*Balade dans le jardin des premiers*[1] *(Denise Vella-Chemla, 17.1.2019)*

On voudrait se rappeler ici d'un petit retour vers la physique.

Ce qu'on aimerait trouver, c'est une opération qui permettrait de passer directement d'un premier à un autre.

Voyons 1, qui n'est pas premier, comme le seul nombre entier qui, divisé par tous les autres nombres, dont les nombres premiers, a pour reste 1.

En ce moment, on est confronté à un problème particulier qui est "Etant donné un ensemble $\{p_1, p_2, \ldots, p_k\}$ de nombres premiers successifs[2], quel est le plus petit nombre premier supérieur à $p_k$ et qui, quel que soit $p_k$, n'est pas congru à $p_k - 1$ $(mod\ p_k)$ ?". On voudrait simplement effectuer une petite promenade à partir de 1 à base de sauts additifs qui amènerait au nombre premier minimum recherché.

Pourquoi des sauts additifs ? Parce que la multiplication fait sortir de l'ensemble des nombres premiers : un nombre premier, multiplié par quoi que ce soit, donne un nombre composé, et ça n'est pas ce qu'on cherche.

Pour simplifier notre problème, on va ne considérer que les nombres impairs, et on va se fixer sur les nombres premiers $3, 5, 7$.

Ce qu'il faut alors avoir à l'esprit, c'est la notion de saut quantique, ou saut discret : l'électron saute de couche en couche et pour ce faire, il absorbe une quantité d'énergie de valeur fixée.

Ici, c'est pareil : quand on saute de 3 en 3 à partir d'un nombre, le reste des nombres obtenus dans leur division par 3 ne change pas. Quand on saute de 5 en 5, c'est le reste des nombres obtenus dans leur division par 5 qui ne change pas et plus généralement, quand on saute de $p$ en $p$, c'est le reste des nombres obtenus dans leur division par $p$ qui ne change pas. Dit quantiquement, pour qu'un nombre donne son reste modulo $p$ à un autre nombre, il faut lui ajouter un multiple de $p$.

On part de 1, on doit sauter de nombre en nombre à la recherche d'une solution qui est un nombre premier supérieur à 7 (dont le reste n'est pas 0 dans les divisions par 3, 5 et 7) et dont le reste n'est pas 2 $(mod\ 3)$, 4 $(mod\ 5)$ et 6 $(mod\ 7)$. Quels choix s'offrent à nous ? Soit faire des sauts de 6 en 6 pour conserver le reste modulo 3 (tout en étant impair), soit faire des sauts de 10 en 10 pour conserver le reste modulo 5 (tout en étant impair), soit faire des sauts de 14 en 14 pour conserver le reste modulo 7 (tout en étant impair).

On sait qu'on trouvera forcément une solution qui vérifie les différentes contraintes du point de vue des congruences, c'est le théorème des restes chinois qui l'assure, et une solution qui soit un nombre premier (car toute suite arithmétique en contient) mais ce qui nous intéresse ici, c'est un moyen sûr de parvenir (directement ?) à la solution minimale car on cherche à majorer cette valeur minimale[3].

1. ou bien balade dans le premier des jardins, ou bien écrire en prose pour ne pas oublier, ou bien écrire en prose pour ne pas être oubliée.

2. supérieurs ou égaux à 3, on oublie 2, et on fera des sauts pairs pour rester dans les impairs.

3. Pour résoudre la conjecture de Goldbach, il faudrait être capable de majorer la solution recherchée par $\frac{n}{2}$ lorsqu'on cherche les décomposants de Goldbach de $n$, les nombres premiers à considérer alors étant les nombres premiers inférieurs à $\sqrt{n}$.

Déroulons l'algorithme de recherche en traitant le module 3 d'abord :

| | | |
|---|---|---|
| $1+2\times 3=7$ | $\to 7\equiv 1\not\equiv 0,2\ (3)$<br>$\to 7\equiv 2\not\equiv 0,4\ (5)$<br>$\to 7\equiv 0\ (7)$ | $\to ok\ (3)$<br>$\to ok\ (5)$<br>$\to raté\ (7)$ |
| $1+4\times 3=13$ | $\to 13\equiv 1\ (3)\not\equiv 0,2\ (3)$<br>$\to 13\equiv 3\not\equiv 0,4\ (5)$<br>$\to 13\equiv 6\ (7)$ | $\to ok\ (3)$<br>$\to ok\ (5)$<br>$\to raté\ (7)$ |
| $1+6\times 3=19$ | $\to 19\equiv 1\not\equiv 2\ (3)$<br>$\to 19\equiv 4\ (5)$ | $\to ok\ (3)$<br>$\to raté\ (5)$ |
| $1+8\times 3=25$ | $\to 25\equiv 1\not\equiv 0,2\ (3)$<br>$\to 25\equiv 0\ (5)$ | $\to ok\ (3)$<br>$\to raté\ (5)$ |
| $1+10\times 3=31$ | $\to 31\equiv 1\not\equiv 2\ (3)$<br>$\to 31\equiv 1\not\equiv 0,4\ (5)$<br>$\to 31\equiv 3\not\equiv 0,6\ (7)$ | $\to ok\ (3)$<br>$\to ok\ (5)$<br>$\to ok\ (7)$ |

Déroulons l'algorithme de recherche en traitant le module 5 d'abord :

| | | |
|---|---|---|
| $1+2\times 5=11$ | $\to 11\equiv 2\ (3)$ | $\to raté$ |
| $1+4\times 5=21$ | $\to 21\equiv 0\ (7)$ | $\to raté$ |
| $1+6\times 5=31$ | $\to 31$ | $\to ok$ |

Déroulons l'algorithme de recherche en traitant le module 7 d'abord :

| | | |
|---|---|---|
| $1+2\times 7=15$ | $\to 15\equiv 0\ (3)$ | $\to raté$ |
| $1+4\times 7=29$ | $\to 29\equiv 2\ (3)$ | $\to raté$ |
| $1+6\times 7=43$ | $\to 43\equiv 1\ (3), 43\equiv 3\ (5), 43\equiv 1\ (7)$ | $\to ok$ |

La solution obtenue en commençant par le module 7 (qui est 43) est plus grande que celle obtenue en commençant par le module 3 (qui est 31).

Est-ce toujours le cas (solution la plus petite en commençant par le module le plus petit sous prétexte que les deux congruences à éliminer sont 0 et $p-1$ $(mod\ p)$ ?
Quelle est la solution minimale pour le problème considéré ?
A force de sauts, ne va-t-on pas atterrir sur des nombres supérieurs à $p_{max}^2$ (avec $p_{max}$ le plus grand nombre premier de l'ensemble considéré), dont il faudrait alors s'assurer de leur indivisibilité par des nombres premier supérieurs à $p_{max}$ ? Quelle est la solution minimale si la seconde congruence à éliminer par module n'est pas $p-1$ mais une classe de congruence quelconque ?

On pense à un arbre de décision. Pour chaque module, soit le nombre obtenu vérifie la contrainte imposée (non congruence à 0 et $p-1$), soit pas. On imagine un arbre binaire à $2^k$ feuilles, mais on n'arrive pas bien à voir encore comment mélanger cet arbre de décision à notre arbre de promenade par sauts quantiques...

On a l'impression qu'il faut mener un raisonnement combinatoire : $1+2\times 3\times 5$ respecte les contraintes modulo 3 et 5, on s'interroge sur son respect des contraintes modulo 7 ; $1+2\times 3\times 7$ respecte les contraintes modulo 3 et 7, on s'interroge sur son respect des contraintes modulo 5 ; $1+2\times 5\times 7$ respecte les contraintes modulo 5 et 7, on s'interroge sur son respect des contraintes modulo 3. Serait-il possible que les trois nombres pêchent simultanément selon le module sur lequel on n'a pas d'assurance ? Est-ce que le maximum de ces 3 nombres est la borne cherchée ? De toute façon, utiliser les primorielles augmente trop la valeur des nombres. Ne pourrait-on être assuré de trouver une solution avec un ou deux pas selon chaque module, ou guère plus, sous prétexte qu'un saut de longueur $2p_i$ change le reste modulo tout $p_j$ avec $j$ différent de $i$ ?

Ce genre de raisonnement montre bien qu'on est ennuyé car il faut répondre à plusieurs questions simultanément et que la réponse à l'une des questions amène une incertitude sur l'une des autres questions posées et dont on nécessite cependant d'avoir la réponse aussi. On a là une illustration de l'aspect si quantique des nombres premiers.

Cela nous ramène aussi à de vieux souvenirs de parcours d'arêtes de polytopes (des simplexes), en recherche opérationnelle, à la recherche là-aussi d'une solution optimale selon une certaine fonction de coût,

et qui vérifiait certaines contraintes, si ce n'est que les contraintes en question étaient des inéquations linéaires, et qu'on se plaçait donc dans des espaces vectoriels, alors qu'ici, l'action se situe dans des produits cartésiens de corps premiers, sur lesquels il n'y a pas de notion d'ordre...

C'est comme un mirage, quand on s'approche, ça s'éloigne.