Réf : Landman, Robertson
Ramsey theory on the integers

Dev

Le grand théorème de Fermat est faux sur $\mathbb{Z}/p\mathbb{Z}$!

Pré-requis : $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

Énoncé : Soit $n \in \mathbb{N}^*$. Il existe un nombre premier q tel que pour tout nombre premier $p \geq q$, l'équation $x^n + y^n = z^n \pmod p$ admet une solution non triviale, c-à-d telle que $xyz \neq 0 \pmod p$.

Dl

Lemme 1 : Soit E un ensemble fini de cardinal m et $n \in \mathbb{N}^*$. Il existe un entier $N(n) \in \mathbb{N}^*$ tel que si $m \geq N(n)$, alors pour toute fonction $\chi : \mathcal{P}_2(E) \longrightarrow \{c_1, \dots, c_n\}$,

« coloriage » ↵ ↳ Parties à 2 éléments de E. ↳ Ensemble de « couleurs »

on peut trouver $x, y, z \in E$ distincts tels que $\chi\{x,y\} = \chi\{y,z\} = \chi\{z,x\}$.

- Par récurrence sur n. Clairement, $N(1) = 3$ convient.
- Supposons que $N(n-1)$ existe. Soit $\chi : \mathcal{P}_2(E) \longrightarrow \{c_1, \dots, c_n\} =: \mathcal{C}$

  Fixons $x \in E$. On considère $\chi_x : E \setminus \{x\} \longrightarrow \mathcal{C}$, $y \longmapsto \chi\{x,y\}$. On a $E \setminus \{x\} = \bigsqcup_{i=1}^{n} \chi_x^{-1}\{c_i\}$.

  Par le principe des tiroirs, il existe $i_0 \in [\![1, n]\!]$ tel que $|\chi_x^{-1}\{c_{i_0}\}| \geqslant \left\lceil \frac{n-1}{n} \right\rceil$.

  Si il existe $y, z \in \chi_x^{-1}\{c_{i_0}\}$ distincts tels que $\chi\{y,z\} = c_{i_0}$, alors x, y, z conviennent.

  Sinon, la restriction de χ à $\mathcal{P}_2(X)$ est à valeurs dans $\mathcal{C} \setminus \{c_{i_0}\}$, de cardinal $n-1$.

  Supposons que $m \geq n N(n-1) + 1$, de sorte que $\left\lceil \frac{m-1}{n} \right\rceil \geqslant N(n-1)$. Alors $|X| \geqslant N(n-1)$.

  Par définition de $N(n-1)$, on peut trouver $y, z, t \in X$ distincts tels que

  $\chi\{y,z\} = \chi\{z,t\} = \chi\{x,t\}$: c'est fini.

  Ainsi, prendre $N(n) := n N(n-1) + 1$ convient. □ (Lemme 1)

Lemme 2 : (Théorème de Schur) Soit $n \in \mathbb{N}^*$. Il existe un entier $s(n) \in \mathbb{N}^*$ tel que pour tout $m \geqslant s(n)$, pour toute fonction $\nabla : [\![1, m]\!] \longrightarrow \{c_1, \dots, c_n\}$, on peut trouver $x, y, z \in [\![1, m]\!]$ tels que $x + y = z$ et $\nabla(x) = \nabla(y) = \nabla(z)$.

• On montre que $s(n) := N(n)-1$ convient. Soit $\nabla : [\![1; N(n)-1]\!] \longrightarrow \{c_1, \dots, c_n\}$.

On définit $E = [\![1; N(n)]\!]$ et $\chi : \mathcal{P}_2(E) \longrightarrow \{c_1, \dots, c_n\}$.

$$\{x, y\} \longmapsto \nabla(|y-x|)$$

Par le lemme 1, on peut trouver $x, y, z \in E$ tels que $\chi\{y,x\} = \chi\{z,y\} = \chi\{x,z\}$.

Supposons $x < y < z$ et posons $X := y-x$, $Y := z-y$, $Z := z-x$. $X, Y, Z \in [\![1; N(n)-1]\!]$.

Ils satisfont $X+Y = Z$ et $\nabla(X) = \nabla(Y) = \nabla(Z)$ par construction.

□ lemme 2

• Soit $n \in \mathbb{N}^*$ et p un nombre premier tel que $p > s(n)$.

Posons $A_n := \{a^n \mid a \in (\mathbb{Z}/p\mathbb{Z})^*\} \subset (\mathbb{Z}/p\mathbb{Z})^*$. C'est un sous-groupe.

On partitionne $(\mathbb{Z}/p\mathbb{Z})^*$ par les classes à gauche de A_n :

$$(\mathbb{Z}/p\mathbb{Z})^* = \bigsqcup_{i=1}^{\kappa} a_i A_n \quad \text{où } a_i \in (\mathbb{Z}/p\mathbb{Z})^* \text{ et } \kappa := \left| \frac{(\mathbb{Z}/p\mathbb{Z})^*}{A_n} \right|.$$

Comme $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique, il est facile de calculer $|A_n| = \frac{p-1}{\mathrm{PGCD}(p-1, n)}$.

(Considérer $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$, $x \longmapsto x^n$. Montrer que $|\mathrm{Ker}(\varphi)| = \mathrm{PGCD}(p-1, n)$).

Ainsi : $\kappa = \mathrm{PGCD}(p-1, n) \leqslant n$.

On définit $\nabla : [\![1; p-1]\!] \longrightarrow \{c_1, \dots, c_\kappa\}$, $x \longmapsto c_i$ ssi $\bar{x} \in a_i A_n$. Comme $\kappa \leqslant n$ et $p-1 \geqslant s(n)$, on peut trouver $x, y, z \in [\![1; p-1]\!]$ tels que $x+y=z$ et $\bar{x}, \bar{y}, \bar{z} \in a_i A_n$. Il existe donc $\alpha, \beta, \gamma \in (\mathbb{Z}/p\mathbb{Z})^*$ tels que $\bar{x} = a_i \alpha^n$, $\bar{y} = a_i \beta^n$ et $\bar{z} = a_i \gamma^n$. On a $a_i \alpha^n + a_i \beta^n = a_i \gamma^n$ dans $\mathbb{Z}/p\mathbb{Z}$.

D'où : $\boxed{\alpha^n + \beta^n = \gamma^n \text{ et } \alpha\beta\gamma \neq 0 \text{ dans } \mathbb{Z}/p\mathbb{Z}.}$

▨

Leçons : 120, 190

(?) 127, 123, 126.