Théorie de Ramsey et Théorème de Schur

Fermat et les hyperchaussettes

Soit E un ensemble de cardinal n, et soit $\mathcal{A}$ l'ensemble des parties de E à deux éléments. Il sera pratique dans la suite de voir E comme les sommets d'un graphe complet et $\mathcal{A}$ comme l'ensemble des arêtes du graphe complet sur E. On colorie les arêtes du graphe, c'est-à-dire que l'on introduit une application χ de $\mathcal{A}$ dans un ensemble $K = \{1, \cdots, k\}$ de couleurs, de cardinal k.

Exemple 0.1. On suppose que $E = \{1, \cdots, 6\}$ et $k = 2$. Alors, dans tout coloriage de $\mathcal{A}$, on peut trouver un triangle unicolore[1]. En effet, il y a 5 arêtes qui partent de 1. On a forcément, parmi ces 5 arêtes , au moins 3 arêtes de même couleur, disons de couleur 1 : on peut supposer que $\{1, 2\}$, {1,3}, {1,4} sont de couleur 1. Si parmi ces arêtes, une seule est de couleur 1, disons l'arête $\{2, 3\}$, on a trouvé un triangle de couleur 1, nommément $\{1, 2, 3\}$. Sinon, $\{2, 3, 4\}$ est de couleur 2. Dans les deux cas, on a trouvé un triangle unicolore.

Dans l'exemple qui précède[2], on a implicitement utilisé le principe des tiroirs. Rappelons-le :

Principe des tiroirs : Si n chaussettes occupent m tiroirs, un des tiroirs doit contenir au moins $\lceil \frac{n}{m} \rceil$ chaussettes, où $\lceil x \rceil$ désigne la partie entière par excès de x, c'est-à-dire $-E(-x)$.

C'est avec cet outil élémentaire que l'on va s'attaquer à l'existence de solutions à l'équation de Fermat modulaire. Comme quoi on commence avec des chaussettes et on finit en grandes pompes !

1. Si l'on veut éblouir en société, on peut raconter l'histoire comme ceci. Parmi 6 personnes, soit 3 d'entre elles se connaissent mutuellement, soit 3 personnes ne se connaissent pas mutuellement. « Se connaître » et « ne pas se connaître » constituent les deux couleurs d'arêtes que l'on construit sur le graphe complet des 6 personnes.

2. Attention tout de même à cet exemple, si élémentaire, qui donne l'illusion que l'on va partir la fleur au fusil généraliser par récurrence le cas pour k couleurs !

Exercice 0.2. [Théorème de Ramsey et théorème de Schur sur l'équation de Fermat] On considère, sur un ensemble E de cardinal n, les arêtes du graphe (complet) colorées par k couleurs ($k \geq 2$), voir ci-dessus. On veut montrer que pour n assez grand, il existe au moins un triangle unicolore sur E (comme dans l'exemple ci-dessus).
On va supposer dans la suite $n \geq k^{k+1}$, et on commence par construire une suite $x_1, x_2, \cdots, x_{k+2}$ d'éléments de E possédant la propriété suivante :
(*) Pour tout i de 1 à $k+1$, les arêtes $\{x_i, x_j\}$ sont de même couleur quel que soit $j > i$.

1. On pose $E_0 := E$ et on fixe un élément x_1 dans E. Montrer qu'il existe une couleur c_1 telle que x_1 est attaché à n_1 sommets de E_0 de couleur c_1, avec $n_1 \geq k^k$. On notera par la suite E_1 l'ensemble de ces n_1 sommets (bien entendu, $x_1 \notin E_1$).
2. Montrer par récurrence sur m, $0 \leq m \leq k+2$, que l'on peut construire
   (i) une suite de parties $E_{m-1} \subsetneq E_{m-2} \subsetneq \cdots \subsetneq E_0$, avec $n_i := |E_i| \geq k^{k-i+1}$,
   (ii) une suite de couleurs $c_1, c_2, \cdots, c_{m-1}$ dans K,
   (iii) une suite d'éléments $x_1, x_2, \cdots, x_{m-1} \in E$, $x_i \in E_{i-1} \backslash E_i$, telle que, pour tout $1 \leq i \leq m-1$, et $x \in E_i$, l'arête $\{x_i, x\}$ est de couleur c_i.
3. Montrer alors la propriété (*), puis, l'existence d'un triangle unicolore dans E.
4. **Application au théorème de Schur :** on colorie cette fois les *sommets* de l'ensemble $E := \{1, \cdots, n\}$ par k couleurs, c'est-à-dire que l'on construit une application χ_0 de E dans K. Montrer que, pour n assez grand, on peut toujours trouver $1 \leq a, b \leq n$, tels que $a + b \leq n$, avec $a, b, a+b$ de même couleur.
5. **Equation de Fermat modulo p :** on fixe un entier $k > 1$. Pour p premier, on pose ici $E = \{1, \cdots, p-1\}$. On fixe un générateur du groupe multiplicatif $\mathbb{F}_p^*$ et soit α le représentant dans E de ce générateur. Pour tout m, $1 \leq m \leq p-1$, on note e_m l'unique représentant dans E de la classe de α^m modulo p. On prend $K := \{1, \cdots, k\}$ pour l'ensemble des couleurs, et on colorie E par l'application χ_0 qui envoie e_m sur l'unique représentant de m modulo k dans K, noté $\chi_0(e_m)$. Appliquer le théorème de Schur à ce coloriage et en déduire que pour p premier assez grand, il existe des solutions non triviales à l'équation de Fermat $x^k + y^k = z^k$ modulo p.

Avant de commencer la correction, regardons ce que l'on cherche à faire avec la propriété (*). On veut ordonner des sommets parmi les éléments de E de sorte que toutes les flèches partant d'un sommet vers un sommet qui lui succède ont même couleur. Par exemple $a < b < c < d$ avec $c_1 = 1$, $c_2 = 2$, $c_3 = 1$ (où la couleur 1 est en trait plein et la 2 en pointillé).

$$\begin{tikzcd} a \arrow[r] \arrow[d] \arrow[dr] & d \\ b \arrow[r, dotted] \arrow[ur, dotted] & c \arrow[u] \end{tikzcd}$$

1. Il y a exactement $n-1$ arêtes qui partent de x_1, et il y a k couleurs. Par le principe des tiroirs, il existe une couleur c_1, telle que $n_1 := \lceil \frac{n-1}{k} \rceil$ arêtes partant de x_1 sont de couleur c_1. Comme $n \geq k^{k+1}$,

$$n_1 = \lceil \frac{n-1}{k} \rceil \geq \lceil k^k - \frac{1}{k} \rceil = k^k, \text{ car } k \geq 2.$$

2. La question 1 prouve que l'on peut passer du rang $m = 1$ au rang $m = 2$. La récurrence, du cas m au cas $m + 1$, n'en est pratiquement qu'un copier-coller, et seule la condition $m \leq k + 1$ mériterait que l'on s'y attarde. Donnons tout de même la preuve complète par soucis de clarté.

   Supposons les assertions vraies jusqu'au rang $m \leq k + 1$. On choisit x_m dans E_{m-1} et on considère toutes les arêtes de type $\{x_m, x\}$, où x parcourt $E_{m-1} \backslash \{x_m\}$. Il y a donc $n_{m-1} - 1$ arêtes, et toujours k couleurs. Par le principe des tiroirs, il existe une couleur c_m qui est représentée par $\lceil \frac{n_{m-1}-1}{k} \rceil$ arêtes. Soit E_m l'ensemble des x tels que $\{x_m, x\}$ est de couleur c_m. On a alors :

$$n_m = \lceil \frac{n_{m-1} - 1}{k} \rceil \geq \lceil \frac{k^{k-m+2} - 1}{k} \rceil = \lceil k^{k-m+1} - \frac{1}{k} \rceil = k^{k-m+1} \geq k^{k-(k+1)+1} = 1.$$

   On voit donc en particulier que E_m n'est pas vide. Les points (i), (ii), (iii) sont assurés au rang m par récurrence et par la formule ci-dessus.

3. Notons que l'on est passé du rang m à $m+1$ pour $m \leq k+1$. On peut donc appliquer (i), (ii) et (iii) avec $m = k + 2$; on trouve alors $x_1, x_2, \cdots, x_{k+1}$ avec $n_{k+1} \geq 1$. Ceci assure au moins un élément x_{k+2} dans E_{k+1}. Bilan des courses, pour tout i de 1 à $k + 1$, $\{x_i, x_j\}$ est de couleur c_i, dès que $i < j \leq k + 2$.

   La suite de couleurs $(c_1, \cdots, c_{k+1})$ est une suite dans un ensemble à k éléments ; il y a donc par le principe des tiroirs au moins une couleur qui se repète $\lceil \frac{k+1}{k} \rceil = 2$ fois. Soit ℓ, $1 \leq \ell \leq k$, une telle couleur, et $1 \leq u < v \leq k + 1$ tels que $c_u = c_v = \ell$.

   Il existe w, tel que $u < v < w$, quitte à prendre $w = k+2$. Par construction, il vient que les arêtes $\{x_u, x_v\}$, $\{x_u, x_w\}$, $\{x_v, x_w\}$ sont de couleur ℓ. On a donc trouvé un triangle unicolore dans E.

4. On considère le coloriage suivant des arêtes du graphe complet sur E :

$$\chi_1 (\{i, j\}) = \chi_0 (j - i), \; 1 \leq i < j \leq n.$$

   Après avoir vérifié que χ_1 était bien défini, on peut affirmer, d'après la question qui précède que, pour n assez grand, il existe un triangle unicolore. On peut donc trouver $u < v < w$ tels que les arêtes entre u, v et w sont de même couleur. Cela signifie que $\chi_0(v - u) = \chi_0(w - u) = \chi_0(w - v)$. On pose $a := v - u$, $b := w - v$, et on voit que $a + b = w - u \leq n$, et que a, b, $a + b$ sont de même couleur.

5. Mettons en équation les données de l'énoncé. Tout d'abord, pour tout m, il existe un entier q_m tel que

$$\alpha^m = pq_m + e_m, \; 1 \leq m \leq p - 1.$$

   D'autre part, la construction de χ_0 fournit une égalité

$$m = kq'_m + \chi_0(e_m), \; 1 \leq m \leq p - 1.$$

   On sait maintenant, d'après le théorème de Schur que l'on peut trouver dans E deux éléments e_a, e_b avec $e_a + e_b \in E$ et e_a, e_b, $e_a + e_b$ de même couleur. Soit r cette couleur commune et c tel que $e_c = e_a + e_b$, de sorte que

$$a = kq'_a + r, \; b = kq'_b + r, \; c = kq'_c + r.$$

On considère le triplet $\left(\alpha^{q'_a}, \alpha^{q'_b}, \alpha^{q'_c}\right)$ modulo p, qui est clairement constitué d'éléments tous non nuls modulo p. Montrons que ce triplet est solution de l'équation de Fermat $x^k + y^k = z^k$, réduite modulo p.

On pose donc $A := \alpha^{kq'_a} + \alpha^{kq'_b} - \alpha^{kq'_c}$; et il suffit de voir que p divise A. Or,

$$\alpha^r A = \alpha^a + \alpha^b - \alpha^c = p(q_a + q_b - q_c) + (e_a + e_b - e_c) = p(q_a + q_b - q_c).$$

Et ainsi, par le lemme d'Euclide, p divise A puisque p ne divise pas α.

Remarque 0.3. Le problème de l'existence d'un triangle unicolore introduit au théorème de Ramsey qui généralise la situation : on obtient également une borne, mais en remplaçant la notion d'arête par la notion de multi-arête (d'un hypergraphe), et le nombre 3 (pour le triangle) par n'importe quel nombre d. Il s'agit d'un théorème remarquable par son ubiquité en mathématique, en particulier en logique, de par l'utilisation du théorème de compacité qui sert à s'affranchir d'une estimation de la borne. On peut également noter un petit parfum de cohomologie dans la preuve du théorème de Ramsey (et dans la solution à la dernière assertion de la question 3). En effet, on passe d'un coloriage de $(d-1)$-multi-arêtes (ici de sommet), à un coloriage de d-multi-arêtes (ici d'arêtes).

Remarque 0.4. La propriété prouvée à la question 4 amène à la notion de *nombre de Schur*. Le nombre de Schur $S(k)$ est par définition le nombre maximal n tel que l'on puisse colorier l'ensemble $\{1, \cdots, n\}$ avec k couleurs sans trouver $a, b, a+b$ de même couleur. On voit facilement que $S(1) = 1$, $S(2) = 4$, ensuite, il faut l'aide d'un logiciel pour obtenir sans trop de mal $S(3) = 13$, $S(4) = 44$. Après, on ne sait plus trop, même si on conjecture $S(5) = 160$. Bref, des nombres hauts en couleur !