C11 - Résumé

Définition de la divisibilité

Pour $a, b \in \mathbb{Z}$, $a|b \Leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que $ak = b$

Propriété divisibilité

$$\forall a, b, c \in \mathbb{Z}, c \mid a \text{ et } c \mid b \Rightarrow \forall \lambda, \mu \in \mathbb{Z}, c \mid (\lambda a + \mu b)$$

$$\forall a, b, c, d \in \mathbb{Z}, a \mid b \text{ et } c \mid d \Rightarrow ac \mid bd$$

Définition de l'Association

a et b $\in \mathbb{Z}$ sont dit associés ssi $a|b$ et $b|a$
Ils sont associés ssi :

$$|a| = |b| \Leftrightarrow a = \pm\, b \Leftrightarrow \exists \epsilon \in \{\pm 1\}, a = \epsilon b$$

Théorème de la division euclidienne

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^*, \exists ! (q, r) \in \mathbb{Z} \times [\![0, |b| - 1]\!], a = bq + r$$

Propriété

Dans le cas ou q et r existent et que $a \in \mathbb{Z}$ $b > 0$

$$q = \left\lfloor \frac{a}{b} \right\rfloor \text{ et } r = a - b \left\lfloor \frac{a}{b} \right\rfloor$$

Définition

Pour $a, b \in \mathbb{N}$
On note : $\mathrm{CD}(a, b) = \mathrm{CD}(b, a)$
Les diviseurs communs de a et de b
(!!!!! Notation du prof)

Lemme qui servira a l'algorithme d'Euclide

Soient $(a,b) \in \mathbb{N} \times \mathbb{N}^*$ et r le reste de la division euclidienne de a par b alors :

$$\mathrm{CD}(a,b) = \mathrm{CD}(b,r)$$

Théorème : Existence du PGCD et son calcul par l'algorithme d'Euclide

Pour $a,b \in \mathbb{N}$ l'ensemble $\mathrm{CD}(a,b)$ de leurs diviseurs (positifs) communs possède un plus grand élément au sens de la divisibilité, qu'on note $a \wedge b$ et qu'on appelle le PGCD (plus grand commun diviseur) de a et b.

De plus, $a \wedge b$ est l'avant-dernier reste obtenu dans l'algorithme d'Euclide. Dans le cas où $(a,b) \neq (0,0)$, il est non nul et c'est donc le “dernier reste non nul” de l'algorithme.

Lemme : Lien entre divisibilité et ordre usuel

Si $n \in \mathbb{N}^*$, tout diviseur de n est inférieur ou égal à n au sens de l'ordre usuel.

Propriété : PGCD et ordre usuel

Pour $(a,b) \in \mathbb{N}^2 \backslash \{(0,0)\}$, $a \wedge b$ est aussi le plus grand des diviseurs communs de a et b au sens de l'ordre usuel.

Relation de Bézout dans $\mathbb{N}$

$$\forall a,b \in \mathbb{N}, \exists u,v \in \mathbb{Z}, a \wedge b = au + bv$$

Définition

Pour $a, b \in \mathbb{Z}$
On appelle PGCD de a et b le nombre :

$$a \wedge b = |a| \wedge |b|$$

Propriété caractéristique du PGCD

Pour $a, b \in \mathbb{N}$ et $d \in \mathbb{Z}$, $d = a \wedge b$ ssi les deux condition suivantes sont réalisées :

- d divise a et b
- Tout diviseur commun de a et b divise d

Relation de Bézout dans $\mathbb{Z}$

$$\forall a, b \in \mathbb{Z}, \exists u, v \in \mathbb{Z}, a \wedge b = au + bv$$

Propriété

$$\forall a, b \in \mathbb{Z}, \forall k \in \mathbb{Z}^*, (ka) \wedge (kb) = |k|(a \wedge b)$$

Théorème

Soit $a, b \in \mathbb{Z}$ alors

$$a \wedge b = 1 \Leftrightarrow (\exists u, v \in \mathbb{Z}, au + bv = 1)$$

Théorème de Gauss

Soient $a, b, c \in \mathbb{Z}$

$$\left.\begin{array}{r} a \mid bc \\ a \wedge b = 1 \end{array}\right\} \Rightarrow a \mid c$$

Théorème : Divisibilité par produit

Soient $a, b, c \in \mathbb{Z}$

$$\left.\begin{array}{r} a \mid b \\ b \mid c \\ a \wedge b = 1 \end{array}\right\} \Rightarrow ab \mid c$$

Théorème

Soient $a, b, c \in \mathbb{Z}$

$$\left.\begin{array}{r} a \wedge b \\ b \wedge c \end{array}\right\} \Rightarrow (ab) \wedge c = 1$$

Théorème

$$\forall r \in \mathbb{Q}, \exists!(p, q) \in \mathbb{Z} \times \mathbb{N}^*, \begin{cases} p \wedge q = 1 \\ \frac{p}{q} = r \end{cases}$$

Définition de l'écriture irréductible

L'écriture $r = \frac{p}{q}$ s'appelle l'écriture irréductible du rationnel r

Théorème de l'unicité de la forme irréductible

Soient $(p, q), (p', q') \in \mathbb{Z} \times \mathbb{N}^*$, tel que $p \wedge q$ = $p' \wedge q' = 1$
et $\frac{p}{q} = \frac{p'}{q'}$

Définition du PGCD de 3 entiers

Soient $a, b, c \in \mathbb{Z}$,
Le PGCD de 3 entiers est :

$$a \wedge b \wedge c$$

Propriété

La loi $\wedge$ est associative et commutative et admet 0 comme élément neutre $\text{sur}\ \mathbb{N}$.

Définition du PGCD de n entiers naturels

L'ensemble des diviseurs communs à $a_1, \wedge a_2, \wedge \cdots \wedge a_n \in \mathbb{N}$ possède un plus grand élément pour $|_\mathbb{N}$ qui est :

$$\bigwedge_{i=1}^{n} a_i = a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

Définition du PGCD de n entiers relatifs

L'ensemble des diviseurs communs à $a_1, \wedge a_2, \wedge \cdots \wedge a_n \in \mathbb{Z}$ possède un plus grand élément pour $|_\mathbb{Z}$ qui est :

$$\bigwedge_{i=1}^{n} a_i = \bigwedge_{i=1}^{n} \mid a_i \mid$$

Propriété (Caractérisation)

Pour tous $a_1, \ldots, a_n \in \mathbb{Z}$ et $d \in \mathbb{Z}$, $d = \bigwedge a_i$ ssi les deux conditions suivantes sont réalisés :

- d divise tous les a_i
- tous diviseurs communs des a_i divise d

Propriété : Relation de Bézout pour n entiers

$$\forall a_1, \ldots, a_n \in \mathbb{Z}, \exists u_1, \ldots, u_n \in \mathbb{Z}, \bigwedge_{i=1}^{n} a_i = \sum_{i=1}^{n} u_i a_i$$

Définition des nombres premiers entre eux deux a deux

Soient $a_1, \ldots, a_n \in \mathbb{Z}$
On dit qu'ils sont

1. Premiers entre eux deux a deux ssi $\forall i, j \in [\![1, n]\!], (i \neq j \Rightarrow a_i \wedge a_j = 1)$
2. Premiers entre eux dans leur ensemble

ssi

$$\bigwedge_{i=1}^{n} a_i = 1$$

Théorème de Bézout pour n entiers

$$\forall a_1, \ldots, a_n \in \mathbb{Z}, \bigwedge_{i=1}^{n} a_i = 1 \Leftrightarrow \left(\exists u_1, \ldots, u_n, \sum_{i=1}^{n} u_i a_i = 1\right)$$

Définition dans $\mathbb{Z}$ du PPCM

Pour $a, b \in \mathbb{Z}$, on pose

$$a \vee b = |a| \vee |b|$$

Propriété

Pour $a \neq 0$ et $b \neq 0$, $a \vee b$ est aussi le plus petit des multiples communs positifs de a et b au sens de l'ordre usuel $\leq$

Propriété : Caractérisation du PPCM

Soient $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}$
Alors

$$m = a \vee b \Leftrightarrow \begin{cases} a \mid m \text{ et } b \mid m \\ \forall n \in \mathbb{Z}, (a \mid n \text{ et } b \mid n \Rightarrow m \mid n) \end{cases}$$

Propriété

$$\forall a, b \in \mathbb{Z}, (a \wedge b)(a \vee b) = |ab|$$

Définition d'un nombre premier

Un nombre premier est un entier naturel $p \neq 1$ et dont les seuls diviseurs positifs sont 1 et p

Notation (du prof)

On notera $\mathcal{P}$ l'ensemble des nombres premiers

Définition

$n \neq 1$ et non premier est dit composé.
Il existe alors $ab \in \mathbb{N} \backslash \{1, n\}$ tel que
$n = ab$. Si $n \neq 0$, on a $a, b \in [\![2, n-1]\!]$ et $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$

Propriété

Soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}$
Alors

$$n \wedge p \neq 1 \Leftrightarrow p \mid n$$

i.e. on a une alternative

- Soit $p \mid n$ et $p \wedge n = p$
- Soit p et n sont premiers entre eux

Lemme d'Euclide

Soit $p \in \mathcal{P}$ et $e, b \in \mathbb{Z}$ Alors

$$p \mid ab \Rightarrow (p \mid a \text{ ou } p \mid b)$$

Théorème

$\mathcal{P}$ est infini

Théorème

$$\forall n \in \mathbb{N}^*, \exists k \in \mathbb{N}, \exists p_1, \ldots, p_k \in \mathcal{P}, \exists \alpha_1, \ldots, \alpha_k \in \mathbb{N}^*, n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

De plus cette écriture est unique à l'ordre des facteurs près

Théorème : limites des suites complexes

Soit $u \in \mathbb{C}^{\mathbb{N}}$, $l \in \mathbb{C}$

$$u_n \to l \Leftrightarrow \begin{cases} Re(u_n) \to Re(l) \\ Im(u_n) \to Im(l) \end{cases}$$

Définition : Valuation p-adique

Soit $p \in \mathcal{P}$,
Pour $n \in \mathbb{N}^*$, on appelle valuation p-adique de n le nombre :

$$v_p(n) = max\{k \in \mathbb{N} \mid (p^k \mid n)\}$$

Lorsque $p \mid n$, c'est aussi la puissance de p dans la décomposition en facteurs premiers de n
Lorsque $p \nmid n$, $v_p(n) = 0$

Définition : Factorisation première

Pour $n \in \mathbb{N}^*$, l'écriture :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

S'appelle la factorisation-première de n

Théorèmes

Avec la convention, on ne prend pas en compte les factorisations $p^0 = 1$ par $p \nmid n$

- $\forall p \in \mathcal{P}, v_p(ab) = v_p(a) + v_p(b)$
- $a \mid b \Leftrightarrow \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$
- $a \wedge b = \prod_{p \in \mathcal{P}} p^{min(v_p(a), v_p(b))}$ et $a \vee b = \prod_{p \in \mathcal{P}} p^{max(v_p(a), v_p(b))}$ i.e.

$$\forall p \in \mathcal{P}, \begin{cases} v_p(a \wedge b) = min(v_p(a), v_p(b)) \\ v_p(a \vee b) = max(v_p(a), v_p(b)) \end{cases}$$

Cas pratique : On utilise ce produit de manière abstraite : en pratique on écrit que les premiers qui servent.

Définition des congruences

Pour $n \in \mathbb{N}$,
On dit que $a, b \in \mathbb{Z}$ sont congrus modulo n ssi $n \mid a - b$
On note $a \equiv b[n]$
et lorsque on a besoin $\equiv_n a_k$ relation sur $\mathbb{Z}$ appelé congruence modulo n

Pour les propriétés suivantes on supposera que $\forall n \in [\![2, +\infty[\![, \equiv_n$

Propriété

$\equiv_n$ est une relation d'équivalence

Notation

On note, lorsqu'il n'y a pas ambiguïté, $\overline{a}$ la classe d'équivalence par $\equiv_n$ qu'on appelle classe de congruences modulo n de a :

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b[n]\} \subset \mathbb{Z}$$

i.e.

$$\overline{a} \in \mathcal{P}(\mathbb{Z})$$

Reformulation

Soient $a, b \in \mathbb{Z}$,

$$a \equiv b[n] \Leftrightarrow n \mid b - a \Leftrightarrow a \in \overline{b} \Leftrightarrow b \in \overline{a} \Leftrightarrow \overline{a} = \overline{b}$$

Propriété

Les classes de congruences modulo n sont au nombre de n. Ce sont $\overline{0}, \overline{1}, \ldots, \overline{n-1}$

Notation

L'ensemble quotient de $\mathbb{Z}$ par $\equiv_n$ qui est l'ensemble des classes de congruences modulo n est noté :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{k}; k \in [\![0, n-1]\!]\}$$

$('\mathbb{Z} \text{ sur } n\mathbb{Z}')$

Rappel

Sur les relations d'équivalences les classes forment une partition de l'ensemble sur lequel est définie la relation binaire, ici :

$$\mathbb{Z} = \bigsqcup_{k=0}^{n-1} \overline{k} = \bigsqcup_{c \in \mathbb{Z}/n\mathbb{Z}} c$$

Avec les classes non vides

Propriété

Compatibilité de $\equiv_n$ avec les opérations de $\mathbb{Z}$

$$\forall a, b, a', b' \in \mathbb{Z}, (a \equiv a'[n] \text{ et } b \equiv b'[n]) \Rightarrow a + b \equiv a' + b'[n] \text{ et } ab \equiv a'b'[n]$$

Propriété

Soit $m \neq 0$ Alors

$$\forall a, b \in \mathbb{Z}, a \equiv b[n] \Leftrightarrow ma \equiv mb[n]$$

Propriété : Avant première

Soit $a, b \in \mathbb{Z}/n\mathbb{Z}$

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$\overline{a} \times \overline{b} = \overline{a \times b}$$

Propriété

$$(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}) \text{ est un anneau}$$

En pratique, on note $\dot{+}$ et $\dot{\times}$ --> $+$ et $\times$ (abus pratique)

Propriété

Soit $a \in \mathbb{Z}$ Alors

$$(\exists u \in \mathbb{Z}, au \equiv 1[n]) \Leftrightarrow a \wedge n = 1$$

Petit théorème de Fermat :

Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tel que $p \nmid a$
Alors :

$$a^{p-1} \equiv 1[p]$$

Lemme 1

Soit $p \in \mathcal{P}$
Alors :

$$\forall a \in \mathbb{N}, a^p = a[p]$$

Lemme 2

$$\forall p \in \mathcal{P}, \forall k \in [\![1, p-1]\!], p \mid \binom{p}{k}$$

Méthode de résolution des équations de la forme $ax + by = c$

Inconnues : $(x, y) \in \mathbb{Z}^2$ (a, b, c sont des constantes dans $\mathbb{Z}$)

- Existence des solutions
  Notons $d = a \wedge b$

- Si $d \mid c$ alors il existe des solutions par la relation de Bézout :
  On trouve d'abord : $u, v \in \mathbb{Z}$
  tel que $au + bv = d$
  Puis en multipliant par le facteur adéquat e,
  $a(ue) + b(ve) = de = c$
- Si $d \nmid c$
  il n'y a pas de solutions
  On le démontre par l'absurde.
  Si x, y étaient solutions de (E)
  On aurait $d \mid a$ et $d \mid b$
  Donc $d \mid ax + by = c$
  Contradiction

- Déterminer l'ensemble des solutions
  On se place dans le cas ou les solutions existent
  i.e. $d \mid c$ ou $d = a \wedge b$
  Etape 1 : Simplification
  On pose : $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$, $c' = \frac{c}{d}$
  et alors pour $(x, y) \in \mathbb{Z}$

  $$(E) \Leftrightarrow (E') : a'x - b'y = c'$$

  et on a $a' \wedge b' = 1$
  Quitte a faire cette etape avant de mettre des notations en on suppose dès le départ que $a \wedge b = 1$

  Etape 2 : Solutions particulières
  On est dans le cadre d'une équation

  $$(E) : ax + by = c \text{ avec } a, b, c \in \mathbb{Z}$$

  On peut alors déterminer $u, v \in \mathbb{Z}$ tel que $au + bv = 1$ (relation de Bézout)
  En posant

  $$x_0 = cu \text{ et } y_0 = cv$$

  On obtiens une solution particulière (x_0, y_0) de (E)

Etape 3 : Résolution (Rédaction subtile)

Pour $(x, y) \in \mathbb{Z}^2$,

$$(E) \Leftrightarrow ax + by = ax_0 + by_0 \Leftrightarrow a(x - x_0) = b(y_0 - y) : (\star)$$

On résout $(\star)$ par Analyse-Synthèse

Analyse :

Supposons que (x, y) vérifie $(\star)$

Alors $a \mid a(x - x_0) = b(y_0 - y)$

et comme $a \wedge b = 1$ par le théorème de Gauss,

$a \mid y_0 - y$ i.e. il existe $k \in \mathbb{Z}$

tel que : $y = y_0 - ak$

En reportant dans $(\star)$, on a $a(x - x_0) = bak$ (Stabilité)

et comme $a \neq 0$, $x = x_0 + bk$

Synthèse :

Pour $k \in \mathbb{Z}$,

$a((x_0 + bk) - x_0) = abk = b(y_0 - (y_0 - ak))$

Conclusion :

L'ensemble des solutions de (E) est celui de $(\star)$ qui est :

$$\mathcal{S}_E = (x_0, y_0) + \mathbb{Z}(b, -a)$$

Autrement dit :

$$\mathcal{S}_E = \{(x_0, y_0) + k(b, -a); k \in \mathbb{Z}\} = \{(x_0 + kb, y_0 - ka); k \in \mathbb{Z}\}$$

Important :

En pratique il faut tout refaire dans le cas particulier ou vous êtres placés