Résumé du cours d'arithmétique

Les ensembles $\mathbb{N}$ et $\mathbb{Z}$
$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers naturels (entiers positifs).
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers relatifs.
$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ (entiers strictement positifs) et $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ (entiers relatifs non nuls).

Dans ce qui suit, entier est synonyme d'entier relatif.

1 Divisibilité dans $\mathbb{Z}$

a) Diviseurs et multiples

Définition. Soit a et b deux entiers. On dit que a **divise** b s'il existe un entier k tel que $b = ka$. On note $a|b$. On dit également que a est un **diviseur** de b ou que b est un **multiple** de a.

Remarque. Si a divise b, alors a divise $-b$, $-a$ divise b et $-a$ divise $-b$.

b) Propriétés

Propriétés 1. Soit a, b, c des entiers relatifs.
(1) Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. En particulier, $b \in \mathbb{Z}^*$ a un nombre fini de diviseurs.
(2) Si a divise b et b divise a alors $a = b$ ou $a = -b$.
(3) Si a divise b et b divise c alors a divise c.
(4) Si a divise b et c, alors, pour tous entiers n et m, a divise $nb + mc$.

La propriété (4) se généralise sans difficulté à 3 termes ou plus.

2 Division euclidienne

Théorème 2 (théorème de la division euclidienne). Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe des entiers q et r tels que $a = bq + r$ et $0 \leq r < b$. De plus, q et r sont uniques.

Définition. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Effectuer la **division euclidienne** de a par b, c'est trouver les entiers q et r tels que $a = bq + r$ avec $0 \leq r < b$. q est le **quotient** et r est le **reste** de la division euclidienne de a par b.

Propriété 3. Le reste de la division euclidienne de a par b est nul si et seulement si b divise a.

3 PGCD

a) Définition

Définition. Soit $a, b \in \mathbb{Z}^*$. Le plus grand entier qui divise à la fois a et b s'appelle le **plus grand commun diviseur** ou **pgcd** de a et b. On le note $\mathbf{pgcd(a, b)}$.

Remarque. $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$.

Propriété 4. Soit $a, b \in \mathbb{Z}^*$. Si a divise b alors $\text{pgcd}(a, b) = |a|$.

b) Algorithme d'Euclide

Théorème 5 (lemme d'Euclide). Soit $a, b \in \mathbb{Z}^*$. S'il existe des entiers k et s avec $s \neq 0$ tels que $a = bk + s$ alors les diviseurs communs à a et b sont exactement les diviseurs communs à b et s, et $\text{pgcd}(a, b) = \text{pgcd}(b, s)$.

Algorithme d'Euclide.
Soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$. On cherche $d = \text{pgcd}(a, b)$. On note $r_0 = b$. On effectue des divisions euclidiennes successives tant que le reste est non nul.

$$\begin{array}{rcll} a & = & r_0 q_1 + r_1 & 0 < r_1 < r_0 \\ b & = & r_1 q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2 q_3 + r_3 & 0 < r_3 < r_2 \\ \vdots & & & \\ r_{n-3} & = & r_{n-2} q_{n-1} + r_{n-1} & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} & = & r_{n-1} q_n + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_n q_{n+1} + 0 & r_{n+1} = 0 \end{array}$$

Théorème 6. Le pgcd de a et b est le dernier reste non nul obtenu par l'algorithme d'Euclide.

Remarque. Si $r_1 = 0$, c'est que b divise a, donc $\text{pgcd}(a, b) = b = r_0$.

Propriété 7. Soit $a, b \in \mathbb{Z}^*$. Si d divise a et b alors d divise $\text{pgcd}(a, b)$.

Remarque. On peut définir le pgcd de 3 entiers ou plus. La propriété 7 reste valable. Il n'y a pas d'équivalent de l'agorithme d'Euclide pour calculer le pgcd de 3 entiers. On peut utiliser la propriété suivante : si $d = \text{pgcd}(a, b)$ alors $\text{pgcd}(a, b, c) = \text{pgcd}(d, c)$.

c) Nombres premiers entre eux

Définition. Soit a et b deux entiers non nuls. On dit que a et b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$. On dit aussi que a est premier avec b.

Propriété 8. Soit $a, b \in \mathbb{Z}^*$ et $d = \text{pgcd}(a, b)$. Alors $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

4 Théorèmes de Bézout et de Gauss

a) Théorème de Bézout

Théorème 9 (théorème de Bézout). Soit a et b deux entiers non nuls.
1) Il existe des entiers relatifs u et v tels que $au + bv = \text{pgcd}(a, b)$.
2) S'il existe des entiers u et v tels que $au + bv = 1$ alors a et b sont premiers entre eux

b) Comment trouver une relation de Bézout

Trouver une relation de Bézout pour a et b, c'est trouver u et v tels que $au + bv = \text{pgcd}(a, b)$. On applique l'algorithme d'Euclide à a et b. Gardons les notations de 3b). On a $\text{pgcd}(a, b) = r_n$. On part de l'égalité donnant le pgcd et on écrit :

$$\text{pgcd}(a, b) = r_{n-2} - r_{n-1} q_n. \quad (*)$$

Puis on utilise la ligne précédente dans l'algorithme d'Euclide pour exprimer r_{n-1} (reste avec l'indice le plus élevé dans $(*)$) : $r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$, on remplace r_{n-1} dans $(*)$, on a :

$$\text{pgcd}(a, b) = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n = -r_{n-3} q_n + r_{n-2}(1 + q_n q_{n-1}). \quad (**)$$

On utilise la ligne précédente dans l'algorithme d'Euclide pour exprimer r_{n-2} (reste avec l'indice le plus élevé dans $(**)$), puis on remplace r_{n-2} dans $(**)$. On continue ainsi jusqu'à éliminer les restes $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$. On a alors le pgcd en fonction de a et b.

c) Théorème de Gauss

Théorème 10 (théorème de Gauss). Soit a, b, c des entiers non nuls. Si a divise bc et si a est premier avec b, alors a divise c.

Théorème 11 (corollaire du théorème de Gauss). Soit a_1, a_2, b des entiers tels que a_1 et a_2 sont premiers entre eux. Si a_1 et a_2 divisent b, alors le produit a_1a_2 divise b.

Remarque. Le théorème 11 se généralise à 3 entiers ou plus : si $a_1, a_2, \ldots, a_n$ sont deux à deux premiers entre eux et divisent b, alors $a_1a_2 \cdots a_n$ divise b.

d) Résoudre l'équation $ax + by = c$

On veut trouver toutes les solutions entières de l'équation : $\quad ax + by = c \qquad (E)$
où a, b, c sont des entiers donnés avec a, b non nuls, et x, y sont les inconnues.

Théorème 12. L'équation (E) admet des solutions si et seulement si $\text{pgcd}(a, b)$ divise c.

Méthode pour résoudre l'équation (E).
• Si $\text{pgcd}(a, b)$ ne divise pas c, il n'y a pas de solution (théorème 12).

• Si $\text{pgcd}(a, b)$ divise c, il y a des solutions par le théorème 12. Voici comment les trouver.

0) Simplifier l'équation
Si $\text{pgcd}(a, b)$ divise c, on divise l'équation par $\text{pgcd}(a, b)$, on trouve que (E) est équivalente à

$$a'x + b'y = c'$$

où $a' = a/\text{pgcd}(a, b)$, $b' = b/\text{pgcd}(a, b)$ et $c' = c/\text{pgcd}(a, b)$ (a', b', c' sont des entiers).
1) Solution particulière
Les entiers a' et b' sont premiers entre eux (propriété 8). Par le théorème de Bézout, il existe des entiers u et v tels que $a'u + b'v = 1$. Alors $x_0 = c'u$ et $y_0 = c'v$ forment une solution particulière de (E) car $a'x_0 + b'y_0 = c'(au + bv) = c'$.

2) Recherche de toutes les solutions
Exprimons les autres solutions en fonction de la solution particulière (x_0, y_0).

$$a'x + b'y = c' \iff a'x + b'y = a'x_0 + b'y_0 \iff a'(x - x_0) + b'(y - y_0) = 0$$

Soit $X = x - x_0$ et $Y = y - y_0$. Pour résoudre (E), il est équivalent de résoudre

$$a'X = -b'Y \quad (E')$$

a' et b' sont premiers entre eux et b' divise $a'X$, donc b' divise X par le théorème de Gauss, autrement dit il existe $k \in \mathbb{Z}$ tel que $X = kb'$. On a alors $ka'b' = -b'Y$, et en simplifiant par $b' \neq 0$ on trouve $Y = -ka'$. On vient de montrer que si (X, Y) est solution de (E') alors il existe $k \in \mathbb{Z}$ tel que $X = kb', Y = -ka'$. On vérifie facilement l'implication inverse : si $X = kb'$ et $Y = -ka'$, (X, Y) est bien une solution de (E') pour tout $k \in \mathbb{Z}$. Les deux implications donnent une équivalence : (X, Y) solution de (E') $\iff \exists k \in \mathbb{Z}, X = kb', Y = -ka'$.

Par conséquent, l'ensemble des solutions de (E) est :
$\boldsymbol{S = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}}$ **avec** $\boldsymbol{a' = \frac{a}{\text{pgcd}(a,b)}}$ **et** $\boldsymbol{b' = \frac{b}{\text{pgcd}(a,b)}}$.

Remarque. Ne pas apprendre par cœur ce résultat, mais refaire la méthode précédénte.

5 Nombres premiers

a) Reconnaître un nombre premier

Définition. Un entier $n \geq 2$ est **premier** si ses seuls diviseurs positifs sont 1 et n.

Propriété 13. Si l'entier $n \geq 2$ n'est divisible par aucun nombre premier $p \leq \sqrt{n}$, alors n est un nombre premier.

Théorème 14 (théorème d'Euclide). Il existe une infinité de nombres premiers.

b) Décomposition en produit de facteurs premiers

Théorème 15 (décomposition en facteurs premiers). Tout entier $n \geq 2$ peut s'écrire de façon unique

$$n = p_1p_2 \cdots p_r,$$

où $r \in \mathbb{N}^*$ et $p_1, p_2, \ldots, p_r$ sont des nombres premiers avec $p_1 \leq p_2 \leq \cdots \leq p_r$.

Définition. Soit $n \in \mathbb{N}^*$ et p un nombre premier.
• Si p divise n, on dit que p est un **facteur premier** de n
• Le plus grand entier k tel que p^k divise n s'appelle **l'exposant de p dans n**.

Dans le théorème 15, on peut regrouper les premiers identiques, on obtient l'énoncé suivant :
Théorème 15' (décomposition en facteurs premiers) Tout entier $n \geq 2$ peut s'écrire de façon unique

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

où $p_1, \ldots, p_s$ sont des nombres premiers distincts avec $p_1 < p_2 < \cdots < p_s$, et $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^*$.

Remarque. Dans le théorème 15', l'exposant de p_i dans n est α_i. Si un nombre premier p n'apparaît pas dans la décomposition de n, son exposant est 0.

c) Application à la divisibilité

Théorème 16 (application de la décomposition en facteurs premiers à la divisibilité). Soit a et b des entiers strictement positifs. Pour tout nombre premier p, notons $\alpha(p)$ l'exposant de p dans a et $\beta(p)$ l'exposant de p dans b. Alors a divise b si et seulement si pour tout nombre premier p on a : $\alpha(p) \leq \beta(p)$.

Théorème 17 (application de la décomposition en facteurs premiers au pgcd). Soit $a, b \in \mathbb{N}^*$ et p un nombre premier. Soit $\alpha(p)$ l'exposant de p dans a et $\beta(p)$ l'exposant de p dans b. Alors l'exposant de p dans $\text{pgcd}(a, b)$ est $\min(\alpha(p), \beta(p))$.

Remarque. Le théorème 17 reste valable pour calculer le pgcd de 3 entiers ou plus.

6 PPCM

Définition. Soit a et b deux entiers non nuls. Le plus petit entier strictement positif qui est à la fois multiple de a et b s'appelle le **plus petit commun multiple** ou **ppcm** de a et b. On le note $\boldsymbol{\text{ppcm}(a, b)}$.

Remarque. $\text{ppcm}(a, b) = \text{ppcm}(|a|, |b|)$.

Propriété 18. Soit $a, b \in \mathbb{Z}^*$. Si c est un multiple de a et b, alors c est un multiple de $\text{ppcm}(a, b)$.

Théorème 19 (application de la décomposition en facteurs premiers au ppcm). Soit $a, b \in \mathbb{N}^*$ et p un nombre premier. Soit $\alpha(p)$ l'exposant de p dans a et $\beta(p)$ l'exposant de p dans b. Alors l'exposant de p dans $\text{ppcm}(a, b)$ est $\max(\alpha(p), \beta(p))$.

Théorème 20 (relation entre pgcd et ppcm). Si $a, b \in \mathbb{Z}^*$, $\text{pgcd}(a, b).\text{ppcm}(a, b) = |ab|$.

Remarque. On peut définir le ppcdm de 3 entiers ou plus. La propriété 18 et le théorème 19 restent valables, mais le théorème 20 ne se généralise pas à 3 entiers. On peut utiliser la propriété suivante : si $\text{ppcm}(a, b) = m$ alors $\text{ppcm}(a, b, c) = \text{ppcm}(m, c)$.

7 Congruences

Dans la suite, on considère un entier $n \geq 2$.

a) Définition et propriétés

Définition. Soit $a, b \in \mathbb{Z}$. On dit que a **est congru à** b **modulo** n si $a - b$ est un multiple de n. On dit aussi que a et b sont congrus modulo n. On note $a \equiv b\ (n)$ ou $a \equiv b \bmod n$.

Remarques.
• La relation de congruence est symétrique : $a \equiv b\ (n) \iff b \equiv a\ (n)$.
• $a \equiv b\ (n) \iff -a \equiv -b\ (n)$.
• $a \equiv b\ (n) \iff \exists k \in \mathbb{Z}, a = b + kn$
• $a \equiv 0\ (n) \iff n$ divise a.

Propriété 21. Soit $a \in \mathbb{Z}$. Il existe un unique entier r tel que $a \equiv r\ (n)$ et $0 \leq r \leq n - 1$.
r est le reste de la division euclidienne de a par n.

Propriété 22. Si $a \equiv b\ (n)$ et $b \equiv c\ (n)$ alors $a \equiv c\ (n)$.

b) Compatibilité avec les opérations

Propriétés 23. Soit $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\ (n)$ et $c \equiv d\ (n)$. Alors
• $a + c \equiv b + d\ (n)$ et $ac \equiv bd\ (n)$.
• pour tout entier $k \geq 1$, $a^k \equiv b^k\ (n)$.

8 Équations de congruence

a) Quand simplifier $ab \equiv ac\ (n)$?

Propriété 24. Soit $a, b, c \in \mathbb{Z}$. S'il existe $u \in \mathbb{Z}$ tel que $ua \equiv 1\ (n)$ alors $ab \equiv ac\ (n)$ implique $b \equiv c\ (n)$.

Théorème 25. Soit $a \in \mathbb{Z}$. Il existe $u \in \mathbb{Z}$ tel que $au \equiv 1\ (n)$ si et seulement si $\text{pgcd}(a, n) = 1$.

Méthode pour trouver u comme dans le théorème : si $au + nv = 1$ est une relation de Bézout entre a et n, alors $au \equiv 1(n)$.

b) Résoudre l'équation $ax \equiv c\ (n)$

On veut trouver toutes les solutions entières de l'équation : $\quad ax \equiv c\ (n) \qquad (E)$

où a et c sont des entiers donnés avec a non nul, et où $x \in \mathbb{Z}$ est l'inconnue.

Cas où a et n sont premiers entre eux.

Propriété 26. Soit a et n des entiers premiers entre eux ($n \geq 2$) et $u \in \mathbb{Z}$ tel que $au \equiv 1\ (n)$. L'équation $ax \equiv c\ (n)$ est équivalente à $x \equiv uc\ (n)$.

Cas où a et n ne sont pas premiers entre eux.

x solution de (E) $\iff \exists k \in \mathbb{Z}, ax = c + kn \iff \exists k \in \mathbb{Z}$, (x, k) solution de $ax - kn = c$.

La dernière équation est de la forme $ax + by = c$ (avec $y = k$ et $b = n$), qui a été vue en 4.d). Si $\text{pgcd}(a, n)$ ne divise pas c, alors $ax - kn = c$ n'a pas de solution. Si $\text{pgcd}(a, n)$ divise c, on pose $a' = a/\text{pgcd}(a, n)$, $n' = n/\text{pgcd}(a, n)$ et $c' = c/\text{pgcd}(a, n)$. On a donc

$$x \text{ solution de (E)} \iff \exists k \in \mathbb{Z}, a'x - n'k = c' \iff a'x \equiv c'\ (n').$$

On est ramené au cas précédent puisque a' et n' sont premiers entre eux.

c) Systèmes de congruences

Théorème 27 (théorème des restes chinois). Si $n_1, n_2, \ldots, n_k$ sont des entiers positifs 2 à 2 premiers entre eux, alors, pour tous $a_1, \ldots, a_k \in \mathbb{Z}$, le système

$$\begin{cases} x & \equiv & a_1\ (n_1) \\ x & \equiv & a_2\ (n_2) \\ & \vdots & \\ x & \equiv & a_k\ (n_k) \end{cases}$$

a des solutions et, si x_0 est une solution particulière, alors l'ensemble des solutions s'écrit $\{x \in \mathbb{Z} \mid x \equiv x_0\ (n_1 n_2 \ldots n_k)\}$.

Méthode pour résoudre un système à deux équations (S) $\begin{cases} x & \equiv & a\ (n) \\ x & \equiv & b\ (m) \end{cases}$

$$\begin{aligned} x \text{ solution de (S)} &\iff \exists k, k' \in \mathbb{Z}, x = a + kn = b + k'm \\ &\iff x = a + kn \text{ avec } (k, k') \text{ solution de } kn - k'm = b - a \end{aligned}$$

On est ramené à résoudre une équation de la forme $AX + BY = C$, avec $X = k, Y = k'$.
On peut se contenter de chercher une solution particulière (k_0, k'_0), on en déduit une solution particulière de (S), puis on applique le théorème 27 pour avoir toutes les solutions de (S).

Méthode pour résoudre un système de congruence à 3 équations.

$(S3)$ $\begin{cases} x & \equiv & a\ (n) \\ x & \equiv & b\ (m) \\ x & \equiv & c\ (p) \end{cases}$ avec n, m, p des entiers 2 à 2 premiers entre eux.

1) On résout le système partiel $\begin{cases} x & \equiv & a\ (n) \\ x & \equiv & b\ (m) \end{cases}$

Selon le théorème 27, on trouve les solutions sous la forme $x \equiv x_0\ (nm)$ pour un certain $x_0 \in \mathbb{Z}$.

2) Le système (S3) est alors équivalent au système de congruence à 2 équations $\begin{cases} x & \equiv & x_0\ (nm) \\ x & \equiv & c\ (p) \end{cases}$

On résout ce système et on obtient les solutions de (S3).

9 Petit théorème de Fermat

Théorème 28 (théorème de Fermat). Soit p un nombre premier et x un entier. Alors :
• $x^p \equiv x\ (p)$,
• si p ne divise pas x, alors $x^{p-1} \equiv 1\ (p)$.