Une preuve topologique de l'infinité des nombres premiers

Christian V. Nguembou Tagne

13 juin 2021

Dans cette note, nous introduisons une topologie sur l'ensemble $\mathbb{Z}$ des entiers relatifs. En outre, après avoir révélé quelques propriétés de cette topologie, nous mettons cette dernière à contribution pour montrer que l'ensemble des nombres premiers est infini. Cette topologie et cette preuve sont dues au mathématicien israélien Hillel Furstenberg.

Avant d'entrer dans le vif du sujet, nous rappelons en prélude le *théorème des restes chinois* et la notion de *base de topologie*.

Prélude

Le théorème des restes chinois

Nous présentons ici la forme primaire du *théorème des restes chinois* pour un système de deux congruences.

Proposition 1.

Soient (a_1, b_1) et (a_2, b_2) des éléments du produit $\mathbb{N}^* \times \mathbb{N}$, puis $d = \text{pgcd}(a_1, a_2)$ et $m = \text{ppmc}(a_1, a_2)$. Pour qu'il existe un entier relatif z satisfaisant les congruences

$$\begin{cases} z \equiv b_1 \,(\text{mod}\, a_1), \\ z \equiv b_2 \,(\text{mod}\, a_2), \end{cases} \tag{‡}$$

il faut et il suffit que $b_1 \equiv b_2 \,(\text{mod}\, d)$. Si cette condition est vérifiée, alors il existe un unique $c \in [0, m-1] \cap \mathbb{N}$ tel que, pour chaque $z \in \mathbb{Z}$, les congruences (‡) sont satisfaites si, et seulement si, $z \equiv c \,(\text{mod}\, m)$.

Démonstration :

Supposons qu'il existe un entier relatif z satisfaisant les congruences (‡). Alors, il existe un couple $(x, y) \in \mathbb{Z}^2$ tel que $z = a_1x + b_1$ et $z = a_2y + b_2$. Ceci entraîne

$$a_1x - a_2y = b_2 - b_1. \qquad (\diamond)$$

De ce fait, $b_2 - b_1$ est un multiple de d, le plus grand commun diviseur de a_1 et de a_2. D'où

$$b_2 - b_1 \equiv 0 \,(\mathrm{mod}\, d).$$

À présent, nous supposons que cette dernière congruence est satisfaite. Alors, l'équation diophantienne ($\diamond$), d'inconnues x et y, admet des solutions dans $\mathbb{Z}^2$. Ainsi, il existe un couple $(x, y) \in \mathbb{Z}^2$ tel que $a_1x + b_1 = a_2y + b_2$. Ce dernier nombre, entier relatif, désigné ici par z, vérifie bien $z \equiv b_1 \,(\mathrm{mod}\, a_1)$ et $z \equiv b_2 \,(\mathrm{mod}\, a_2)$.

Pour la suite, soit $b_1 \equiv b_2 \,(\mathrm{mod}\, d)$. Alors, il existe un couple $(x_0, y_0) \in \mathbb{Z}^2$ tel que

$$a_1x_0 - a_2y_0 = b_2 - b_1,$$

c'est-à-dire $a_1x_0 + b_1 = a_2y_0 + b_2$. Du reste, pour qu'un couple (x, y) de $\mathbb{Z}^2$ soit solution de l'équation ($\diamond$), il faut et il suffit qu'il existe un $k \in \mathbb{Z}$ tel que

$$(x, y) = \left(x_0 - \frac{a_2}{d}k, y_0 - \frac{a_1}{d}\right).$$

De ce fait, si $z = a_1x + b_1 = a_2y + b_2$, alors

$$z = a_1\left(x_0 - \frac{a_2}{d}k\right) + b_1 = a_1x_0 + b_1 - \frac{a_1a_2}{d}k$$

et

$$z = a_2\left(y_0 - \frac{a_1}{d}\right) + b_2 = a_2y_0 + b_2 - \frac{a_1a_2}{d}k.$$

Cependant, $a_1a_2 = dm$. Il en résulte que

$$z = a_1x_0 + b_1 - mk = a_2y_0 + b_2 - mk,$$

puis

$$z \equiv a_1x_0 + b_1 \,(\mathrm{mod}\, m) \qquad \text{et} \qquad z \equiv a_2y_0 + b_2 \,(\mathrm{mod}\, m).$$

Maintenant, soit c le reste de la division euclidienne de $a_1x_0 + b_1 = a_2y_0 + b_2$ par m. Alors, les égalités $z = a_1x + b_1 = a_2y + b_2$ induisent $z \equiv c \,(\mathrm{mod}\, m)$.

En outre, il existe des entiers relatifs q_1 et q_2 tels que

$$a_1x_0 + b_1 = mq_1 + c \qquad \text{et} \qquad a_2y_0 + b_2 = mq_2 + c.$$

Par suite, s'il existe un entier relatif k tel que $z = c + mk$, alors

$$z = a_1x_0 + b_1 - mq_1 + mk \equiv b_1 \,(\mathrm{mod}\, a_1)$$

et

$$z = a_2y_0 + b_2 - mq_2 + mk \equiv b_2 \,(\mathrm{mod}\, a_2),$$

car $m \equiv 0 \,(\mathrm{mod}\, a_1)$ et $m \equiv 0 \,(\mathrm{mod}\, a_2)$.

Par conséquent, les congruences (‡) sont équivalentes à $z \equiv c \,(\mathrm{mod}\, m)$. □

Base de topologie

Soit X un ensemble. Une partie $\mathfrak{B}$ de $\mathscr{P}(X)$ est **base d'une topologie** sur X si les deux conditions suivantes sont satisfaites :

(i) $X = \bigcup \mathfrak{B}$.

(ii) Pour tout couple (A, B) d'éléments de $\mathfrak{B}$, si x est un élément de $A \cap B$, alors il existe un $C \in \mathfrak{B}$ tel que $x \in C \subset A \cap B$.

Soit X un ensemble. La **réunion** d'une partie $\mathfrak{A}$ de $\mathscr{P}(X)$ est l'ensemble $\bigcup \mathfrak{A}$ défini par :

$$x \in \bigcup \mathfrak{A} \Leftrightarrow (\exists A \in \mathfrak{A})\ x \in A.$$

En particulier, $\bigcup \emptyset = \emptyset$.

Chaque base permet de définir une topologie. La proposition 2 ci-dessous précise les modalités de cette définition.

Proposition 2.

Soit X un ensemble et $\mathfrak{B}$ une partie de $\mathscr{P}(X)$. Alors, les conditions suivantes sont équivalentes :

(a) $\mathfrak{B}$ est base d'une topologie sur X.

(b) L'ensemble $\langle \mathfrak{B} \rangle$, constituée des parties U de X telles que, pour tout $u \in U$, il existe un $B \in \mathfrak{B}$ vérifiant $u \in B \subset U$, est une topologie sur X.

(c) L'ensemble des réunions des parties de $\mathfrak{B}$ est une topologie sur X.

Démonstration :

(**a**) $\Rightarrow$ (**b**) : Soit $\mathfrak{B}$ une base d'une topologie sur X, puis l'ensemble

$$\langle \mathfrak{B} \rangle = \Big\{ U \in \mathscr{P}(X) \mid (\forall x \in U)(\exists B \in \mathfrak{B})\ x \in B \subset U \Big\}.$$

Alors, manifestement, $\emptyset \in \langle \mathfrak{B} \rangle$. En outre, l'égalité $X = \bigcup \mathfrak{B}$ entraîne $X \in \langle \mathfrak{B} \rangle$. De plus, si U et V sont des éléments de $\langle \mathfrak{B} \rangle$, alors pour tout $x \in U \cap V$, il existe des éléments A et B de $\mathfrak{B}$ tels que $x \in A \subset U$ et $x \in B \subset V$; d'où $x \in A \cap B \subset U \cap V$. Cependant, d'après la définition des bases, il existe un $C \in \mathfrak{B}$ tel que $x \in C \subset A \cap B$; ceci induit $x \in C \subset U \cap V$. Ainsi, $U \cap V \in \langle \mathfrak{B} \rangle$ pour tout couple (U, V) d'éléments de $\langle \mathfrak{B} \rangle$. Au demeurant, pour toute partie $\mathfrak{A}$ de $\langle \mathfrak{B} \rangle$, si $x \in \bigcup \mathfrak{A}$, alors il existe un $U \in \langle \mathfrak{B} \rangle$ tel que $x \in U$. De ce fait, en vertu de la définition de l'ensemble $\langle \mathfrak{B} \rangle$, il existe un $B \in \mathfrak{B}$ tel que $x \in B \subset U \subset \bigcup \mathfrak{A}$. Par conséquent, $\bigcup \mathfrak{A} \in \langle \mathfrak{B} \rangle$ pour toute partie $\mathfrak{A}$ de l'ensemble $\langle \mathfrak{B} \rangle$. Ce dernier est donc une topologie sur X.

(**b**) $\Rightarrow$ (**c**) : Nous supposons que l'ensemble $\langle \mathfrak{B} \rangle$ est une topologie sur X, et désignons par $\mathfrak{O}$ l'ensemble des réunions des parties de $\mathfrak{B}$. Nous allons montrer que $\langle \mathfrak{B} \rangle = \mathfrak{O}$. À cet

effet, soit $U \in \langle \mathfrak{B} \rangle$. Alors, pour tout $x \in U$, il existe un $B_x \in \mathfrak{B}$ tel que $x \in B_x \subset U$. D'où

$$U \subset \bigcup \Big\{ B_x \mid x \in U \Big\} \subset U,$$

et donc U est la réunion d'une partie de $\mathfrak{B}$. Par conséquent, $\langle \mathfrak{B} \rangle \subset \mathfrak{O}$. Par ailleurs, pour toute partie $\mathfrak{A}$ de $\mathfrak{B}$, si $x \in \bigcup \mathfrak{A}$, alors il existe un $B \in \mathfrak{A}$ tel que $x \in B$. Cependant, $B \subset \bigcup \mathfrak{A}$. Donc, $x \in B \subset \bigcup \mathfrak{A}$. Puisque $B \in \mathfrak{B}$, il en résulte que $\bigcup \mathfrak{A} \in \langle \mathfrak{B} \rangle$. Par conséquent, la réunion de toute partie de $\mathfrak{B}$ appartient à $\langle \mathfrak{B} \rangle$. Ceci signifie que $\mathfrak{O} \subset \langle \mathfrak{B} \rangle$. Tout compte fait, $\langle \mathfrak{B} \rangle = \mathfrak{O}$.

(**c**) $\Rightarrow$ (**a**) : Supposons que l'ensemble $\mathfrak{O}$ des réunions des parties de $\mathfrak{B}$ est une topologie sur X. Alors, il existe une partie $\mathfrak{A}$ de $\mathfrak{B}$ telle que $X = \bigcup \mathfrak{A}$. Cependant, $\bigcup \mathfrak{A} \subset \bigcup \mathfrak{B}$. D'où $X \subset \bigcup \mathfrak{B}$. Puisque par définition $\bigcup \mathfrak{B} \subset X$, il en résulte que

$$X = \bigcup \mathfrak{B}.$$

À présent, soit (A, B) un couple d'éléments de $\mathfrak{B}$. Alors, $A \cap B \in \mathfrak{O}$, car $\mathfrak{B} \subset \mathfrak{O}$. Il existe donc une partie $\mathfrak{A}$ de $\mathfrak{B}$ telle que $A \cap B = \bigcup \mathfrak{A}$. Par suite, si $x \in A \cap B$, alors il existe un $C \in \mathfrak{A}$ vérifiant $x \in C$. Or, $C \subset \bigcup \mathfrak{A}$. D'où $x \in C \subset A \cap B$. Donc, pour tout couple (A, B) d'éléments de $\mathfrak{B}$, si $x \in A \cap B$, alors il existe un $C \in \mathfrak{B}$ tel que $x \in C \subset A \cap B$. Par conséquent, $\mathfrak{B}$ est base d'une topologie sur X. □

✍

Pour toute base $\mathfrak{B}$ sur un ensemble X, la topologie

$$\langle \mathfrak{B} \rangle = \Big\{ U \in \mathscr{P}(X) \mid (\forall x \in U)(\exists B \in \mathfrak{B})\ x \in B \subset U \Big\}$$

sur X est appelée **topologie engendrée** par $\mathfrak{B}$. Les éléments de cette topologie sont les réunions des parties de $\mathfrak{B}$.

1. Définition de la topologie

La famille constituée des ensembles

$$S(a, b) = \Big\{ an + b \mid n \in \mathbb{Z} \Big\} = a\mathbb{Z} + b,$$

où $a \in \mathbb{N}^*$ et $b \in \mathbb{N}$, définit un ensemble

$$\mathfrak{B} = \Big\{ S(a, b) \mid (a, b) \in \mathbb{N}^* \times \mathbb{N} \Big\},$$

partie de $\mathscr{P}(\mathbb{Z})$. Par ailleurs, $S(1, 0) = \mathbb{Z}$. De ce fait, $\mathbb{Z} = \bigcup\limits_{(a,b) \in \mathbb{N}^* \times \mathbb{N}} S(a, b) = \bigcup \mathfrak{B}$. Au demeurant, d'après le *théorème des restes chinois* (voir la proposition 1 à la page 1), pour des éléments quelconques (a_1, b_1) et (a_2, b_2) de $\mathbb{N}^* \times \mathbb{N}$, nous avons

$$S(a_1, b_1) \cap S(a_2, b_2) = \begin{cases} \emptyset & \text{si } \ b_1 \not\equiv b_2 \,(\mathrm{mod}\, d), \\ S(m, c) & \text{si } \ b_1 \equiv b_2 \,(\mathrm{mod}\, d), \end{cases}$$

où $d = \text{pgcd}(a_1, a_2)$ et $m = \text{ppmc}(a_1, a_2)$, puis $c \in [0, m-1] \cap \mathbb{N}$. Il en résulte que $\mathfrak{B}$ est base d'une topologie sur $\mathbb{Z}$.

Soit $\mathfrak{O} = \langle \mathfrak{B} \rangle$ la topologie engendrée par cette base.

2. Le complémentaire d'une partie finie non vide n'est pas fermé

Soit F une partie finie non vide de $\mathbb{Z}$. Nous supposons que F est un ouvert de la topologie sur $\mathbb{Z}$ engendrée par $\mathfrak{B}$. Alors, il existe un couple $(a, b) \in \mathbb{N}^* \times \mathbb{N}$ tel que $S(a, b) \subset F$. Ainsi, $S(a, b)$ est une partie finie de $\mathbb{Z}$. Cependant, une application bijective φ est définie de $\mathbb{Z}$ sur $S(a, b)$ par $\varphi(z) = az + b$. Ceci entraîne que $\mathbb{Z}$ est un ensemble fini : une contradiction. La supposition est donc fausse. Autrement dit, F n'est pas un ouvert, et par suite $\mathbb{Z} \setminus F$ n'est pas un fermé.

3. Tout élément de la base est simultanément ouvert et fermé

Soit $(a, b) \in \mathbb{N}^* \times \mathbb{N}$. Alors, $S(a, b)$ est un ouvert, par définition de la topologie. Maintenant, soit r le reste de la division euclidienne de b par a. Alors, $S(a, b) = S(a, r)$. D'où

$$\mathbb{Z} \setminus S(a, b) = \bigcup_{k \in K} S(a, k) = \bigcup \Big\{ S(a, k) \mid k \in K \Big\},$$

où $K = \big([0, a-1] \cap \mathbb{N}\big) \setminus \{r\}$. Ainsi, $\mathbb{Z} \setminus S(a, b)$ est un ouvert, et donc $S(a, b)$ est un fermé.

4. Réunion d'une partie de la base

Soit $\mathbb{P}$ l'ensemble des nombres premiers.

Nous considérons un entier relatif z distinct de -1 et de 1. Alors, $z = 0$ ou $|z| \geq 2$. D'après le *théorème fondamental de l'arithmétique*, il en résulte que z possède au moins un diviseur premier. De ce fait, il existe un $p \in \mathbb{P}$ tel que $z \in p\mathbb{Z} = S(p, 0)$. Ceci entraîne

$$\mathbb{Z} \setminus \{-1, 1\} \subset \bigcup_{p \in \mathbb{P}} S(p, 0).$$

Du reste, $S(p, 0) = p\mathbb{Z} \subset \mathbb{Z} \setminus \{-1, 1\}$ pour chaque $p \in \mathbb{P}$, car tout nombre premier est supérieur ou égale à 2. Par conséquent,

$$\bigcup_{p \in \mathbb{P}} S(p, 0) = \mathbb{Z} \setminus \{-1, 1\}. \qquad (\star)$$

5. Sur l'infinité de l'ensemble des nombres premiers

Nous supposons que l'ensemble $\mathbb{P}$ des nombres premiers est fini. Au regard de l'égalité $(\star)$ ci-dessus, il en résulte que $\mathbb{Z} \setminus \{-1, 1\}$ est fermé, en tant que réunion finie de fermés. Ceci contredit la conclusion de la section 2. La supposition est par conséquent fausse. En d'autres termes, l'ensemble des nombres premiers est infini.