MPSI – Colle 18 (19 au 23 février 2024) : Arithmétique

Chapitre 17 : Arithmétique

Dans ces lignes, le terme "entier" est synonyme "d'entier relatif".

1 – Divisibilité dans $\mathbb{Z}$

Définitions : diviseur et multiple. Exemples : pour tout $n \in \mathbb{Z}$, $1|n$ et $(-1)|n$; si $n \in \mathbb{Z}\setminus\{\pm 1\}$, n admet au moins quatre diviseurs : ± 1 et $\pm n$. 0 ne divise aucun entier non nul, et est multiple de tout entier.

Propriétés. Soient a, b, c et d entiers.

1/ $(\forall\ (n,m) \in \mathbb{Z}^2,\ a|b \text{ et } a|c) \implies (a|nb+mc)$

2/ $(a|c \text{ et } b|d) \implies (ab|cd)$

Notation. Soit a un entier. On note $a\mathbb{Z} = \{ka \,/\, k \in \mathbb{Z}\}$.

Propriétés. Soient a, b et c dans $\mathbb{Z}$.
Alors : 1/ $a|a$ 2/ $[a|b \text{ et } b|a] \implies |a| = |b|$ $[a|b \text{ et } b|c] \implies a|c$

Conséquence : la relation de divisibilité est une relation d'ordre dans $\mathbb{N}$.

2 – Division euclidienne dans $\mathbb{Z}$ et PGCD

Théorème (division euclidienne). Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q,r) d'entiers tels que : $a = bq + r$ et $0 \leqslant r < b$.
Conséquence : $b|a \iff r = 0$.

PGCD. Définition et propriétés.

Algorithme d'Euclide pour le calcul du PGCD de deux entiers.

Théorème (Bezout). $\forall\ (a,b) \in \mathbb{Z}^2,\ \exists\ (u,v) \in \mathbb{Z}^2,\ au + bv = a \wedge b$.

Corollaire. Soient a et b deux entiers. On a : $[d|a \text{ et } d|b] \iff [d|\ a \wedge b]$.

Ainsi, $a \wedge b$ est aussi le plus grand commun diviseur à a et b pour la relation (d'ordre, dans $\mathbb{N}$) de divisibilité.

Corollaire. Soient a et b deux entiers. On a : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\,\mathbb{Z}$.

Corollaire. Soient a et b deux entiers. S'il existe deux entiers u et v tels que $au + bv = 1$, alors $a \wedge b = 1$

3 – Congruences

Définition. Soient a, b et n trois entiers relatifs. On dit que a **est congru à** b **modulo** n si $b - a$ est multiple de n, c'est à dire s'il existe $k \in \mathbb{Z}$ tel que : $b = a + kn$. On le note $a \equiv b\ [n]$.

Rque : $a \equiv 0\ [n]$ si et seulement si a est multiple de n.

Lemme : la relation de congruence est une relation d'équivalence ; propriétés algébriques des congruences.

Lemme. Soit n un entier, $n \geqslant 2$, et a un entier quelconque. On a : $a \equiv r\ [n]$, où r est le reste dans la division euclidienne de a par n.

Définition. Soit a et n deux entiers, avec $n \neq 0$. On appelle **inverse de** a **modulo** n un entier b tel que $ab \equiv 1\ [n]$.

Exemples. 3 a pour inverse 5 modulo 7. Mais 12 et -2 sont aussi des inverses de 3 modulo 7. Plus généralement : si b est un inverse de a modulo n, alors $b + kn$ est un inverse de a modulo n (pour tout $k \in \mathbb{Z}$).

Propriété. Soient a et b deux entiers, avec $b \neq 0$. L'entier a est inversible modulo b si et seulement si $a \wedge b = 1$.

4 – Entiers premiers entre eux, Lemme de Gauss

Définition. Deux entiers a et b sont **premiers entre eux** si $a \wedge b = 1$.

Lemme. Soient a et b deux entiers non nuls. On note $d = a \wedge b$.
Alors : $\exists!\ (a',b') \in \mathbb{Z}^2$ tel que : $a = da'$, $b = db'$ et $a' \wedge b' = 1$.

Théorème (Lemme de Gauss). Soient a, b et c trois entiers.
Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.

Propriété. Si $a \wedge b = 1$, alors : $a|c$ et $b|c$ impliquent $ab|c$.

5 – L'équation diophantienne (E) $ax + by = c$

Théorème. S'il existe $(X,Y) \in \mathbb{Z}^2$ un couple solution de (E), alors l'ensemble des solutions de (E) est : $\{(X + kb',\ Y - ka')\ /\ k \in \mathbb{Z}\}$

On dispose donc d'une formule explicite donnant la solution générale de (E), s'il en existe au moins une.

Deux cas peuvent se présenter :

➤ Si $a \wedge b | c$: alors l'équation (E) possède des solutions. On en trouve une en déterminant les coefficients de Bezout de a et b, puis toutes à l'aide de la propriété ci-dessus.

➤ Sinon (si c n'est pas multiple de $a \wedge b$) : aucune solution.

6 – Nombres premiers

Définition. Un nombre **premier** est un entier admettant exactement deux diviseurs dans $\mathbb{N}$: 1 et lui-même.

Notation. On note $\mathscr{P}$ l'ensemble des nombres premiers.

Observation. Tout entier $n \geqslant 2$ composé admet au moins un diviseur compris entre 2 et $\lfloor \sqrt{n} \rfloor$.

Théorème. Soit $p \in \mathbb{N}$. LASSE :

1/ p est premier

2/ p est premier avec tout entier qu'il ne divise pas.

3/ p est premier avec tout entier compris entre 2 et $p-1$.

➤ *Théorème de Fermat*

Lemme. Soit $p \in \mathscr{P}$. Alors : $\forall\, k \in [\![1, p-1]\!], \quad p \mid \binom{p}{k}$

"Petit" théorème de Fermat. $\forall\, p \in \mathscr{P},\ \forall\, m \in \mathbb{Z},\ m^p \equiv m\ [p]$.

Corollaire. $\forall\, p \in \mathscr{P},\ \forall\, m \in \mathbb{Z} \backslash p\mathbb{Z},\ m^{p-1} \equiv 1\ [p]$.

➤ *Décomposition en facteurs premiers d'un entier*

Lemme. Tout entier $n \geqslant 2$ admet au moins un diviseur premier.

Corollaire. Il existe une infinité de nombres premiers.

Théorème(décomposition en facteurs premiers). Soit N un entier $\geqslant 2$. Il existe n nombres premiers $p_1, \ldots, p_n$ et n entiers naturels $\alpha_1, \ldots, \alpha_n$ tels que : $n = \prod_{i=1}^{N} p_i^{\alpha_i}$.

➤ *Notion de valuation p-adique*

Questions de cours

➤ **Théorème (division euclidienne)**. Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que : $a = bq + r$ et $0 \leqslant r < b$.

➤ **Propriété**. Soient a et b deux entiers. On a : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\,\mathbb{Z}$.

➤ **Propriété**. Soit a et b deux entiers, $b \neq 0$. L'entier a est inversible modulo b si et seulement si $a \wedge b = 1$.

➤ **Théorème (Lemme de Gauss)**. Soient a, b et c trois entiers. Si $a | bc$ et $a \wedge b = 1$ alors $a | c$.

➤ **Théorème (Euclide)**. Il existe une infinité de nombres premiers.

➤ **Propriété**. $\forall\, p \in \mathscr{P},\ \forall\, k \in [\![1, p-1]\!], \quad p \mid \binom{p}{k}$

➤ **Théorème (Fermat)**. Soit p un nombre premier. Alors : $\forall\, m \in \mathbb{Z},\ m^p \equiv m\ [p]$.