Memento 5/6 - Arithmétique

1. Divisibilité Soient a et b deux entiers relatifs. On dit que "a divise b" ou encore que "b est divisible par a", ce que l'on note $a|b$, si et seulement s'il existe un entier $c \in \mathbf{Z}$ tel que $a = bc$.

Ceci définit une relation binaire sur $\mathbf{Z}$. Elle est réflexive, antisymétrique et transitive, il s'agit donc d'une relation d'ordre. Par exemple $2 \mid 6$ mais $3 \nmid 5$ et $5 \nmid 3$, il s'agit donc d'un relation d'ordre partiel.

On dit que deux entiers a et b sont *premiers entre eux* s'ils n'ont aucun diviseur commun autre que 1. On note (a, b) le *plus grand commun diviseur* (en abrégé PGCD) de deux nombres a et b. On a donc $(a, b) = 1$ si et seulement si a et b sont premiers entre eux.

2. Primalité Un nombre $p \in \mathbf{N}$ est dit *premier* s'il est divisible uniquement par 1 et par lui même. Par convention, le nombre 1 n'est *pas* premier. Il y a une infinité de nombres premiers mais le théorème de raréfaction montre qu'il y en a de "moins en moins". Plus précisément le nombre $\pi(x) := \#\{p \text{ premier}, \ p \leq x\}$ de nombres premiers plus petits que x tend asymptotiquement vers $x/\ln x$, i.e.,

$$\lim_{x\to\infty} \pi(x)\frac{\ln x}{x} = 1. \tag{1}$$

Le théorème fondamental de l'arithmétique affirme que tout nombre entier se décompose de manière unique en un produit de facteurs premiers (à l'ordre des facteurs près).

3. Division euclidienne Soient $(a, b) \in \mathbf{Z} \times \mathbf{N} \setminus \{0\}$. Il existe un unique couple $(q, r) \in \mathbf{Z} \times \mathbf{Z}$ tel que

$$a = bq + r, \quad \text{avec } 0 \leq r < b. \tag{2}$$

On dit que le nombre q est le *quotient* et r le *reste* de la division euclidienne de a par b. Pour déterminer les valeurs q et r, on utilise l'algorithme de la division euclidienne étudié dans les classes du primaire.

4. Algorithme d'Euclide On calcule le PGCD de deux entiers a et b très simplement à l'aide des règles de réécriture suivantes :

$$(a, b) \mapsto \begin{cases} (b, a), & \text{si } a < b. \\ (b, a \mod b), & \text{si } b \neq 0. \\ a, & \text{si } b = 0. \end{cases}$$

5. Identité de Bezout Soient a, b deux éléments de $\mathbf{Z}$ et d un entier. Il existe deux entiers relatifs u et v tels que

$$au + bv = d. \tag{3}$$

si et seulement si $(a, b) \mid d$.

6. Algorithme d'Euclide étendu Si l'on cherche à calculer les deux valeurs u et v de (3), on applique l'algorithme d'Euclide aux deux entiers $a/(a, b)$ et $b/(a, b)$ (premiers entre eux) et on récupère tout d'abord la suite des quotients obtenus. Observons par exemple l'équation

$$165u + 42v = 6. \tag{4}$$

Les règles de réécritures ci-dessus donnent la suite

$$(165, 42) \mapsto (42, 39) \mapsto (39, 3) \mapsto (3, 0) \mapsto 3.$$

On a $3 \mid 6$, donc l'équation (5) admet bien (au moins) une solution (u, v) et en divisant les deux membres de l'égalité par 3 on obtient la nouvelle équation équivalente :

$$55u + 14v = 2. \tag{5}$$

On applique à présent l'algorithme d'euclide au couple $(55, 14)$ pour $d = 2$:

$$55 = \mathbf{3} \times \mathbf{14} + \mathbf{13}$$
$$\mathbf{14} = \mathbf{1} \times \mathbf{13} + \mathbf{1}$$

On dispose donc de 2 quotients $q_1 = 3$ et $q_2 = 1$. Il reste alors à calculer le produit des 2 matrices associées à q_1 et q_2 et (u, v) est donné par la deuxième colonne de la matrice résultat multiplié par $d = 2$. ices :

$$\begin{pmatrix} 0 & 1 \\ 1 & \mathbf{-3} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{-1} \\ -1 & \mathbf{4} \end{pmatrix}$$

et ainsi $(u, v) = 2 \times (-1, 4)$, soit

$$55 \times \mathbf{-2} + 14 \times (\mathbf{8}) = 2.$$

7. Théorème de Gauss Soient a, b et u des entiers. Si $(u, a) = 1$ et $u \mid ab$ alors $u \mid b$.

8. Théorème d'Euclide Soient a, b deux entiers et p un nombre premier. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

9. Anneau modulaire Soit $m \in \mathbf{N}$ et $(a, b) \in \mathbf{Z} \times \mathbf{Z}$. On définit la relation de *congruence modulo* m sur $\mathbf{Z}$ par "a est congru à b modulo m", ce que l'on note $a \equiv b \pmod m$ si et seulement s'il existe un entier $k \in \mathbf{Z}$ tel que

$$a - b = km. \tag{6}$$

Cette relation binaire est réflexive, symétrique et transitive. Il s'agit donc d'une relation d'équivalence et l'ensemble quotient est noté $\mathbf{Z}/m\mathbf{Z}$. L'application $\varphi : \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ définie par

$$x \mapsto x \pmod m. \tag{7}$$

est un morphisme d'anneaux surjectif. C'est à l'aide de cette propriété que l'on détermine les critères de divisibilité.

Les éléments inversibles de cet anneau sont les entiers x premiers avec m. Si m est premier alors tous les entiers non-nuls de $\mathbf{Z}/m\mathbf{Z}$ sont inversibles