Arithmétique

Définition :

a divise b : $\exists k \in \mathbb{Z} : b = ak$

On dit que a est un diviseur de b

Proposition

Si $a|b$ alors $a|-b$, $-a|b$, $-a|-b$

Proposition

Si $a|b$ alors $|b| \geq |a|$

~~Démonst~~

Définition

- On note $div(a)$ L'ensemble des diviseurs de a.
- On note $Mul(a)$ l'ensemble des multiples de a.

$Div(a) = \{b \in \mathbb{Z} / b | a\}$

$Mul(a) = \{a.k / k \in \mathbb{Z}\}$

$Div(6) = \{1, 2, 3, 6, -1, -2, -3, -6\}$

Proposition.

$a|b$ et $b/c \Rightarrow a|c$

$a|b$ et $b|a \Rightarrow |a| = |b|$

$a|b$ et $a|c \Rightarrow a|b+c$

$a|b$ et $c|d \Rightarrow ac|bd$

$a|b \Rightarrow a^p | b^p$

Division Euclidienne

Théorème.

$\forall a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$

$\exists! (q, R)$ tq : $a = bq + r$

avec $b > 0$ et $R \geq 0$

$0 \leq r < b$

Proposition :

$b|a \Leftrightarrow a = kb \Leftrightarrow a = kb + r \Leftrightarrow r = 0$

Congruence.

Définition.

$a \equiv b[n] \Leftrightarrow n | a - b \Leftrightarrow a = kn + b$

$n|a \Leftrightarrow a \equiv 0[n]$

Proposition.

$\forall a \in \mathbb{Z}, \exists! r \in \{0 \dots n-1\}$ tq : $a \equiv r[n]$

Proposition.

$a \equiv b[n]$
1. $n / b - a$
2. Si $a \equiv b[n]$, $b \equiv c[n]$ alors $a \equiv c[n]$

Proposition :

1. $a + b \equiv a' + b' [n]$
2. $ab \equiv a'b'[n]$
3. $-a \equiv -a' [n]$
4. $a^p \equiv a'^p [n]$

$(a+b)^n = \sum_{i=0}^{n} C_n^i a^n b^{n-i}$

PGCD :

Définition.

- Si $d|a$ et $d|b$ alors d est un div de a et b.
- $Div(a,b)$ l'ensemble des div commun de a et b.

$Div(a,b) = div(a) \cap div(b)$

Proposition.

$Div(a,b)$ a tjrs un max / $div \neq (0,0)$

Définition

$Max(Div(a,b)) = pgcd(a,b)$

Définition.

$pgcd(0,0) = 0$.

Proposition

1. $Pgcd(a,b) \in \mathbb{N}$
2. $pgcd(a,b) = pgcd(b,a)$
3. $pgcd(a,b) = pgcd(|a|,|b|)$
4. Si $a|b$ alors $pgcd(a,b) = |a|$

Proposition.

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

Université Internationale de Casablanca

LAUREATE INTERNATIONAL UNIVERSITIES

Définition : (dérivation)

$P = \sum_{i=0}^{n} a_i X^i$

$P' = \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i$

Définition

On pose :

$D : \mathbb{K}[X] \to \mathbb{K}[X]$

$P \mapsto P'$

On appelle dérivée d'ordre supérieur le polynôme $\Lambda^n(P) = P^n$

Proposition.

$P \in \mathbb{K}[X]$, $n \geq 2$

$\deg(P^{(n)}) = -\infty$ Si $n > \deg(P)$

$\deg(P^{(n)}) = \deg(P) - n$ Si $n \leq \deg(P)$

Proposition.

- $P' = 0 \iff P$ constante.
- $\deg(P') = \deg(P) - 1$

Proposition

$(P.Q)^{(n)} = \sum_{k=0}^{n} \binom{p}{n} P^k Q^{n-k}$

$(P \circ Q)' = Q' \times (P' \circ Q)$.

$C_n^p = \frac{n!}{p!(n-p)!}$

Définition.

$\exists \lambda \in \mathbb{K}^*$ tq : $P = \lambda Q$.

On dit cela si un poly $P \in \mathbb{K}[X]$ et associé à un polynôme $Q \in \mathbb{K}[X]$

l'association est une équivalence.

Proposition.

$\sum a_i X^i = \sum b_i X^i \iff a_n = b_n$

Définition.

On dit que P est unitaire si $a_n = 1$

$P \in \mathbb{K}[X]$, P est associé à un polynôme unitaire

Définition.

$Q \mid P \Rightarrow \exists U \in \mathbb{K}[X]$ tq : $P = UQ$.

Définition.

Soit $P \in \mathbb{K}[X]$

$\mathrm{Div}(P) = \{Q \in \mathbb{K}[X] \mid Q \mid P\}$

~~Div~~

$\mathrm{Mul}(P) = \{Q \in \mathbb{K}[X] \mid P \mid Q\}$.

Proposition.

C et D associé à A et B

$A \mid B \Rightarrow C \mid D$

Proposition.

- Si $A \mid B$ et $B \mid C$ Alors $A \mid C$
- Si $A \mid B$ et $B \mid A$ alors $A = B$.

Proposition.

- Si $A \mid B$ et $A \mid C$ alors $A \mid B + C$
- Si $A \mid B$ et $C \mid D$ alors $AC \mid BD$

Proposition

- Si $A \mid B$ alors $\deg(A) \leq \deg(B)$
- Si $A \mid B$ et $\deg(A) = \deg(B)$ alors $A = B$.

Théorème

Soient $A, B \in \mathbb{K}[X]$

$\exists! (Q, R) \in \mathbb{K}^2[X]$ tq :

$A = BQ + R$.

Université Internationale
de Casablanca

Définition.

facteur premier de n tout p tq:

$p|n$.

Proposition.

"n" a au moin un facteur premier

Proposition,

P est un ensemble infini.

Proposition.

Si p ne divise pas a alors: $a \wedge p \neq 1$

Théoreme

si $p|ab$ alors $p|a$ ou $p|b$

Corollaire

Si $p|(a_1 \dots a_m)$ alors $\exists i$ tq $p|a_i$

Théorème

Soit $n \in \mathbb{N}^*$

$\exists N \in \mathbb{N}^*$, $\exists \alpha_1 \dots \alpha_m$ et $\exists p_1 \dots p_m \in P$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

$0 \leq \beta_i \leq \alpha_i$

Si $d|n$

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}$$

Polynômes :

Définition.

Un polynôme est : $P = \sum_{i=0}^{+\infty} a_i X^i$

$i \in \mathbb{N}$ et une suite nulle ~~et~~ à partir d'un certain rang. $P = \sum_{i=0}^{m} a_i X^i$

Définition

$P = Q \iff a_i = b_i \iff \sum a_i X_i = \sum b_i X_i$

avec $\forall i \geq 0$

Définition

Polynôme est constant si $P = a_0$

Définition

On dit que P est un monôme ssi :

(un seul coef non nul)

$P = a_n X^n$

Définition :

$P = \sum_{i=0}^{+\infty} a_i X^i$ et $Q = \sum_{i=0}^{+\infty} b_i X^i$

$P + Q = \sum_{i=0}^{+\infty} (a_i + b_i) X^i$.

Définition.

$P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$

$P = \sum_{i=0}^{+\infty} a_i X^i$

On a $\alpha P = \sum_{i=0}^{+\infty} \alpha a_i X^i$

Définition.

l'indice le plus grand du coef non nul

On note $\deg(P)$

En général si $P = \sum_{i=0}^{m} a_i X^i$

$\deg(P) = n$.

Définition

Si $\deg(P) = n$ alors a_n est appellé dominant.

Convention.

Si $P = 0$ alors $\deg(P) = -\infty$

Proposition.

$$\deg(\alpha P) = \begin{cases} \deg(P) = n & \text{si } \alpha \neq 0 \\ \deg(P) = -\infty & \text{si } \alpha = 0 \end{cases}$$

Proposition.

$P = \sum_{i=0}^{+\infty} a_i X^i$, $Q = \sum_{i=0}^{+\infty} b_i X^i$

$\deg(P+Q) \leq \text{Max}(\deg(P), \deg(Q))$

On a égalité si $\deg(P) \neq \deg(Q)$

Définition.

$\mathbb{K}[X]_n$ l'ensemble des polynômes degré $\leq n$

$\mathbb{K}[X]_m = \{aX + b \ / \ a, b \in \mathbb{K}\}$.

Définition.

$P = \sum_{i}^{+\infty} a_i X^i$, $Q = \sum^{+\infty} b_i X^i$

$P . Q = \sum_{n=0}^{+\infty} \delta_n X^n \ / \ \delta_n = \sum$

Théorème

$\deg(P.Q) = \deg(P) + \deg(Q)$

Corollaire.

Si $P.Q = 0 \iff P = 0$ ou $Q = 0$.

Définition.

$P = \sum^{+\infty} a_i X_i$ et $Q = \sum^{+\infty} b_i X_i$

$P \circ Q = P(Q) = \sum_{i=0}^{+\infty} a_i (Q)^i$

Proposition.

$(\alpha P + \delta Q) \circ R = \alpha P \circ R + \delta Q \circ R$

$(PQ) \circ R = (P \circ R) . (Q \circ R)$.

Définition.

$P = \sum_{i=0}^{m} a_i X^i = a_0 + a_1 X + a_2 X^2 + \dots a_m X^m$

Proposition.

Définition

On dit que $x_0 \in \mathbb{K}$ est un zéro de P ssi

$P(x_0) = 0$

Définition.

Fonction polynominale.

$$\tilde{P} : \begin{cases} \mathbb{K} \longrightarrow \mathbb{K} \\ x \longmapsto P(x) \end{cases}$$

Algorithme d'Euclide

$pgcd(24,9) = pgcd(9,6)$
$= pgcd(6,3)$
$= pgcd(3,0)$

le pgcd est donc le dernier reste non nul.

Egalité de bezout.

Théorème.

$\exists u,v \in \mathbb{Z}$ tq: $pgcd(a,b) = aU + bV$
$a \wedge b = aU + bV$

Théorème.

Si $d|a$ et $d|b$ alors $d | pgcd(a,b)$

Corollaire

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

Proposition

$pgcd(da, db) = d\, pgcd(a,b)$.

PPCM.

Si $a|m$ et $b|m$ alors m est dit le multiple commun de a et b.

Proposition.

$Mul(a,b) \cap \mathbb{N}^*$ à un ~~...~~ min.
le min $(Mul(a,b) \cap \mathbb{N}^*)$ est $ppcm(a,b)$.

$ppcm(5,3) = 15$.
$ppcm(0,0) = 0$

Proposition

$a|m$ et $b|m \Rightarrow ppcm(a,b) | m$.

Proposition

Si $a|b$ alors $ppcm(a,b) = |b|$

Proposition

$ppcm(da, db) = d\, ppcm(a,b)$

Théorème.

$pgcd(a,b) \cdot ppcm(a,b) = |ab|$

Nombre premier entre eux.

Définition:

$a \wedge b = 1$ / a et b premier entre eux

Proposition.

$a \wedge b = 1 \Leftrightarrow a \vee b = |ab|$

Proposition.

Si $a'|a$ et $b'|b$ et $a \wedge b = 1$
Donc $a' \wedge b' = 1$

Théorème (de Bezout).

$a \wedge b = 1 \Leftrightarrow \exists u,v \in \mathbb{Z}$ tq : $Ua + bV = 1$

Proposition.

Si $a \wedge b = 1$ et $a \wedge c = 1$
alors $a \wedge bc = 1$

Proposition

- Si $a_1 \wedge b = a_2 \wedge b = a_3 \wedge b = \dots\ a_n \wedge b = 1$
- Si $a \wedge b = 1 \Rightarrow a^n \wedge b^n = 1$

Théorème de Gauss.

Théorème:

Si $a|bc$ et $a \wedge b = 1$
Donc $a|c$

Proposition.

Si $a_1|b$ et $a_2|b$ ... $a_n|b$ et $a_1 \dots a_n$ sont premiers entre eux.
alors
$a_1 \dots a_n | b$

Théorème.

$\delta = pgcd(a,b)$
Donc $a = \delta a'$ et $\delta b' = b$
tq $= a' \wedge b' = 1$

Définition.

$Div(p) \cap \mathbb{N} = \{1, p\}$