À la recherche du polynôme perdu...

Jean-Paul Delahaye [1]

La rubrique récréation informatique propose une petite énigme algorithmique ou à propos d'un thème de mathématiques discrètes susceptible d'intéresser un lecteur de 1024. La solution est donnée dans le numéro suivant.

Rappel et solution du problème précédent

Un arbitre dépose au hasard des chapeaux sur les têtes de N joueurs. Un joueur ne peut voir le chapeau qu'il a sur la tête. Les couleurs possibles des chapeaux sont prises parmi N, mais plusieurs des chapeaux utilisés peuvent avoir la même couleur. « Au hasard » signifie précisément que l'arbitre tire avec une roue de loterie équitable à N cases la couleur du chapeau de chaque joueur. L'arbitre interroge alors les N joueurs de l'assemblée qui répondent en même temps (ils écrivent par exemple leur réponse sur un papier et le montrent au même instant). Les joueurs ont pu avant le jeu convenir d'une méthode de jeu, mais pendant le jeu, ils n'échangent aucune information. Chaque joueur essaie de deviner la couleur du chapeau qu'il a sur la tête. Si l'un d'eux réussit, alors l'assemblée des joueurs gagne un voyage collectif gratuit... au prochain congrès de la SIF.

On vérifie sans peine que si les joueurs jouent au hasard, ils ont une probabilité de gagner de $1-(1-\frac{1}{N})^N$. Cette suite a pour limite $1-\frac{1}{e}=0,6321...$, ce qui signifie qu'en gros les N joueurs (s'ils sont assez nombreux et jouent au hasard) gagnent avec une probabilité de 63%. C'est assez bien, mais s'ils sont malins, ils peuvent être certains à 100% de gagner. Quel algorithme de jeu (convenu entre eux avant que l'arbitre pose les chapeaux) doivent-ils appliquer pour cela ?

1. Université de Lille 1, Sciences et Technologies, Laboratoire d'Informatique Fondamentale de Lille, UMR 8022 CNRS, Bât M3-ext, 59655 Villeneuve d'Ascq Cedex. E-mail : delahaye@lifl.fr.

SOLUTION. Les joueurs conviennent entre eux d'une numérotation des couleurs de 1 à N, et d'une numérotation des joueurs, elle aussi de 1 à N. Cette convention est une *rupture de symétrie*. Ils décident alors que le joueur k fera la somme des nombres associés aux couleurs des chapeaux qu'il voit et proposera, pour la couleur de son chapeau, celle qui fait du total de toutes les valeurs des couleurs un nombre congru à k modulo N (autrement dit un nombre dont le reste quand on le divise par N est k).

Expliquons sur un exemple cette consigne de choix. Supposons que $N = 5$ et que le joueur 2 observe les chapeaux de couleur 1, 3, 1, 4. Le joueur 2 recherche un entier x tel que $1+3+1+4+x = 2 \pmod 5$. La solution est $x = 3$ car $1+3+1+4+3 = 12 = 2 \pmod 5$. Donc le joueur 2 propose la couleur 3 comme couleur de son propre chapeau.

En opérant de cette façon, et si bien sûr chaque joueur mène correctement son calcul, l'assemblée des joueurs est certaine de gagner. En effet, la somme de toutes les couleurs utilisées vaut k modulo N, pour un certain entier k compris entre 1 et N (ce k n'est bien sûr connu d'aucun joueur). Or le joueur k, d'après la stratégie convenue, a choisi de jouer en faisant l'hypothèse que la somme inconnue valait k, et donc le joueur k a proposé la bonne couleur pour son propre chapeau. Notons que le joueur k est le seul qui donne la bonne réponse : tous les autres se trompent.

L'astuce de cette stratégie de jeu est que chaque joueur parie sur une valeur différente de la somme des couleurs modulo N. Comme les joueurs sont au nombre de N et qu'il y a N couleurs, ils sont juste assez nombreux pour être certains que l'un d'eux (et un seul) gagnera. S'il y avait $N+1$ couleurs possibles et N joueurs alors, dans certains cas, cette méthode ne fonctionnerait pas.

Parmi les jolis résultats mathématiques démontrés à propos de ce type de problème, il faut citer celui-ci dû à Christopher Hardin et Alan Taylor[2]. Ils se sont intéressés au problème que nous venons d'envisager, mais ils ont imaginé que seules certaines vues étaient possibles. Par exemple, le joueur 2 voit le chapeau du joueur 3, le joueur 5 celui du joueur 1. Le graphe qui fixe « qui voit qui » est appelé *graphe de visibilité* et, bien sûr, on suppose toujours que le joueur numéro k ne voit pas son propre chapeau (pas d'arc dans le graphe reliant le nœud k à lui-même). Hardin et Taylor démontrent un double résultat :

> (A) Ils prouvent d'abord que s'il y a deux couleurs possibles de chapeaux, alors il existe une stratégie qui assure au moins une réponse exacte si et seulement si le graphe de visibilité comporte un cycle ($J(1)$ voit $J(2)$, $J(2)$ voit $J(3)$, ..., $J(p)$ voit $J(1)$).
>
> (B) La seconde partie de leur résultat concerne le cas d'un jeu avec une assemblée de N joueurs et N couleurs de chapeaux. Dans un tel cas, il existe une

2. Christopher Hardin, Alan Taylor, An Introduction to Infinite Hats Problems, *The Mathematical Intelligencer*, 30-4, pp. 2–6 (2008).

stratégie assurant qu'au moins une réponse est juste si et seulement si le graphe de visibilité est complet (chaque joueur voit tous les chapeaux sauf le sien).

Cela signifie que pour le problème traité juste au-dessus, si un seul des N joueurs ne peut voir un des chapeaux des autres joueurs, alors il n'existe aucune méthode de jeu assurant de gagner dans 100% des cas.

Nouveau problème : Dépensez le moins possible

Vous êtes face à une machine qui, lorsque vous lui donnez un entier n, vous répond par $P(n)$, où P est un polynôme à coefficients entiers positifs dont vous ignorez le degré et les coefficients. Vous voulez connaître le polynôme que la machine utilise (donc son degré et ses coefficients). Chaque calcul de $P(n)$ est payant et vous coûte 100 euros. Combien allez-vous dépenser en vous y prenant au mieux ?

Envoyez vos réponses à delahaye@lifl.fr. Le nom des 10 premiers lecteurs à me donner la bonne réponse (et à la justifier) seront mentionnés dans le prochain numéro de 1024.