

IV Arithmétique dans \mathbb{Z}

Divisibilité dans \mathbb{Z}

$$b/a \Leftrightarrow \exists q \in \mathbb{Z}, a = bq$$

- $D(a)$: ensemble des diviseurs de a , $D(a)$ est borné par $(-a, a)$
- $a\mathbb{Z}$: ensemble des multiples de a
- $\forall a$, a admet au moins 6 diviseurs : $a, -a, 1, -1$
- $1, -1$ divisent tous les entiers
- 0 est un multiple de tous les entiers mais ne divise que 0
- $a|a$
- a/b et $b/a \Rightarrow a = \pm b$
- a/b et $b/c \Rightarrow a/c$
- a/b et $a/c \Rightarrow a/(ab + vc)$

Division Euclidienne dans \mathbb{Z}

Soit $a \in \mathbb{Z}$ $b \in \mathbb{N}^*$, il existe deux entiers $q, r \in \mathbb{Z}$ tels que

$$\boxed{a = bq + r \quad 0 \leq r < b}$$

PGCD et PPCM

- L'ensemble des diviseurs communs à a et b possède un plus grand élément appelé "plus grand commun diviseur". Il est noté $\text{PGCD}(a, b) = a \cap b$
- L'ensemble des multiples strictement positifs communs à a et b possède un plus petit élément appelé "plus petit commun multiple" et noté $\text{PPCM}(a, b) = a \vee b$
- Soient a et b deux entiers naturels non nuls, soient q et r le quotient et le reste de la division euclidienne de a par b .
 - si $r = 0$ alors $a \cap b = b$
 - si $r \neq 0$ alors $a \cap b = b \cap r \Rightarrow$ algorithme d'euclide.

ex: 15648 n 657

$$\begin{aligned} 15648 &= 657 \times 23 + 939 \\ 657 &= 531 \times 1 + 120 \\ 537 &= 120 \times 4 + 57 \\ 120 &= 57 \times 2 + 6 \\ 57 &= 6 \times 9 + 3 \\ 6 &= 3 \times 2 + 0 \end{aligned}$$

$$\Rightarrow 15648 \text{ n } 657 = 3$$

Théorème de Bezout

- Soient a, b deux entiers relatifs, il existe deux entiers $u, v \in \mathbb{Z}$ tels que $au + bv = \text{rg}(a, b)$
- Corollaires du théorème de Bezout: Soient $a, b \in \mathbb{Z}$ si $d' \mid a$ et $d' \mid b$ alors $d' \mid \text{rg}(a, b)$
- Si a et b premiers entre eux alors $\text{rg}(a, b) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$
- Lemme de Gauß: Soient $a, b, c \in \mathbb{Z}$ si $a \mid bc$ et $\text{rg}(a, b) = 1 \Rightarrow a \mid c$

Nombre premiers entre eux

- a et $a+1$ sont premiers entre eux
- Soient $a, b \in \mathbb{Z}$ avec $\text{rg}(a, b) = d$ alors $\exists a', b'$ tels que $a = a'd$ et $b = b'd$ et $a' \mid b'$
- $\frac{a}{b} = \frac{a'}{b'} \Rightarrow$ on appelle $\frac{a'}{b'}$ la forme irréductible de $\frac{a}{b}$
- $\text{rg}(a, b) = 1$ et $\text{rg}(a, c) = 1 \Rightarrow \text{rg}(a, bc) = 1$
- généralisation: $\text{rg}(a_1 b_1 b_2 \dots b_n) = \text{rg}(a_1 | \prod_{i=2}^n b_i) = 1 \Leftrightarrow \text{rg}(a, b_2) = 1 \text{ et } \text{rg}(a, b_3) = 1 \dots \text{ et } \text{rg}(a, b_n) = 1$
- Soit $\text{rg}(a, b) = 1$ alors $\forall (m, n) \in \mathbb{N}^2$, $\text{rg}(a^m b^n) = 1$

Équation diophantienne

Résolvons: $ax + by = z$ (E)

Etape 1: calculer $\text{rg}(a, b)$, si $\text{rg}(a, b)$ divise z alors (E) admet des solutions

Etape 2: On cherche une solution particulière (x_0, y_0)

Etape 3: On a: $ax_0 + by_0 = z$ $\Rightarrow a(x_0 - x) = b(y_0 - y)$
soit $a \mid b = d$ $a = a'd$ et $b = b'd$ avec $a' \mid b' = 1$

comme $a' \mid b' = 1$: alors $\exists K \quad a'K = y_0 - y \Rightarrow y = a'K + y_0$
 $\exists K \quad b'K = x_0 - x \Rightarrow x = b'K + x_0$

Les nombres premiers

- Un nb premier est un entier ≥ 2 dont les seuls diviseurs positifs sont 1 et lui-même
- Tout entier ≥ 2 admet un diviseur qui est un nb premier
- $n > 1$ est premier si l n'est divisible par aucun nombre premier inférieur à \sqrt{n}
- Il existe un infinité de nbs premiers
- Soit p un nb premier , et a et b des entiers positifs
 $p/a b \Rightarrow p/a$ ou p/b
- Tout entier naturel $n > 1$ peut s'écrire comme un produit de nombres premiers. Cette décomposition en facteur premier est unique à l'ordre près.
ex = $24 = 2^3 \times 3$
 $48 = 2^4 \times 3$

Congruence

- $a \equiv b [c] \Leftrightarrow a - b = kc$
- $a \equiv b [c] \Leftrightarrow a$ et b ont le même reste par la division euclidienne par n
- Si $a \equiv b [n]$ et $c \equiv d [n]$
alors $a+c \equiv b+d [n]$
 $ac \equiv bd [n]$
 $a^k \equiv b^k [n]$

→ Dans le triangle de Pascal, on remarque que :
Soit P un entier premier alors P divise C_p^k

$0 \rightarrow 1$
 $1 \rightarrow 11$
 $2 \rightarrow 121$
 $3 \rightarrow 1331$
 $4 \rightarrow 14641$
 $5 \rightarrow 15101051$
 $6 \rightarrow 1615201561$
 $7 \rightarrow 1718353571$

- Soit P un entier premier , soit $a, b \in \mathbb{Z}$ on a :

$$(a+b)^P \equiv a^P + b^P [P]$$

- Théorème de Fermat : $n^P \equiv n [P]$

$$n^{P-1} \equiv 1 [P]$$