme d'Euclide) :
Soit p un nombre premier ;
si $p \mid bc$ alors $p \mid b$ ou $p \mid c$.

preuve : si p ne divise pas $b \Rightarrow (p, b)$ sont premiers entre eux. (les seuls diviseurs positifs de p sont 1 et p).

Conséquences du th de Gauss :

Proposition : Soient a, b, c des entiers qui vérifient : $pgcd(a,b) = 1$, $a \mid c$ et $b \mid c$

alors $ab \mid c$.

preuve : $c = ka = k'b$
$a \mid c = k'b$; $(a,b) = 1$, d'après Gauss
$a \mid k'$ ce qui s'écrit : $k' = k''a$,
$c = k'b = \cancel{k} k''ab$, $ab \mid c$.

plus généralement si $(a_1, \dots, a_r)$ sont des entiers premiers entre eux deux à deux ; ie $(a_i, a_j) = 1$ $i \neq j$
et si $a_i \mid n$, $\forall i = 1 \dots, r$ alors : $\prod_{i=1}^{r} a_i \mid n$.

Exemples :

(1) Soit p un nombre premier, $p > 3$; alors :

$24 \mid p^2 - 1$.

Solution : $24 = 3 \times 8$; $(3,8) = 1$; il suffit d'après la proposition précédente de montrer que $3 \mid p^2 - 1$ et $8 \mid p^2 - 1$.

(vu en T.D).

(2) $\forall n \in \mathbb{N}$; $35 \mid 3^{6n} - 2^{6n} = u_n$

preuve : comme dans l'exple précédent ; on va montrer que $7 \mid u_n$ et $5 \mid u_n$.

On va utiliser les congruences :

$3^2 \equiv 4\,[5] = \cancel{-1\,[5]}$.

$3^{6n} = 3^{2 \times 3n} \equiv 4^{3n} \equiv (2^2)^{3n} \equiv 2^{6n}$.

donc : $5 \mid u_n$.

$3^{6n} - 2^{6n} \equiv (3^2)^{3n} - (2^3)^{2n}\,[7]$

$\equiv 2^{3n} - 1\,[7]$

$\equiv (2^3)^n - 1\,[7] \equiv 1 - 1\,[7]$

donc $7 \mid u_n$; $(5,7) = 1 \Rightarrow 35 \mid u_n$.