Arithmétique dans $\mathbb{Z}$
Résumé

Divisibilité dans $\mathbb{Z}$.

Déf Soient a et $b \in \mathbb{Z}$.
On dit que a **divise** b **si et ssi** $(\exists k \in \mathbb{Z},\ b = ka)$

Notations a/b

Propriétés immédiates
Tous les nombres seront des entiers relatifs.
1) $(\pm 1) / a$.
2) $(\pm a) / a$ et $a / (\pm a)$.
3) a / a
4) i) $a/b \Leftrightarrow (\pm a) / (\pm b)$
   ii) $a/b \Leftrightarrow a / |b| \Leftrightarrow |a| / |b|$.

Prop
1) Supp que a et $b \in \mathbb{N}^*$, on a $a/b \Rightarrow a \leq b$.
2) Supp que a et $b \in \mathbb{Z}^*$, on a $a/b \Rightarrow |a| \leq |b|$.

Prop Soient a et $b \in \mathbb{Z}$ on a :
$a/b \Leftrightarrow (b\mathbb{Z}) \subset (a\mathbb{Z})$.

Prop

Les entiers ici sont dans $\mathbb{Z}$.

1) $(a/b$ et $b/c) \Rightarrow a/c$

2) $(a/b$ et $b/a) \Leftrightarrow |a| = |b| \Leftrightarrow a = \pm b$

3) $\begin{pmatrix} a/b \\ a/c \end{pmatrix} \Rightarrow a/(\alpha b + \beta c)$ (où α et $\beta \in \mathbb{Z}$)

Coroll Si a et $b \in \mathbb{N}$, alors :

$(a/b$ et $b/a) \Leftrightarrow a = b$

Coroll $/$ est une relation d'ordre dans $\mathbb{N}$.

Vocab :

Si a/b et b/a, on dit que a et b sont associés.

Notations : $a \equiv b$

NB : $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$.

Prop 8 : Éléments inversibles de $\mathbb{Z}$

Soit $a \in \mathbb{Z}$. Les propositions suivantes sont équivalentes

1) a inversible de l'anneau $(\mathbb{Z}, +, \times)$

2) $a/1$

3) $a = \pm 1$

NB : $U(\mathbb{Z}) = \{-1, 1\}$, le groupe des éléments inversibles de l'anneau $(\mathbb{Z}, +, \times)$

Division euclidienne dans $\mathbb{Z}$

Prop (Théorème de la division euclidienne)

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

$\exists ! (q, r) \in \mathbb{Z}$ tel que $\begin{cases} 1) \ a = bq + r \\ 2) \ 0 \leq r < |b| \end{cases}$

R/R : Si $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, on a :

$$\begin{cases} a = bq + r \\ 0 \leq r \leq b - 1 \end{cases}$$

Prop Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, on a :

$b \mid a \iff r = 0$

où r est le reste de la div euclidienne de a par b

Pgcd de deux entiers relatifs non tous deux nuls

Déf Soient a et $b \in \mathbb{Z}$, non tous deux nuls.

Le plus grand élément de $D(a) \cap D(b)$ s'appelle **le plus grand commun diviseur** à a et à b.

Il se note $a \wedge b$.

NB : Il se note aussi $\text{pgcd}(a, b)$.

NB : Le pgcd est toujours **positif**.

Prop immédiates du pgcd

1) $\forall a \in \mathbb{N}^*, a \wedge a = a$
2) $\forall a \in \mathbb{Z}^*, a \wedge a = |a|$
3) Si (b/a) alors $a \wedge b = |b|$
4) $a \wedge 1 = 1$
5) $a \wedge b = b \wedge a$
6) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

<< on note aussi $a \wedge b \wedge c$ ou pgcd (a, b, c) >>

Prop :

Soient a, b et $c \in \mathbb{Z}^*$. On a :

1) $a \wedge b = |a| \wedge |b|$
2) $\exists (u, v) \in \mathbb{Z}^2, a \wedge b = au + bv$
   (Relation de Bezout)
3) $(d/a$ et $d/b) \Leftrightarrow d/(a \wedge b)$
4) $(ca) \wedge (cb) = c \cdot (a \wedge b)$
5) $\left(\frac{a}{a \wedge b}\right) \wedge \left(\frac{b}{a \wedge b}\right) = 1$

Vocabulaire :

Si $a \wedge b = 1$, on dit que a et b sont premiers entre eux.

NB :

$\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux.

PPCM de deux entiers relatifs non nuls

Prop

1) i) $\forall a \in \mathbb{N}^*,\ a \vee a = a$

   ii) $\forall a \in \mathbb{Z}^*,\ a \vee a = |a|$

2) $a \vee b = |a| \vee |b|$

3) $\forall a \in \mathbb{Z}^*,\ 1 \vee a = |a|$

4) $\begin{pmatrix} a \mid m \\ b \mid m \end{pmatrix} \Leftrightarrow (a \vee b) \mid m$

5) $\forall a, b \in \mathbb{Z}^*,\ a \mid b \Rightarrow a \vee b = |b|$

6) $a \vee b = b \vee a$

   $(a \vee b) \vee c = a \vee (b \vee c)$

Prop

Soient a et $b \in \mathbb{Z}^*$. On a :

$$(a \wedge b) \times (a \vee b) = |ab|$$

Théorèmes classiques

Prop : (Théorème de Bezout)

Soient $a, b \in \mathbb{Z}^*$. On a :

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

Prop (Lemme d'Euclide)

Si $\begin{pmatrix} a \mid m \\ b \mid m \\ a \wedge b = 1 \end{pmatrix}$ alors $ab \mid m$

Prop (Théorème de Gauss)

Si $\begin{pmatrix} a \mid bc \\ a \wedge b = 1 \end{pmatrix}$ alors $a \mid c$

Nombres premiers

Déf

Soit $p \in \mathbb{N}^*$.

p est dit nombre premier si et seulement si les conditions suivantes sont vérifiées :

1) $p \geqslant 2$
2) Les seuls diviseurs positifs de p sont 1 et p.

Prop (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Prop (Théorème fondamental de l'arithmétique)

Tout entier $n \geqslant 2$ peut s'écrire comme produit de facteurs premiers.
De plus, cette écriture est unique à l'ordre près des facteurs premiers.

(Décomposition d'un entier en produit de facteurs premiers)

Soit $a \geq 2$.

a peut s'écrire sous la forme :

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

où $\mathcal{P}$ désigne l'ensemble des nombres premiers.
$v_p(a) \in \mathbb{N}$.

$v_p(a)$ s'appelle la valuation p-adique de a.

Prop :

Pour $a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$ et $b = \prod_{p \in \mathcal{P}} p^{v_p(b)}$, on a :

1) $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$

2) $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$

3) $a \mid b \iff (\forall p \in \mathcal{P},\ v_p(a) \leq v_p(b))$

Congruence dans $\mathbb{Z}$

Déf

Soient a et $b \in \mathbb{Z}$. Soit $n \in \mathbb{N}^*$.

On dit que a est congru à b modulo n si et ssi :

$$\exists k \in \mathbb{Z},\ a = b + nk$$

Notation : $a \equiv b\ [n]$

Résumé :

$$a \equiv b\ [n] \iff (\exists k \in \mathbb{Z},\ a = b + nk) \iff n \mid (a-b)$$

Prop

1) $a \equiv 0\ [n] \iff n \mid a \iff (a \text{ multiple de } n)$
2) $\forall k \in \mathbb{Z},\ kn \equiv 0\ [n]$
3) $\forall a \in \mathbb{Z},\ a \equiv a\ [n]$

Prop

Soient $n \in \mathbb{N}^*$ et $(a,b,c,d) \in \mathbb{Z}^4$.

1) La relation de congruence $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$.
2) $a \equiv r\ [n]$
où r le reste de la division euclidienne de a par n.
3) i) $a \equiv b\ [n] \implies a + c \equiv b + c\ [n]$
ii) $\begin{pmatrix} a \equiv b\ [n] \\ c \equiv d\ [n] \end{pmatrix} \implies a + c \equiv b + d\ [n]$
4) i) $a \equiv b\ [n] \implies ac \equiv bc\ [n]$
ii) $\begin{pmatrix} a \equiv b\ [n] \\ c \equiv d\ [n] \end{pmatrix} \implies a \cdot c \equiv b \cdot d\ [n]$
iii) $a \equiv b\ [n] \implies (\forall k \in \mathbb{N},\ a^k \equiv b^k\ [n])$

Petit théorème de Fermat

Prop

Soit $a \in \mathbb{N}^*$ et q un nombre premier. On a :

$$q \wedge a = 1 \iff q \nmid a$$

À retenir !

Soit q un nombre premier.

$$\forall\, 1 \leq k \leq q-1,\ k \wedge q = 1$$

Prop

Soit q un nombre premier. On a :

1) $\forall\, 1 \leq k \leq q-1,\ q \mid C_q^k$

2) $\forall a \in \mathbb{N},\ a^q \equiv a\ [q]$

Corollaire (Petit théorème de Fermat)

Soit q un nombre premier.

$$\forall a \in \mathbb{N}^*,\ q \wedge a = 1 \Rightarrow a^{q-1} \equiv 1\ [q]$$

Autrement dit : $q \nmid a \Rightarrow a^{q-1} \equiv 1\ [q]$

Fin