Théorème de Fermat modulaire

Leçons : 120 ; 121 ; 126 ; 190

Références : LANDMAN–ROBERTSON, *Ramsey Theory on the Integers*(p.222) [?]

Prérequis :

- le lemme des tiroirs
- l'ordre de $A = \{a^r, a \in (\mathbb{Z}/p\mathbb{Z})^\times\}$

Introduction :

L'équation de Fermat-Wiles $x^n + y^n = z^n$ n'admet pas de solution non triviale pour $n \geqslant 3$ dans $\mathbb{Z}$. Cependant si on ne se place plus sur $\mathbb{Z}$ mais sur $\mathbb{Z}/p\mathbb{Z}$ pour un p bien choisi, l'équation admet au moins une solution non triviale. C'est ce résultat là que l'on va prouver maintenant en utilisant des lemmes de dénombrement.

Théorème 1. Soit $r \in \mathbb{N}^*$, il existe un entier q tel que pour tout entier premier $p > q$, l'équation $x^r + y^r = z^r$ admet une solution dans $\mathbb{Z}/p\mathbb{Z}$ avec x, y, z tous non nuls.

Lemme 1. Soient $r \in \mathbb{N}^*$ et $a_1, \dots, a_r \in \mathbb{C}^r$ deux à deux distincts, il existe un entier $N(r)$ tel que pour tout ensemble fini E de cardinal $n \geqslant N(r)$ et pour toute application $\chi : \mathcal{P}_2(E) \to \{a_1, \dots, a_r\}$, il existe trois éléments distincts $x, y, z \in E$ tels que $\chi(\{x, y\}) = \chi(\{x, z\}) = \chi(\{y, z\})$, où $\mathcal{P}_2(E)$ est l'ensemble des sous ensembles de cardinal 2 de E.

Remarques :

L'ensemble $\{a_1, \dots, a_r\}$ peut être vu comme un ensemble de couleurs, ce qui fait de χ un coloriage par r couleurs des sous ensembles de cardinal 2 de E.

Démonstration du Lemme 1. On va procéder par récurrence sur r.
Initialisation : Pour $r = 1$, toute application χ sera constante égale à la couleur a_1. Donc dès que l'ensemble E sera de cardinal supérieur à 3, on pourra trouver trois éléments distincts qui ont la même couleur. Ainsi on peut prendre $N(r) = 3$.

Hérédité : On suppose que l'on a le résultat au rang $r-1$, on veut le prouver au rang r.

Soit un ensemble E de cardinal n et soit une application $\chi : \mathcal{P}_2(E) \to \{a_1, \dots, a_r\}$. On pose l'application

$$\chi_x : \begin{cases} E\backslash\{x\} & \to & \{a_1, \dots, a_r\} \\ y & \mapsto & \chi(\{x, y\}) \end{cases}.$$

On a $E\backslash\{x\} = \bigsqcup_{i=1}^{r} \chi_x^{-1}(\{a_i\})$, or $E\backslash\{x\}$ est de cardinal $n-1$, donc il existe un $i_0 \in [\![1; r]\!]$ tel que

$$|\chi_x^{-1}(\{a_{i_0}\})| \geqslant \lceil \frac{n-1}{r} \rceil,$$

par le lemme des tiroirs. On pose

$$X := \chi_x^{-1}(\{a_{i_0}\}).$$

S'il existe $y, z \in X$ distincts tels que $\chi(\{y,z\}) = a_{i_0}$, on aura x, y, z distincts tels que $\chi(\{x,y\}) = \chi(\{x,z\}) = \chi(\{y,z\}) = a_{i_0}$.

Sinon on prend l'application

$$\tilde{\chi} : \begin{cases} \mathcal{P}_2(X) & \to & \{a_1, \dots, a_{i_0-1}, a_{i_0+1}, \dots, a_r\} \\ \{y,z\} & \mapsto & \chi(\{y,z\}) \end{cases},$$

on veut appliquer l'hypothèse de récurrence sur $\tilde{\chi}$ car il y a $r-1$ couleurs. Il faut que $|X| \geqslant N(r-1)$ pour pouvoir appliquer l'hypothèse.
Prenons $N(r) = rN(r-1)+1$ ainsi

$$|X| \geqslant \lceil \frac{n-1}{r} \rceil \geqslant \lceil \frac{N(r)-1}{r} \rceil \geqslant N(r-1)$$

donc on peut appliquer l'hypothèse de récurrence ainsi il existe $t, y, z \in X$ distincts tels que

$$\chi(\{t,y\}) = \chi(\{y,z\}) = \chi(\{t,z\})$$

puisque $\tilde{\chi} = \chi_{|\mathcal{P}_2(X)}$. Donc comme $X \subset E$, on a le résultat pour $N(r) = rN(r-1)+1$. □

Lemme 2 (de Schur)**.** Soient $r \in \mathbb{N}^*$ et $a_1, \dots, a_r \in \mathbb{C}^r$ deux à deux distincts, il existe un entier $s(r)$ tel que pour tout $n \geqslant s(r)$ et pour toute application $\sigma : [\![1;n]\!] \to \{a_1, \dots, a_r\}$, il existe trois éléments x, y, z de $[\![1;n]\!]$ tels que $x+y=z$ et $\sigma(x) = \sigma(y) = \sigma(z)$.

Démonstration du lemme 2. Soit $r \in \mathbb{N}^*$ et $n \in \mathbb{N}$, soit une application $\sigma : [\![1;n]\!] \to \{a_1, \dots, a_r\}$, On veut se ramener au cas du lemme 1. On prend $E = [\![1; n+1]\!]$ et on pose l'application

$$\chi : \begin{cases} \mathcal{P}_2(E) & \to & \{a_1, \dots, a_r\} \\ \{x,y\} & \mapsto & \sigma(|x-y|) \end{cases}.$$

Pour $n+1 \geqslant N(r)$, on a x, y, z distincts dans $[\![1; n+1]\!]$ tel que

$$\chi(\{x,y\}) = \chi(\{x,z\}) = \chi(\{y,z\}).$$

On suppose $x < y < z$, et on pose

$$X := y - x, \quad Y := z - y \quad \text{et} \quad Z := z - x,$$

on a bien $X, Y, Z \in [\![1;n]\!]$. Ainsi, on a

$$X + Y = Z \quad \text{et} \quad \sigma(X) = \sigma(Y) = \sigma(Z).$$

Donc on peut prendre $s(r) = N(r) - 1$ pour bien vérifier $n+1 \geqslant N(r)$. □

Démonstration du théorème. Soit $r \in \mathbb{N}^*$, on prend un nombre premier $p > s(r)$. On pose l'ensemble

$$A = \{a^r, a \in (\mathbb{Z}/p\mathbb{Z})^\times\}$$

qui est un sous groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$. On partitionne $(\mathbb{Z}/p\mathbb{Z})^\times$ par les classes à gauche de A :

$$(\mathbb{Z}/p\mathbb{Z})^\times = \bigsqcup_{i=1}^{k} a_i A \quad \text{où } a_i \in (\mathbb{Z}/p\mathbb{Z})^\times \text{ et } k = |(\mathbb{Z}/p\mathbb{Z})^\times / A|.$$

On veut prouver que A est de cardinal $\dfrac{p-1}{\text{pgcd}(p-1,r)}$. On sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, donc il existe $\xi \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre $p-1$ tel que ξ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. Donc ξ^r engendre A [1], or ξ^r est d'ordre $\dfrac{p-1}{\text{pgcd}(p-1,r)}$. Ainsi A est de cardinal $\dfrac{p-1}{\text{pgcd}(p-1,r)}$.

Donc $k = \text{pgcd}(p-1,r) \leqslant r$.

On prend l'application

$$\sigma : \left\{ \begin{array}{ccc} [\![1, p-1]\!] & \to & \{a_1, \ldots, a_k\} \\ x & \mapsto & a_i \text{ SSI } \bar{x} \in a_i A \end{array} \right. .$$

On a $p-1 \geqslant s(r)$ et $k \leqslant r$, donc il existe $X, Y, Z \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $X + Y = Z$ et X, Y, Z appartiennent à la même classe $a_i A$, d'où on peut écrire

$$a_i x^r + a_i y^r = a_i z^r$$

avec a_i inversible, par conséquent, on a

$$x^r + y^r = z^r$$

dans $\mathbb{Z}/p\mathbb{Z}$ et x, y, z tous non nuls dans $\mathbb{Z}/p\mathbb{Z}$ car ils sont dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

□

Astuces de l'agrégatif :

Le développement est relativement long, en fonction de la leçon dans laquelle je mets ce développement je choisissais ce que je démontrais

- pour la 120, je passe forcément plus de temps sur la dernière démonstration, j'enlève la preuve du lemme 1, en disant que la preuve était une récurrence non triviale utilisant le lemme des tiroirs
- pour la 126, je fais à peu près comme pour la 120
- pour la 190, je passe vite sur la preuve du théorème en temps que tel car l'outil de dénombrement que l'on utilise est le lemme des tiroirs dans la preuve du lemme 1.

1. il suffit d'écrire ... en disant que chaque élément α de $(\mathbb{Z}/p\mathbb{Z})^\times$ s'écrit $\alpha = \xi^k$ avec $k \in \mathbb{Z}$