Chapitre 14 : Arithmétique

1 Divisibilité et division euclidienne

On étend à $\mathbb{Z}$ la définition de la divisibilité dans $\mathbb{N}$.

Définition 1.

Soit $(a,b) \in \mathbb{Z}^2$.
On dit que b divise a ou que b est un diviseur de a ou encore que a est un multiple de b s'il existe $c \in \mathbb{Z}$ tel que $a = bc$.
Si b est un diviseur de a on note $b|a$.

Remarque 1.
- *1 et -1 divisent tous les entiers mais ne sont divisibles que par 1 et -1.*
- *0 est multiple de tous les entiers mais n'est diviseur que de lui-même.*
- *L'ensemble des multiples de b se note $b\mathbb{Z} = \{bn \mid n \in \mathbb{Z}\}$.*
- *La relation $|$ est réflexive et transitive mais ni symétrique, ni antisymétrique (par exemple $5|-5$, $-5|5$ mais $5 \neq -5$). Ce n'est donc pas une relation d'ordre.*

▶ Exemple : 1 Trouver tous les diviseurs de 12.
▶ Exemple : 2 : Montrer que si $n \geq 1$, $3 \times 5^{2n-1} + 2^{3n-2}$ est divisible par 17.

Propriété 1.

Soient a et b deux entiers relatifs.
- *$(a|b)$ et $(b|a) \iff |a| = |b|$. On dit que a et b sont associés.*
- *Si $(u,v) \in \mathbb{Z}^2$ alors $(d|b$ et $d|a) \implies d|au + bv$.*
- *Si $x \in \mathbb{Z}^*$ alors $a|b \iff ax|bx$.*

Théorème 1 (Division euclidienne dans $\mathbb{Z}$).

Soient $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ $\exists!\,(q,r) \in \mathbb{Z}^2$ $a = bq + r$ et $0 \leqslant r < |b|$
q et r s'appellent respectivement quotient et reste de la division euclidienne de a par b.

Remarque 2. *Soit a un entier et b un entier non nul. b divise a ssi le reste de la division euclidienne de a par b est nul.*
Division euclidienne dans $\mathbb{N}$: Soient $(a,b) \in \mathbb{N} \times \mathbb{N}^*$ $\exists!\,(q,r) \in \mathbb{N}^2$ $a = bq + r$ et $0 \leqslant r < b$. On a alors $q = \left\lfloor \frac{a}{b} \right\rfloor$.

▶ Exemple : 3 Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. On suppose que le reste et le quotient de la division euclidienne de a par b sont les mêmes que le reste r et le quotient q de la division euclidienne de $a + 45$ par $b + 3$, déterminer q.
▶ Exemple : 4 Caractériser a et b sachant que le reste et le quotient de la division euclidienne de a par b valent respectivement 10 et 16. Même question si de plus $(a - 3b) = 426$.

2 PGCD et algorithme d'Euclide

Définition 2 (PGCD de deux entiers naturels sont l'un au moins est non nul).

Soient a et b deux entiers naturels dont l'un au moins est non nul. Le PGCD de a et de b, noté $a \wedge b$, est le plus grand élément (pour l'ordre naturel dans $\mathbb{N}$) de l'ensemble des diviseurs communs à a et à b.

Exemple : $15 \wedge 24$, $15 \wedge 0$
L'ensemble des diviseurs communs à a et b est une partie de $\mathbb{N}$ non vide puisqu'il contient 1 et majorée par exemple par ab ou $\max(ab)$. Il possède donc un plus grand élément supérieur ou égal à 1.

Propriété 2 (Propriétés de $a \wedge b$).

Soient a et b deux entiers naturels non nuls.
- $a \wedge b = b \wedge a$.
- $a \wedge 1 = 1$
- $a \wedge b = b$ *ssi* $b|a$.
- *Si* $a = bq + r$ *avec* $(q, r) \in \mathbb{N}^2$ *alors* $a \wedge b = b \wedge r$.
- *l'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de $a \wedge b$.*
- $a \wedge b$ *est le plus grand élément (au sens de la divisibilité) de l'ensemble des diviseurs communs à a et b.*
- *Pour* $k \in \mathbb{N}^*$, $(ka) \wedge (kb) = k(a \wedge b)$.

Propriété 3 (Calcul pratique du PGCD).

Le PGCD est le dernier reste non nul dans l'algorithme d'Euclide

▶ Exemple : 5 Déterminer le PGCD de 4653 et 299 avec l'algorithme d'Euclide.

Définition 3 (PGCD de deux entiers relatifs).

Soient a et b deux entiers relatifs. Le PGCD de a et de b, noté $a \wedge b$, est le plus grand élément de l'ensemble des diviseurs communs à a et à b.

On a $a \wedge b = |a| \wedge |b|$.
Point méthode : le pgcd de a et de b est l'unique entier naturel d tel que $d|a$, $d|b$ et si $n \in \mathbb{Z}$ est tel que $n|a$ et $n|b$ alors $n|d$.

Propriété 4 (Relation de Bézout).

Si a et b sont deux entiers relatifs non nuls, $\exists (u, v) \in \mathbb{Z}^2,\ au + bv = a \wedge b$. *$(u, v$ est appelé couple de coefficients de Bézout.*

▶ Exemple : Si d est tel que $d|a$ et $d|b$ et $\exists (u, v) \in \mathbb{Z}^2,\ au + bv = d$ alors d est le pgcd de a et de b. Autrement dit d est le seul multiple commun à a et à b qui s'exprime sous la forme d'une combinaison linéaire de a et de b.
Pas unicité des coefficients : si (u, v) est un tel couple alors $(u - b, v + a)$ aussi.
Détermination d'un couple de coefficients de Bézout par l'algorithme d'Euclide étendu.

Définition 4 (PPCM de deux entiers naturels sont l'un au moins est non nul).

Soient a et b deux entiers naturels non nuls. Le PPCM de a et de b, noté $a \vee b$, est le plus petit élément non nul (pour l'ordre naturel dans $\mathbb{N}$) de l'ensemble des multiples de a et de b.

Par convention, si $a = 0$ ou $b = 0$, $a \vee b = 0$.

Propriété 5 (Propriétés de $a \vee b$).

Soient a et b deux entiers naturels non nuls.
- $a \vee b$ *est le plus petit élément (au sens de la divisibilité) de l'ensemble des multiples communs de a et de b.*
- *Pour* $k \in \mathbb{N}^*$, $(ka) \vee (kb) = k(a \vee b)$.
- *Si* $a \wedge b = 1$ *alors* $a \vee b = ab$.
- $ab = (a \vee b)(a \wedge b)$

Point méthode : le ppcm de a et de b est l'unique entier naturel m tel que $a|m$, $b|m$ et si $n \in \mathbb{N}$ est tel que $a|n$ et $b|n$ alors $m|n$.
La démonstration de cette propriété utilise les propriétés 6 et 7 ci-dessous.

3 Entiers premiers entre eux

Définition 5 (Couples d'entiers premiers entre eux).

Deux entiers dont le PGCD est égal à 1 sont dits premiers entre eux.

Exemples : 3 et 5, 9 et 22, ...

Théorème 2 (Théorème de Bézout).

Pour tout $a, b \in \mathbb{Z}^*$, $a \wedge b = 1$ ssi $\exists u, v \in \mathbb{Z}$, $au + bv = 1$.

Propriété 6 (Lemme de Gauss).

Soient a, b, c trois entiers relatifs non nuls. Si $a|bc$ et si $a \wedge b = 1$ alors $a|c$.

Propriété 7 (Forme irréductible d'un rationnel).

Soient a et b deux entiers non tous les deux nuls et d leur PGCD. Il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.
Par conséquent, si $r \in \mathbb{Q}^*$, r admet un unique représentant $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $p \wedge q = 1$.

Propriété 8 (Produit et nombres premiers entre eux).

1. *Soient a, b et c trois entiers relatifs. Si $a \wedge b = 1$ et si $a \wedge c = 1$ alors $a \wedge bc = 1$.*
2. *Pour tout $(a, b_1, \cdots, b_n) \in (\mathbb{Z}^*)^{n+1}$, si $\forall i \in [[1, n]]$, $a \wedge b_i = 1$alors $a \wedge (b_1 b_2 \cdots b_n) = 1$*
3. *Si a et b sont premiers entre eux et divisent n, alors ab divise n.*

Le point 2 est en fait une équivalence : Un produit est premier avec un entier a ssi chacun de ses facteurs est premier avec a.

Définition 6 (PGCD d'un nombre fini d'entiers).

Soit $p \in \mathbb{N}^*$. Soit $(a_1, \cdots, a_p) \in \mathbb{Z}^p \setminus \{(0, \cdots, 0)\}$. Le PGCD de $a_1, \cdots, a_p$, noté $a_1 \wedge \cdots \wedge a_p$, est le plus grand élément de l'ensemble des diviseurs communs à $a_1, \cdots, a_p$.

Cas où l'un des a_i est nul.
Déterminer $6 \wedge 16 \wedge 24$ et $0 \wedge 16 \wedge 24$.

Propriété 9.

Soit $p \in \mathbb{N}^*$. Soit $(a_1, \cdots, a_p) \in \mathbb{Z}^p \setminus \{(0, \cdots, 0)\}$ et d leur PGCD. On a $\mathcal{D}(d) = \mathcal{D}(a_1) \cap \mathcal{D}(a_2) \cap \cdots \cap \mathcal{D}(a_p)$.

Propriété 10 (Relation de Bézout).

Soit $p \in \mathbb{N}^*$. Soit $(a_1, \cdots, a_p) \in \mathbb{Z}^p \setminus \{(0, \cdots, 0)\}$ et d leur PGCD. Il existe $(u_1, \cdots, u_p) \in \mathbb{Z}^p$ tel que $d = a_1 u_1 + \cdots + a_p u_p$.

Définition 7 (Entiers premiers entre eux dans leur ensemble).

$a_1, \cdots, a_p$ sont dits premiers entre eux dans leur ensemble lorsque $a_1 \wedge \cdots \wedge a_p = 1$.

Cela signifie qu'ils n'ont pas de diviseurs communs autres que 1 et -1.

Définition 8 (Entiers premiers entre eux deux à deux).

$a_1, \cdots, a_p$ sont dits premiers entre eux deux à deux lorsque $\forall (i, j) \in [[1, p]]^2$, $i \neq j \Rightarrow a_i \wedge a_j$.

Si les a_i sont premiers entre eux deux à deux alors ils sont premiers entre eux dans leur ensemble mais la réciproque est fausse. Par exemple, 4, 6 et 9 sont premiers entre eux dans leur ensemble mais ne sont pas premiers entre eux deux à deux.

Propriété 11 (Corollaire - théorème de Bézout).

Soit $p \in \mathbb{N}^*$. Soit $(a_1, \cdots, a_p) \in \mathbb{Z}^p \setminus \{(0, \cdots, 0)\}$. $a_1, \cdots, a_p$ sont premiers entre eux ssi il existe $(u_1, \cdots, u_p) \in \mathbb{Z}^p$ tel que $1 = a_1u_1 + \cdots + a_pu_p$.

4 Nombres premiers

Ici on se limite à l'ensemble des entiers naturels.

Définition 9.

On appelle nombre premier tout entier naturel différent de 1 n'admettant pour diviseurs que 1 et p.

Notation : l'ensemble des nombres premiers est noté $\mathcal{P}$.

Propriété 12.

- *Si $n \in \mathbb{N}^*$ n'est pas premier, il admet un diviseur p tel que $2 \leq p \leq \sqrt{n}$.*
- *Tout nombre premier est premier avec tous les entiers qu'il ne divise pas. En particulier, si p est un nombre premier alors $\forall k \in [[1, p-1]]$, $k \wedge p = 1$.*
- *Tout entier naturel supérieur ou égal à 2 admet au moins un diviseur premier.*
- *L'ensemble $\mathcal{P}$ est infini.*

Crible d'Eratosthène.
Deux nombres premiers distincts sont premiers entre eux.

Théorème 3 (Décomposition en produit de facteurs premiers).

Tout entier naturel n supérieur ou égal à 2 se décompose d'une unique façon, à l'ordre près des facteurs, en un produit fini de nombres premiers ; c'est-à-dire, il existe $N \in \mathbb{N}^*$, des entiers naturels premiers, deux à deux distincts, $p_1 < ... < p_N$ et des entiers naturels $\alpha_1, ..., \alpha_N$ strictements positifs tels que $n = p_1^{\alpha_1}...p_N^{\alpha_N}$, et cette dé"composition est unique. Les nombres premiers $p_1, ..., p_N$ sont appelés facteurs premiers de n.

★ Exercice : Décomposer en produit de facteurs premiers l'entier 2200.

Définition 10 (Valuation p-adique d'un nombre premier).

Soit p un nombre premier. Pour tout entier naturel non nul, on appelle valuation p-adique de n et l'on note $v_p(n)$ le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n.

Propriété 13 (Caractérisation de la valuation).

Soit p un nombre premier et n un entier strictement positif.
$v_p(n) = k$ ssi il existe $q \in \mathbb{N}$ tel que $p \wedge q = 1$ et $n = p^k q$.

dans la définition précédente on a donc $v_p(n) = \alpha_p$.

Propriété 14 (Valuation p-adique d'un produit).

Soit un nombre premier p et deux entiers naturels a et b non nuls. On a $v_p(ab) = v_p(a) + v_p(b)$.

Propriété 15 (expression du pgcd, du ppcm et caractérisation de la divisibilité à l'aide de la valuation).

Soient a et b deux entiers naturels non nuls.

1. *$b|a$ ssi pour tout nombre premier p, $v_p(b) \leq v_p(a)$.*
2. *Pour tout nombre premier p, $v_p(a \wedge b) = min(v_p(a), v_p(b))$ et $v_p(a \vee b) = max(v_p(a), v_p(b))$.*

Appliquer cette propriété à $a = p_1^{\alpha_1}...p_N^{\alpha_N}$ et $b = p_1^{\beta_1}...p_N^{\beta_N}$.

On retrouve ainsi le fait que $(a \wedge b).(a \vee b) = ab$.

Déterminer $a \wedge b$ et $a \vee b$ dans le cas où $a = 252$ et $b = 120$:

5 Congruences

Définition 11 (Relation de congruence modulo un entier sur $\mathbb{Z}$).

Soit $n \in \mathbb{Z}$. On dit que deux entiers relatifs a et b sont congrus modulo n si n divise $b - a$, c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. On écrit $a \equiv b[n]$.

Exemple : $9 \equiv 0[3]$, $7 \equiv 3[4]$....

Propriété 16 (Relation d'équivalence-classes d'équivalence).

La congruence modulo n est une classe d'équivalence sur $\mathbb{Z}$. Les classes d'équivalence sont appelées classes de congruence modulo n. Il y a exactement n classes de congruence modulo $n \in N$ lorsque $n \neq 0$.

Propriété 17 (Opérations sur les congruences : somme, produit).

Soit $n \in \mathbb{N}$. La congruence modulo n est compatible avec l'addition et la multiplication.

Définition 12 (Inverse modulo n).

Soit $(a, b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}^*$. On dit que b est l'inverse de a modulo n si $ab \equiv 1[n]$.

Propriété 18 (Existence d'un inverse modulo n).

Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. a admet un inverse modulo n ssi $a \wedge n = 1$.

Propriété 19 (Utilisation d'un inverse modulo n pour résoudre une congruence modulo n).

Soient a, b et c trois entiers relatifs et $n \in \mathbb{N}^*$. On suppose que b est l'inverse de a modulo n. Alors : $\forall x \in \mathbb{Z}$, $ax \equiv c[n]$ ssi $x \equiv bc[n]$.

▶ Exemple : : Résoudre l'équation $2x \equiv 3[5]$ d'inconnue $x \in \mathbb{Z}$.

Théorème 4 (Petit théorème de Fermat).

Pour tout nombre premier p et tout relatif n, on a $n^p \equiv n[p]$.

▶ Exemple : : Soit p un nombre premier.

1. Montrer que pour tout $(a, b) \in \mathbb{Z}^2$, on a $(a + b)^p \equiv a^p + b^p[p]$.
2. Soit n un entier non multiple de p. Montrer que $n^{p-1} \equiv 1[p]$.