PETIT COURS D'ARITHMÉTIQUE

ABRAHAM BROER

1. Introduction

Nous allons rappeler quelques propriétés élémentaires et bien connues des nombres entiers, rencontrées déjà dans le cours MAT1500. Par exemple, que chaque nombre entier est un produit de nombres premiers, et ce produit est unique à permutation près. Comme point de départ nous prenons l'idée qu'on sait compter !

Les nombres entiers se trouvent vraiment à la base de toutes les mathématiques, leur *existence* est un de ses axiomes même ! On suppose que les nombres entiers existent. Mais après, en acceptant les nombres naturels, on *construit* les nombres entiers négatifs, les fractions, les nombres réels et les nombres complexes.[1] Nous rappelons des définitions des fractions et des nombres réels.

2. Un rappel de définitions

Essayez avant tout de vous rappeler ou de vous imaginer comment les nombres naturels peuvent être caractérisé exactement (peut-être à l'école primaire ?), et puis l'addition et la multiplication.

L'idée est qu'il est possible de compter aussi loin qu'on veut à partir de 1 :

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$$

Les nombres qu'on obtient ainsi sont les nombres naturels. Donc implicitement, chaque nombre naturel a un unique successeur et chaque nombre sauf 1 a un unique nombre naturel comme prédécesseur.

Il existe essentiellement un unique ensemble $\mathbb{N}$ (l'ensemble des nombres naturels) avec un élément spécial noté 1, dont chaque élément a un unique *successeur* et dont chaque élément sauf 1 a un *unique prédécesseur*, et aucun sous-ensemble contenant 1 a la même propriété. En particulier, si $S \subseteq \mathbb{N}$ est un sous-ensemble avec les deux propriétés que $1 \in S$ et que avec $s \in S$ aussi son successeur est dans S, alors on a nécessairement que $S = \mathbb{N}$.

Nous allons accepter l'existence de $\mathbb{N}$. En consqence nous allons aussi accepter le principe d'induction mathématique ! Supposons que $P(n)$ est une préposition logique qui dépend du nombre naturel $n \in \mathbb{N}$. Supposons que $P(1)$ est vraie et que pour chaque $n \in \mathbb{N}$ la préposition $P(n)$ implique $P(n')$, où n' est le successeur de n. Alors, parce que $P(1)$ implique $P(2)$ et $P(1)$ est vraie, on a que $P(2)$ est aussi vraie. Donc $P(3)$ est vraie. Donc $P(4)$ est vraie. Et cetera. Donc $P(n)$ est vraie pour chaque $n \in \mathbb{N}$, parce qu'on peut compter jusqu'à n. De façon analogue pour les *définitions* inductives.

Date: August 31, 2009.

[1] L. Kronecker (1823-1891, un mathématicien allemand) a dit que Dieu a créé les nombres entiers et tout le reste est le travail d'homme. Voir le bouquin très lisible : Eric Temple Bell, Men of Mathematics, New York, Simon and Schuster, 1986. La bibliothèque a une version française.

Pour donner la définition d'addition sur $\mathbb{N}$ correctement, il faut nécessairement utiliser l'induction (c'est à dire : une propriété définissantes de l'ensemble des nombres naturels !).

Soit $n \in \mathbb{N}$ on va définir $n+m \in \mathbb{N}$ par induction sur m. Si $m = 1$ nous *définissons* $n+1$ comme le successeur (unique) de n. Supposons que $n+m$ a été défini. Alors on *définit* :

$$n + (m+1) := (n+m) + 1$$

(c'est à dire, le successeur de $n+m$). Alors par le principe d'induction on a maintenant défini $n+m$ pour chaque $n, m \in \mathbb{N}$.

Nous pouvez voir (comme on pourrait demander un enfant de 7 ans) que

$$a + b = b + a \text{ et } (a+b) + c = a + (b+c) \ :$$

Preuve. Soient $a, b \in \mathbb{N}$. Nous allons montrer par induction sur n que $(a+b)+n = a+(b+n)$. Si $n = 1$, alors $(a+b)+1 = a+(b+1)$ par définition de $+$. Supposons maintenant que $(a+b)+n = a+(b+n)$. Alors

$$\begin{aligned}
(a+b)+(n+1) &= ((a+b)+n)+1 \quad \text{(par définition de } +) \\
&= (a+(b+n))+1 \quad \text{(par hypothèse d'induction)} \\
&= a+((b+n)+1) \quad \text{(par définition de } +) \\
&= a+(b+(n+1)) \quad \text{(par définition de } +).
\end{aligned}$$

Donc par induction nous avons montré la règle d'associativité.

Pour montrer la commutativité, nous commençons par montrer que $a+1 = 1+a$ par induction sur a. Si $a = 1$ on a la tautologie $1+1 = 1+1$. Supposons que $a+1 = 1+a$. Alors

$$(a+1)+1 = (1+a)+1 = 1+(a+1)$$

et on conclut par induction.

Fixons a. Nous allons montrer par induction sur n que $a+n = n+a$. On vient de montrer le cas ou $n = 1$. Supposons maintenant que $a+n = n+a$, alors on a en utilisant l'associativité

$$a+(n+1) = (a+n)+1 = (n+a)+1 = 1+(n+a) = (1+n)+a = (n+1)+a.$$

On conclut par induction. □

Rappelez-vous la définition de "a est plus petit que b", pour des nombres naturels a et b. On a $n < m$ (ou $m > n$) si et seulement si il existe un $a \in \mathbb{N}$ tel que $m = n+a$. Si $n < m$ et $m < k$ alors $n < k$ (pourquoi ?). Pour deux nombres naturels a et b il existe trois alternatives : $a < b$ ou $b < a$ ou $a = b$ (pourquoi ?). On écrit $a \leq b$ si $a = b$ ou si $a < b$.

Exercice 2.1. Montrer que chaque sous-ensemble non-vide S de $\mathbb{N}$ *contient* un *unique* élément qui est plus petit que tous les autres éléments de S.

La définition du produit de deux nombres naturels ? Soit $n, m \in \mathbb{N}$ on définit $n \cdot m \in \mathbb{N}$ par induction sur n. Si $n = 1$ on définit $1 \cdot m := m$. Supposons $n \cdot m$ a été défini. Alors on pose $(n+1) \cdot m := (n \cdot m) + m$.

Pouvez vous voir pourquoi

$$a \cdot b = b \cdot a,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)\ ?$$

Exercice 2.2. Montrer la règle de distributivité:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

pour chaque $a, b, c \in \mathbb{N}$.

Puis, à partir de $\mathbb{N}$ on *construit* par induction l'ensemble des nombres entiers

$$\mathbb{Z} := \{\ldots, -12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots\}$$

en ajoutant à l'ensemble $\mathbb{N}$ un nombre appelé 0 premièrement (donc 0 n'était pas encore dans $\mathbb{N}$) et puis successivement pour chaque nombre naturel n un nouveau nombre appelé $-n$ (alors $-n$ n'était pas encore dans $\{-(n-1), -(n-2), \ldots, -1, 0, 1, 2, \ldots\}$). On obtiendra une extension unique des opérations $+$ et $\cdot$ tels que

$$n + (-n) = (-n) + n = 0,\ (-1) \cdot n = (-n),\ 0 + n = n + 0 = n,$$

pour chaque $n \in \mathbb{N}$. Les règles d'associativité, de commutativité et de distributivité restent vrai. On pose $-(-n) := n$ et $-0 := 0$, pour $n \in \mathbb{N}$. Et $a - b := a + (-b)$. Si $n \in \mathbb{N}$ on pose $|n| = |(-n)| = n$ et $|0| = 0$. On a $|a||b| = |ab|$ et $|a + b| \leq |a| + |b|$.

3. Division avec reste

En général, on ne peut pas diviser un nombre entier par un autre nombre entier et obtenir un nombre entier. Mais on peut diviser avec reste, comme on a vu dans MAT1500. Par exemple, si on divise 3599 par 112 on aura un reste :

$$3599 = 32 \cdot 112 + 15.$$

Théorème 3.1 (Division avec reste)**.** *Soient $a, b \in \mathbb{Z}$, où $b \neq 0$. Alors il existe deux unique nombres entiers, q, r tel que*

$$a = qb + r \text{ et } 0 \leq r < |b|.$$

Preuve. Premièrement nous allons montrer que si $a \geq 0$ et $b > 0$, alors il existe q et r tels que $a = qb + r$ et $0 \leq r < b$. Nous procédons par induction sur a. Si $a = 0$ alors $a = 0 = 0 \cdot b + 0$. Soit $0 < a$. Supposons par induction qu'il existe q' et r' tels que $a = q'b + r'$ et $0 \leq r' < b$. Il y a deux cas possible. (1) Si $r' + 1 = b$. Alors $a + 1 = q'b + r' + 1 = q'b + b = (q' + 1) \cdot b + 0$. (2) Si $r' + 1 < b$. Alors $a + 1 = q' \cdot b + (r' + 1)$. Donc il existe q et r tels que $a + 1 = qb + r$.

D'une manière analogue on montre le cas où $a \leq 0$ et $b > 0$.

Supposons maintenant $b < 0$. Alors $-b > 0$ et nous venons de montrer qu'ils existent q et r tels que $a = q(-b) + r$ et $0 \leq r < |b|$. Donc $a = (-q)b + r$.

Il reste à montrer l'unicité. Supposons que $a = qb + r$, $a = q'b + r'$, $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors $0 \leq |r - r'| < |b|$ et $|r - r'| = |q' - q| \cdot |b|$. Donc $0 \leq |q' - q| \cdot |b| < |b|$, et $0 \leq |q' - q| < 1$. Donc le nombre entier $|q' - q|$ est 0, d'où $q' = q$. Aussi $r = a - qb = a - q'b = r'$. □

On dit que "b divise a", ou $b|a$, s'il existe $q \in \mathbb{Z}$ tel que $a = qb$ (alors un tel q est unique). Propriétés élémentaires :

$$c|b \wedge\ b|a \Rightarrow c|a$$

$$b|a \wedge\ b|a' \Rightarrow b|(na + ma') \ \forall n, m \in \mathbb{Z}$$

$$\forall b:\ b|0\ \text{ et } \forall a:\ 1|a$$

$$b|a \Leftrightarrow |b| \mid |a|$$

$$b|a \wedge\ (a \neq 0)\ \Rightarrow |b| \leq |a|.$$

4. Le pgcd

Si $(a, b) \neq (0, 0)$, on définit le $\text{pgcd}(a, b)$ comme le plus grand diviseur commun de a et b, ou

$$\text{pgcd}(a, b) := \text{Max}\{d; d|a \wedge d|b\}.$$

Et on définit $\text{pgcd}(0, 0) := 0$. On a $\text{pgcd}(n, 0) = |n|$.

Lemme 4.1. *Soient $a, b, q, r \in \mathbb{Z}, b \neq 0$, tels que $a = qb + r$. Alors*

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

Preuve. Soit $d \in \mathbb{N}$ tel que $d|a$ et $d|b$, donc $d|(a - qb) = r$. Si $d \in \mathbb{N}$ tel que $d|b$ et $d|r$, donc $d|(qb + r) = a$. Donc l'ensemble des diviseurs en commun de a et b est égal à l'ensemble des diviseurs en commun de b et r. Donc par définition $\text{pgcd}(a, b) = \text{pgcd}(b, r)$. □

Le lemme donne une suggestion pour calculer le pgcd itérativement, l'algorithme d'Euclide. Nous donnons seulement un exemple.

$$\begin{aligned}
\text{pgcd}(1057, 315) &= \text{pgcd}(315, 112)\ \ (\text{parce que } 1057 = 3 \cdot 315 + 112) \\
&= \text{pgcd}(112, 91)\ \ (\text{parce que } 315 = 2 \cdot 112 + 91) \\
&= \text{pgcd}(91, 21)\ \ (\text{parce que } 112 = 1 \cdot 91 + 21) \\
&= \text{pgcd}(21, 7)\ \ (\text{parce que } 91 = 4 \cdot 21 + 7) \\
&= \text{pgcd}(7, 0)\ \ (\text{parce que } 21 = 3 \cdot 7 + 0) \\
&= 7
\end{aligned}$$

Théorème 4.1. *Soient $a, b \in \mathbb{Z}$. Alors il existe $x, y \in \mathbb{Z}$ tel que*

$$xa + yb = \text{pgcd}(a, b).$$

Preuve. Nous pouvons supposer que $a \neq 0$, parce que sinon $\text{pgcd}(a, b) = |b| = 0 \cdot a + (\pm 1)b$. Soit $S \subset \mathbb{N}$ le sous-ensemble défini par

$$S := \{n \in \mathbb{N}; \exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}:\ xa + yb = n\}$$

On a $|a| \in S$, donc S n'est pas vide. Soit s le plus petit élément de S, en particulier $s \leq |a|$ et il existe x, y tels que $xa + yb = s$. Soit $m = x'a + y'b \in S$ quelconque. Par division avec reste il existe q, r tels que $m = qs + r$ et $0 \leq r < s$, et

$$r = m - qs = (x'a + y'b) - q(xa + yb) = (x' - qx)a + (y' - qy)b.$$

Si $r > 0$, on aurait $r \in S$ et $r < s$, une contradiction avec le choix de s. Donc $r = 0$ et $s|m$. En particulier, s divise $|a|$ et $|b|$ ($|a| \in S$, et $|b| \in S$, si $b \neq 0$) et alors aussi a et b. Donc s est un diviseur commun de a et b et $s \leq \text{pgcd}(a, b)$.

Par contre, $\text{pgcd}(a, b)$ divise a et b, donc aussi $xa + yb = s$ et nécessairement $\text{pgcd}(a, b) \leq s$. Donc $s = \text{pgcd}(a, b) = xa + yb$. □

On peut aussi donner un algorithme (de Bézout) pour trouver x et y. Un exemple suffit peut-être.

Exemple 4.1. Nous calculons des x et y tels que $x \cdot 1057 + y \cdot 315 = \text{pgcd}(1057, 315)$. On commence par deux équations triviales et puis on utilise division avec reste :

$$\begin{aligned}
1 \cdot 1057 + 0 \cdot 315 &= 1057 \\
0 \cdot 1057 + 1 \cdot 315 &= 315 \\
1 \cdot 1057 + (-3) \cdot 315 &= 112 \quad (\text{parce que } 112 = 1057 - 3 \cdot 315) \\
(-2) \cdot 1057 + (7) \cdot 315 &= 91 \quad (\text{parce que } 91 = 315 - 2 \cdot 112) \\
3 \cdot 1057 + (-10) \cdot 315 &= 21 \quad (\text{parce que } 21 = 112 - 1 \cdot 91) \\
(-14) \cdot 1057 + (47) \cdot 315 &= 7 \quad (\text{parce que } 7 = 91 - 4 \cdot 21)
\end{aligned}$$

Donc $x = -14$ et $y = 47$. Les x et y ne sont pas unique, parce que on a aussi

$$(-14 + 315) \cdot 1057 + (47 - 1057) \cdot 315 = 301 \cdot 1057 - 1010 \cdot 315 = 7.$$

Exercice 4.1. Calculer $\text{pgcd}(987654321, 123456789)$. Trouver a, b tels que $-14a + 47b = \text{pgcd}(14, 47)$.

Corollaire 4.1. *Soient $a, b, d \in \mathbb{Z}$ tels que $d|a$ et $d|b$, alors $d|\text{pgcd}(a, b)$. Si $c = xa + yb$, pour certains $x, y \in \mathbb{Z}$, alors $\text{pgcd}(a, b)|c$.*

Preuve. Le nombre d divise $xa + yb$ pour chaque x, y, donc en particulier divise le $\text{pgcd}(a, b)$ (par le théorème). L'autre préposition est montrée dans la preuve du théorème. □

Un *nombre premier* est un nombre naturel $p > 1$ ayant seulement 1 et p comme diviseurs dans $\mathbb{N}$.

Corollaire 4.2. *Soit p un nombre premier. Si $p|a_1 a_2 \dots a_n$, alors il existe au moins un i tel que $p|a_i$.*

Preuve. Par induction sur n. Si $n = 1$, il n'y a rien à montrer. Supposons que si p divise un produit de moins que n facteurs, alors il divise au moins un des facteurs. Supposons que $p|a_1 a_2 \cdots a_n$ et que p ne divise pas a_n. Alors $\text{pgcd}(p, a_n) = 1$, donc il existe x, y tels que $xp + ya_n = 1$. Donc après multiplier par $(a_1 a_2 \cdots a_{n-1})$ on obtient que

$$(a_1 a_2 \cdots a_{n-1} x)p + y(a_1 a_2 \cdots a_{n-1} a_n) = a_1 a_2 \cdots a_{n-1}$$

est divisible par p, donc par l'hypothèse d'induction p divise l'un des a_i. □

5. Factorisation unique

Théorème 5.1. *Soit $1 < n$. Alors il existe un nombre naturel m et m nombres premiers $p_1, \dots, p_m$ tels que $n = p_1 p_2 \dots p_m$. Le nombre m est unique et les nombres premiers sont uniques à une permutation près des facteurs p_i.*

Preuve. Nous allons montrer l'existence d'une telle décomposition par induction sur n. Si n est premier, par exemple si $p = 2$, on prend $m = 1$ et $p_1 := n$. Sinon, ils existent $a, b \in \mathbb{N}$ tels que $n = ab$, $n > a > 1$, $n > b > 1$. Par l'hypothèse d'induction il existe s, t et décompositions $a = q_1 \cdots q_s$ et $b = r_1 \cdots r_t$, où les q_i et r_j sont premiers. Donc $n = q_1 \cdots q_s r_1 \cdots r_t$ est un produit de $s + t$ nombres premiers.

Maintenant nous montrons l'unicité par induction sur n. Si n est premier, c'est clair. Supposons que n n'est pas premier et

$$n = p_1 \cdots p_m = q_1 \cdots q_s,$$

où les p_i et q_j sont premiers et $m \geq 1, s \geq 1$. p_m divise n et est premier, donc divise un des facteurs q_i. Possiblement après renuméroter on peut supposer que ce facteur est q_s. Mais q_s est aussi premier, donc $p_m = q_s$. Soit n' tel que $n = n' p_m = n' q_s$. Alors

$$n' = p_1 \cdots p_{m-1} = q_1 \cdots q_{s-1},$$

et donc par induction $m - 1 = s - 1$ et (possiblement après renuméroter les $q_1, \dots, q_{s-1}$) on a $p_i = q_i$ pour chaque i. Alors par induction nous avons montré l'unicité. □

Exercice 5.1. Le théorème ne dit pas si le nombre de nombres premiers différents est fini ou non. Montrer qu'il existe un nombre infini de nombres premiers.

6. Relations d'équivalence

Soit X un ensemble. Une *relation* (binaire) sur X est un sous-ensemble $R \subseteq X \times X$ du produit cartésien. On utilisera la notation

$$x \sim y :\iff (x, y) \in R.$$

On dit que c'est une *relation d'équivalence* si les trois propriétés suivantes sont satisfaites :

(1) $x \sim x$ pour chaque $x \in X$ (réflexivité);
(2) $x \sim y$ implique $y \sim x$ (symétrie);
(3) $x \sim y$ et $y \sim z$ implique $x \sim z$ (transitivité).

Si $\sim$ est une relation d'équivalence sur X et $x \in X$ on écrit

$$\mathrm{Cl}(x) := \{y \in X; x \sim y\},$$

la *classe d'équivalence contenant* x. Une *classe d'équivalence* est un sous-ensemble de la forme $\mathrm{Cl}(x)$ pour un $x \in X$.

Proposition 6.1. *Soit $\sim$ une relation d'équivalence sur un ensemble X.*

(i) On a $\mathrm{Cl}(x) = \mathrm{Cl}(y)$ si et seulement si $x \sim y$.
(ii) Supposons Cl et Cl' sont deux classes d'équivalence. Si $\mathrm{Cl} \neq \mathrm{Cl}'$ alors Cl et Cl' sont disjoints.
(ii) X est la réunion disjointe de ses classes d'équivalence.

Preuve. (i) Si $\mathrm{Cl}(x) = \mathrm{Cl}(y)$, alors $x \in \mathrm{Cl}(x) = \mathrm{Cl}(y)$, donc $x \sim y$. Si $x \sim y$ et $z \in \mathrm{Cl}(x)$, alors $z \sim x$ et par la transitivité $z \sim y$, d'où $z \in \mathrm{Cl}(y)$. (ii) et (iii) suivent de (i). □

On écrit $X/\sim$ pour l'ensemble des classes d'équivalence et on a une application

$$\mathrm{Cl} : X \longrightarrow X/\sim : x \mapsto \mathrm{Cl}(x).$$

Faites attention: une classe d'équivalence C peut être vu comme un *élément* de $X/\sim$ ou comme un *sous-ensemble* de X. On a $x \sim y$ si et seulement si $\mathrm{Cl}(x) = \mathrm{Cl}(y)$.

6.1. **Les fractions.** Maintenant on va rappeler comment on définit les fractions. Soit

$$X = \{(n, d) \in \mathbb{Z}^2; d \neq 0\},$$

avec la relation d'équivalence

$$(n, d) \sim (n', d') \iff nd' = n'd \text{ (une égalité dans } \mathbb{Z}).$$

Nous vérifions la transitivité. Si $(n, d) \sim (n', d')$ et $(n', d') \sim (n'', d'')$ alors $nd' = n'd$ et $n'd'' = n''d'$. Donc

$$(nd'' - n''d)d' = nd'd'' - n''dd' = nd'd'' - n'dd'' = nd'd'' - nd'd'' = 0,$$

et parce que $d' \neq 0$ il suit que $nd'' = n''d$, d'où $(n, d) \sim (n'', d'')$.

La classe d'équivalence de (n, d) est appelé une *fraction*, et s'écrit comme d'habitude comme $\frac{n}{d}$:

$$\frac{n}{d} := \mathrm{Cl}(n, d).$$

On a $\frac{n}{d} = \frac{n'}{d'}$ si et seulement si $\mathrm{Cl}(n, d) = \mathrm{Cl}(n', d')$ si et seulement si $nd' = n'd$. Maintenant

$$\mathbb{Q} := X/\sim = \{\frac{n}{d}; d \neq 0\}$$

est l'ensemble des fractions.

On définit l'addition et la multiplication sur $\mathbb{Q}$ par

$$\frac{n}{d} \cdot \frac{n'}{d'} := \frac{nn'}{dd'}; \ \frac{n}{d} + \frac{n'}{md'} := \frac{nd' + n'd}{dd'}.$$

Il y a quelque chose à faire encore ! Les formules sont données en termes de représentants de classes d'équivalence; changer les représentants ne change pas les classes, mais change les formules. Vérifions par exemple que l'addition est *bien-définie*. Supposons $\frac{n}{d} = \frac{r}{s}$ et $\frac{n'}{d'} = \frac{r'}{s'}$. Il faut vérifier si

$$\frac{nd' + n'd}{dd'} = \frac{rs' + r's}{ss'},$$

c'est à dire si

$$(nd' + n'd)ss' = (rs' + r's)dd'.$$

On a $ns = rd$ et $n's' = r'd'$ et donc on a en effet

$$(nd' + n'd)ss' = ns \cdot d's' + n's' \cdot ds = rd \cdot d's' + r'd' \cdot ds = (rs' + r's)dd'.$$

On considère $\mathbb{Z}$ comme un sous-ensemble par l'inclusion $\mathbb{Z} \longrightarrow \mathbb{Q}; n \mapsto \frac{n}{1}$. Il y a une extension de l'ordre partiel : soit $\frac{n}{d}$ et $\frac{n'}{d'}$ deux fractions où on peut supposer que $d, d' \in \mathbb{N}$. On écrit

$$\frac{n}{d} \leq \frac{n'}{d'} \iff nd' \leq n'd$$

et $|\frac{n}{d}| := \frac{|n|}{|d|}$.

6.2. **Modulo n.** Pour chaque entier n on a une relation d'équivalence $\equiv (\mathrm{mod}\ n)$ sur $\mathbb{Z}$. On écrit $a \equiv a'(\mathrm{mod}\ n)$ et on dit que a est *congruent à a' modulo n* si $n|(a-a')$, ou si a et a' ont le même reste après division par n :

$$a \equiv a'(\mathrm{mod}\ n) \iff n|(a-a').$$

Pour n fixé, ça donne une relation d'équivalence sur $\mathbb{Z}$, parce que

(1) $a \equiv a(\mathrm{mod}\ n)$ (on a $n|(a-a)$);

(2) $a \equiv a'(\mathrm{mod}\ n) \iff a' \equiv a(\mathrm{mod}\ n)$ (on a $n|(a-a') \iff n|(a'-a)$);

(3) $a \equiv a'(\mathrm{mod}\ n)$ et $a' \equiv a''(\mathrm{mod}\ n) \Rightarrow a \equiv a''(\mathrm{mod}\ n)$, (on a $n|(a-a')$ et $n|(a'-a'') \Rightarrow n|(a-a'')$.)

Écrivons $\overline{a} = \mathrm{Cl}(a)$ pour la classe d'équivalence de a pour l'équivalence $\equiv (\mathrm{mod}\ n)$, donc

$$\overline{a} := \{m \in \mathbb{Z};\ m \equiv a(\mathrm{mod}\ n)\} = \{a + mn;\ m \in \mathbb{Z}\}.$$

Donc $\overline{a} = \overline{a'}$ si et seulement si $a \equiv a'(\mathrm{mod}\ b)$.

On écrit $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv (\mathrm{mod}\ n)$ pour l'ensemble des classes d'équivalence pour $\equiv (\mathrm{mod}\ n)$.

Addition et multiplication respectent la relation d'équivalence modulo n

$$\overline{a} + \overline{a'} := \overline{a+a'}; \overline{a} \cdot \overline{a'} := \overline{aa'}.$$

Exercice 6.1. (i) Montrer que $+$ et $\cdot$ sont bien définies et que les règles de commutativité, transitivité et distributivité sont satisfaites.

(ii) Montrer que si $n \neq 0$, alors $\mathbb{Z}/n\mathbb{Z}$ est d'ordre fini $|n|$.

Preuve. Par exemple la règle de distributivité

$$\begin{aligned}
\overline{a_1} \cdot (\overline{a_2} + \overline{a_3}) &= \overline{a_1} \cdot \overline{(a_2 + a_3)} \ \text{(par la définition de } +) \\
&= \overline{a_1 \cdot (a_2 + a_3)} \ \text{(par la définition de } \cdot) \\
&= \overline{a_1 a_2 + a_1 a_3} \ \text{(par la distributivité dans } \mathbb{Z}) \\
&= \overline{a_1 a_2} + \overline{a_1 a_3} \ \text{(par la définition de } +) \\
&= \overline{a_1} \cdot \overline{a_2} + \overline{a_1} \cdot \overline{a_3} \ \text{(par la définition de } \cdot)
\end{aligned}$$

□

Par exemple, si $n = 2$, alors $\mathbb{Z}/2\mathbb{Z}$ a deux éléments $\overline{0}$="Pair" et $\overline{1}$="Impair'. On a

$$\overline{0} + \overline{0} = \overline{0},\ \overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{1},\ \overline{1} + \overline{1} = \overline{2} = \overline{0},\ \overline{0} \cdot \overline{0} = \overline{0},\ \overline{0} \cdot \overline{1} = \overline{1} \cdot \overline{0} = \overline{0},\ \overline{1} \cdot \overline{1} = \overline{1}.$$

Proposition 6.2. *a et n sont relativement premier si et seulement si il existe un $x \in \mathbb{Z}$ tel que $\overline{a} \cdot \overline{x} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

Preuve. Si $\mathrm{pgcd}(a,n) = 1$ alors il existe x et y tels que $xa + yn = 1$. On a $\overline{n} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$, donc $\overline{xa} + \overline{yn} = \overline{xa} = \overline{1}$. Par contre, si $\overline{ax} = \overline{1}$, alors $\overline{ax - 1} = \overline{0}$, donc $ax - 1$ est divisible par n, disons $ax - 1 = -yn$. Alors $ax + yn = 1$, et donc a et n sont relativement premier. □

6.3. **Nombres réels.** (Les deux sous-sections finales ne seront pas utilisées dans le cours Algèbre 1.) On donnera une définition d'un nombre réel (est-ce qu'on a déj donné dans un de vos cours une définition d'un nombre réel, pas basée sur l'intuition géométrique ?) Une suite $(a_i)_{i\in\mathbb{N}}$ où $a_i \in \mathbb{Q}$ est appelé une suite de Cauchy, si pour chaque $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, il existe un $N \in \mathbb{N}$ tel que $|a_i - a_j| \leq \epsilon$ pour chaque $i, j \geq N$. Chaque fraction $a \in \mathbb{Q}$ définit une suite de Cauchy $(a_i)_{i\in\mathbb{N}}$, si on pose $a_i = a$ pour chaque $i \in \mathbb{N}$. Soit X la collection de toutes les suites de Cauchy. On définit une relation d'équivalence sur X, comme $(a_i)_{i\in\mathbb{N}} \sim (a'_i)_{i\in\mathbb{N}}$ si et seulement si pour chaque $\epsilon \in \mathbb{Q}, \epsilon > 0$ il existe un $N \in \mathbb{N}$ tel que pour chaque $i \geq N$ on a $|a_i - a'_i| \leq \epsilon$.

Les classes d'équivalence $X/\sim$ sont appelées "nombres réels" et $\mathbb{R} := X/\sim$. Comment définir la somme et le produit de deux "nombres réels"?

Une autre dfinition courante de nombre réel (pas basée sur l'intuition) est basée sur les coupures de Dedekind.

6.4. **Nombres p-adiques.** Presque la même définition définit un autre genre de nombre, nommé *p-adique*, étrange mais quand-même très utile. Pour chaque nombre premier p, il existe une autre valeur absolue $|x|_p$ sur $\mathbb{Q}$ que celui d'habitude. Soit $\frac{n}{d}$ une fraction. Écrit $n = p^i n'$, où $p \not| n'$, et $d = p^j d'$ où $p \not| d'$. On définit alors

$$|\frac{n}{d}|_p := p^{j-i} \text{ (dans } \mathbb{Q}).$$

Donc un entier est petit pour cette valeur absolue si et seulement si cet entier est divisible par une haute puissance de p.

Une suite $(a_i)_{i\in\mathbb{N}}$ où $a_i \in \mathbb{Q}$ est appelé une suite p-adique de Cauchy, si pour chaque $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, il existe un $N \in \mathbb{N}$ tel que $|a_i - a_j|_p \leq \epsilon$ pour chaque $i, j \geq N$. Chaque fraction $a \in \mathbb{Q}$ définit une suite de Cauchy $(a_i)_{i\in\mathbb{N}}$, si on pose $a_i = a$ pour chaque $i \in \mathbb{N}$. Soit X_p la collection de toutes les suites p-adique de Cauchy. On définit une relation d'équivalence sur X_p, comme $(a_i)_{i\in\mathbb{N}} \sim (a'_i)_{i\in\mathbb{N}}$ si et seulement si pour chaque $\epsilon \in \mathbb{Q}, \epsilon > 0$ il existe un $N \in \mathbb{N}$ tel que pour chaque $i \geq N$ on a $|a_i - a'_i|_p \leq \epsilon$.

Les classes d'équivalence $X_p/\sim$ sont appelées *nombres p-adique* et $\mathbb{Q}_p := X_p/\sim$. Comment définir la somme et le produit de deux nombres p-adique ?

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA