1. Divisibilité dans $\mathbb{Z}$

1.3. Relation de congruence modulo un entier

Si $n|b-a$ alors $b-a=kn$ où $k\in\mathbb{Z}$, soit $b=a+kn$

$a\equiv b \bmod n$, $a\equiv b\ [n]$, $a\equiv b\ (n)$

$11-1=10$ et $5|10$, ou $11=1+2\times5$ donc $11\equiv 1\ [5]$

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

Ex 17. $2^{518}+8^{211}\equiv 0\ [3]$.

$2\equiv -1\ [3]$, donc $2^{518}\equiv (-1)^{518}\ [3]$ (518 pair) $= 1$

$8\equiv -1\ [3]$ donc $8^{211}\equiv (-1)^{811}\ [3]$ (811 impair) $=-1$

$2^{518}+8^{211}\equiv \underbrace{1+(-1)}_{0}\ [3]$

$15\equiv 1\ [7]$. $15n\equiv n\ [7]$ $n\equiv -5\ [7]$

et $-5\equiv 2\ [7]$

$n\equiv 2\ [7]$: $7|n-2$ donc $n-2=7\times k$, $n=2+k7$ avec $k\in\mathbb{Z}$.

• Montrons que $n^2-1\equiv 0\ [8]$.

$a=q\times n+r$ avec $q\in\mathbb{Z}$ et $0\le r\le n-1$

$a\equiv r\ [n]$.

$\bar{a}=\{b\in\mathbb{Z},\ a\equiv b\ [n]\}=\{b\in\mathbb{Z}\mid b=a+kn\}$

$a\in\mathbb{Z}$, $\exists!\ r\in\{0..n-1\}$, $a\equiv r\ [n]$, donc $\bar{a}=\bar{r}$

2. PGCD, PPCM

1. PGCD

$x \in a\mathbb{Z}+b\mathbb{Z}$ si $x = ak_1 + bk_2$ avec $k_1 \in \mathbb{Z}$, $k_2 \in \mathbb{Z}$.

$a|b$ ssi $b\mathbb{Z} \subset a\mathbb{Z}$

ssi $b \subset a\mathbb{Z}$

$q_1\mathbb{Z} + \dots + q_n\mathbb{Z} = d\mathbb{Z}$ avec $d \in \mathbb{N}$.

↑ $\text{pgcd}(a_1, \dots a_n)$.

si $d' | a$ et $d' | b$ alors $0 < d' \leq \text{pgcd}(a,b)$

si $d' | a$ et $d' | b$ alors $0 < d' | \text{pgcd}(a,b)$

$D_+(12,18) = \{1, 2, 3, 6\}$

↑ $\text{pgcd}(12,18)$

$d = d \times 1 \in d\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z}$ donc $d = au_0 + bv_0$, $u_0, v_0 \in \mathbb{Z}$.

Prop 32.

- $d\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z} = -a\mathbb{Z}+(-b)\mathbb{Z}$

$a\mathbb{Z} = \{ak, k \in \mathbb{Z}\} = \{a(-p), p \in \mathbb{Z}\} = \{-a \times p, p \in \mathbb{Z}\} = -a\mathbb{Z}$.

$a\mathbb{Z} + 0\mathbb{Z} = a\mathbb{Z} = |a|\mathbb{Z}$

Lemme 33.

$a = bq + r$. $\quad a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ avec $d \in \mathbb{N}$. ($d = \text{pgcd}(a,b)$)

$a\mathbb{Z}+b\mathbb{Z} = (bq+r)\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z} = \underbrace{\text{pgcd}(b,r)\mathbb{Z}}_{\in \mathbb{N}}$.

$x \in (bq+r)\mathbb{Z} + b\mathbb{Z}$: $x = (bq+r)k_1 + bk_2$

$= b(qk_1 + k_2) + rk_1 \in b\mathbb{Z} + r\mathbb{Z}$.

$x \in b\mathbb{Z} + r\mathbb{Z}$: $x = bk_1' + rk_2'$

$= bk_1' + rk_2' + bqk_2' - bqk_2'$

$= \underbrace{(r+bq)}_{=a} \underbrace{k_2'}_{\in \mathbb{Z}} + b\underbrace{(k_1' - qk_2')}_{\in \mathbb{Z}}$

2. PGCD, PPCM

2_3. Entiers premiers entre eux

$a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

Thm 39. • Si $pgcd(a,b) = 1$, alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

Or $1 \in \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Donc $1 = au + bv$.

• Supposons $au + bv = 1$.

$1 \in a\mathbb{Z} + b\mathbb{Z}$, soit $p \in \mathbb{Z}$, alors $p = p \times 1 = aup + bvp \in a\mathbb{Z} + b\mathbb{Z}$

Donc $\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}$ Donc $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} = 1\mathbb{Z}$.

$1 = pgcd(a,b)$.

Ex 41. 1795 et 343.

Algorithme d'Euclide.

$1795 = 5 \times 343 + 80$
$343 = 4 \times 80 + 23$
$80 = 3 \times 23 + 11$
$23 = 2 \times 11 + 1$
$11 = 11 \times 1 + 0$ reste nul.

$PGCD(1795, 343) = 1$.

On cherche u et $v \in \mathbb{Z}$ tels que $1795u + 343v = 1$.

$r_k = u_k \cdot a + v_k \cdot b$

$1795 = 1 \times 1795 + 0 \times 343$
$343 = 0 \times 1795 + 1 \times 343$
$80 = 1 \times 1795 + (-5) \times 343$
$1 \times \quad 23 = -4 \times 1795 + 21 \times 343$
$(-2) \times \quad 11 = 13 \times 1795 + -68 \times 343$
$1 = -30 \times 1795 + 157 \times 343$

(u, a, v, b)

$a \mid c$ donc $c = ka$ donc $bc = kab$.