DES CONJECTURES

Eugène EHRHART

Nous allons d'abord faire le point pour quelques conjectures classiques, en relavant le rôle joué à présent par l'ordinateur. Puis *nous montrerons que la conjecture de Goldbach est sans doute exacte.* Enfin nous signalerons trois nouveaux problèmes ouverts sur les nombres premiers.

I.— Quelques conjectures arithmétiques historiques

Parmi les plus connues — qui ont fasciné une foule de chercheurs grands ou moins grands par un énoncé simple contrastant avec une grande difficulté — citons les conjectures :
1) **de Fermat** : l'équation diophantienne $X^n + Y^n = Z^n$ n'a pas de solution pour $n > 2$;
2) **de Gauss** : pour tout entier n, $2^{2^n} + 1$ est un nombre premier;
3) **d'Euler** : une puissance n-ième n'est décomposable en une somme de moins de n puissances n-ièmes;
4) **de Goldbach** : tout entier pair est somme de deux nombres premiers (à part 2, car 1 ne compte pas comme nombre premier);
5) **des nombres premiers jumeaux** (*) : il y en a une infinité;
6) **de Collatz** : quel que soit l'entier positif u_1, un terme égal à 1 figure dans la suite

$$u_{n+1} = \begin{cases} 3u_n + 1 & \text{si } u_n \text{ est impair,} \\ \frac{1}{2}u_n & \text{si } u_n \text{ est pair.} \end{cases}$$

Où en sont actuellement ces conjectures?
1) En 1983 FALTING a prouvé que l'équation ne pourrait avoir qu'un nombre fini de solutions pour $n > 2$. En 1984 MORISHIMA et GUNDERSON ont montré que si l'équation avait une solution, **il faudrait que** $n > 5710^9$, et l'on verra qu'**il faudrait aussi que** $X, Y, Z > n$. Y a-t-il quelqu'un qui doute encore de l'exactitude de la conjecture?

Sans nuire à la généralité on peut supposer $X > Y$. Comme $Z \geq Y + 1$,

$$X^n \geq (Y+1)^n - Y^n > nY^{n-1}. \tag{1}$$

D'où $n/Y < (X/Y)^n < 1$. Donc $Z > Y > n$, mais aussi $X > n$, car (1) donne

$$n \log X > \log n + (n-1) \log Y > n \log n$$

la dernière ingégalité pouvant s'écrire :

(*) Deux premiers sont dits jumeaux si leur différence est 2.

$$(n-1)\log Y > (n-1)\log n.$$

2) EULER a constaté que la conjecture est déjà en défaut pour $n = 5$. Depuis on a trouvé d'autres contre-exemples.
3) Deux contre-exemples infirment la conjecture :

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5 \qquad \text{(trouvé en 1966)},$$
$$95800^4 + 217519^4 + 414560^4 = 422418^4 \qquad \text{(trouvé en 1971)}.$$

Une première grande victoire de l'ordinateur!
4) Nous montrerons plus loin que la conjecture est sans doute exacte.
5) Un raisonnement "**plausible**" conduit à estimer que le nombre de paires de jumeaux jusqu'à n grand, est de l'ordre de :

$$J_n \simeq 1,32032\frac{n}{(\log n)^2}$$

ce qui impliquerait l'exactitude de la conjecture [1]. Soit j le nombre de paires de jumeaux de l'intervalle $(10^m, 10^m + 150000)$ et j' la valeur approchée déduite de la formule empirique précédente. Alors [1]

m	8	9	10	11	12	13	14	15
j	601	466	389	276	276	208	186	161
j'	584	461	374	309	259	221	191	166

On voit que l'approximation est remarquable : **la conjecture 5 est probablement vraie.**

Par ailleurs j'ai montré que **dans la suite illimitée des nombres premiers il existe des intervalles arbitrairement grands sans jumeaux** [2].

6) Malgré plusieurs prix offerts pour sa résolution la conjecture, vieille d'une trentaine d'années, reste ouverte. ISHIHATA l'a vérifiée pour $u_1 < 3.10^{12}$.

Remarque : La réponse, oui ou non, à ces problèmes importe d'ailleurs peu pour la science mathématique. Ici ce n'est pas tant le résultat qui compte, que le moyen d'y parvenir. Il est bien connu que la conjecture de FERMAT, par exemple, a conduit KUMMER à introduire les idéaux, théorie belle et féconde.

II.— L'aide de l'ordinateur

Pour **infirmer** une conjecture arithmétique l'ordinateur est un outil puissant, puisqu'il suffit de trouver un seul contre-exemple. C'est ainsi qu'on a pu écarter celle d'EULER.

Mais l'ordinateur peut aussi **confirmer** une conjecture, si on peut réduire une question à l'examen d'un nombre fini, même très grand, de cas répétitifs. Ainsi il y a quelques années la conjecture des quatre couleurs a enfin été validée, en la ramenant à quelques 2000 cas de figures, que l'ordinateur a tranchés. Récemment, je me posais la question : *Quel est le plus petit cercle passant par juste cinq nœuds d'un quadrillage* J'ai pu ramener ce problème ardu à écarter près de 1000 cercles, ce que l'ordinateur a réalisé. Le cercle conjecturé était le bon : $3(X^2+Y^2)-25(X+Y)=0$, en axes normaux du quadrillage.

III.— Le raisonnement plausible

En voici un exemple, appliqué à la conjecture de GOLDBACH. En face de chaque entier pair n de 4 à 100, plaçons le nombre d de ses décomposotitions en sommes de deux nombres premiers.

n	d	n	d	n	d	n	d
4	1	28	2	52	3	76	4
6	1	30	3	54	5	78	6
8	1	32	2	56	3	80	4
10	2	34	4	58	4	82	5
12	1	36	4	60	6	84	8
14	2	38	2	62	3	86	5
16	2	40	3	64	5	88	4
18	2	42	4	66	6	90	9
20	2	44	3	68	2	92	4
22	3	46	4	70	5	94	5
24	3	48	5	72	6	96	7
26	3	50	4	74	5	98	3
						100	6

On constate que la variation de d est très capricieuse, mais que "*en gros*" d est croissant, croissance plus visible dans les deux listes ci-dessous. La première donne dans chaque centaine jusqu'à 1200, le plus grand d avec le plus grand n correspondant. La seconde donne pour chaque d de 1 à 12 le plus grand n associé jusqu'à 1200.

d	9	14	19	27	30	32	32	42	50	50	56	57
n	90	180	270	390	420	510	660	780	840	990	1050	1170

d	1	2	3	4	5	6	7	8	9	10	11	12
n	12	68	128	152	188	332	398	368	488	632	692	808

Nous allons montrer que *pour n grand cette croissance "en gros" continue* toujours. Quoique, par suite de certaines approximations, notre raisonnement manque

parfois de rigueur, il permet, je pense, de conclure que la conjecture de GOLDBACH est très probablement exacte.

2	$n-2$
3	$n-3$
4	$n-4$
$\vdots$	$\vdots$
$K-2$	$K+2$
$K-1$	$K+1$
K	K

Soit un nombre pair $n = 2K$. En face des entiers consécutifs de 2 à K, plaçons leurs compléments à n. On sait que pour K grand les deux colonnes de cette liste contiennent sensiblement respectivement $\frac{K}{\log K}$ et $\frac{2K}{\log 2K} - \frac{K}{\log K}$ nombres premiers. La probabilité qu'en face d'un nombre premier choisi de gauche se trouve un nombre premier de droite est :

$$P_1 \simeq \frac{\frac{2K}{\log 2K} - \frac{K}{\log K}}{K} = \frac{2\log K - \log K - \log 2}{\log K \log 2K} \simeq \frac{1}{\log 2K}.$$

(On suppose ici une équiprobabilité, qui n'est qu'approximative.) La probabilité qu'un premier déterminé de gauche ne soit pas en face d'un premier de droite est donc

$$P_1' \simeq 1 - \frac{1}{\log 2K}.$$

Par suite la probabilité qu'aucun premier de gauche ne soit en face d'un premier de droite — c'est-à-dire que $n = 2K$ ne soit décomposable en somme de deux nombres premiers — est inférieure à :

$$P = \left(1 - \frac{1}{\log 2K}\right)^{\frac{K}{\log K}}$$

car pour le second premier choisi à gauche

$$P_2 = \frac{\frac{2K}{\log 2K} - \frac{K}{\log K}}{K-1} > \frac{1}{\log 2K}$$

puisqu'un des non-premiers de droite est maintenant supprimé. Donc $P_2' < 1 - 1/\log 2K$. Pareillement pour les premiers suivants choisis à gauche : la suite $P_1', P_2', P_3', \ldots$ est décroissante. Or quand K croît, P **décroît rapidement et tend vers zéro**. En effet

$$P = \left[\left(1 - \frac{1}{\log 2K}\right)^{\log 2K}\right]^{\frac{K}{\log K \log 2K}}$$

où l'expression entre crochets croît lentement et tend vers $1/e$, pendant que son exposant croît et tend vers l'infini.

Remarque

Par un raisonnement probabiliste analogue, plausible au sens de POLYA [3], j'ai montré que le produit

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{p}\right)\log p,$$

où les dénominateurs sont les nombres premiers jusqu'à p, est *"voisin" de* $1/2$ *quand* p *est très grand.* (La valeur exacte de la limite est 0,561...) [4].

IV.— Conjectures sur les nombres premiers.

Voici une supposition qui implique celle de GOLDBACH. Elle est vérifiée pour les nombres jusqu'à 1200, et par le raisonnement plausible fait plus haut son exactitude est également très probable.

Conjecture 1. Tout entier pair supérieur à 12 est, **de plus d'une manière**, la somme de deux nombres premiers (plus de 10 manières pour $n > 632$).
Le chapitre III suggère aussi :

Conjecture 2. Le nombre de décomposition de l'entier pair n en somme de deux premiers tend vers l'infini avec n.
Enfin généralisons le problème des jumeaux :

Conjecture 3. Tout nombre pair est, d'une infinité de manières, la différence de deux nombres premiers.

Je remercie François PLUVINAGE. A l'aide de l'ordinateur, il a calculé les d des nombres pairs $n < 1200$ et écarté près de 1000 cercles dans le problème terminal du chapitre II.

Bibliographie

[1] P. DAVIS & R. HERSCH.– *The Mathematical Experience.* p. 215–216, Boston, 1982.
[2] E. EHRHART.– *On prime numbers.* The Fibonaci Quarterly, p. 271–274, août 1988.
[3] G. POLYA.– *Les Mathématiques et le raisonnement plausible.* Gauthier-Villars, 1958.
[4] E. EHRHART.– *Nombres premiers et calcul de probabilité.* Articles de mathématiques, p. 177, Cédic/Nathan, 1986.