

# SOMMES DE CARRÉS ET D'INVERSE POUR «PETITS» ET «GRANDS»

Christian Aebi

C.O. de la Gradelle & Collège Calvin, Genève

*En hommage à Nicolas Rouche, grand maître de l'écoute, de la pédagogie et de la mathématique, ayant toujours défendu une approche à large spectre de l'enseignement de cette dernière.*

## INTRODUCTION

L'arithmétique est certainement le seul domaine mathématique dans lequel un jeune élève peut comprendre, tester et s'émerveiller devant des conjectures dont la démonstration demeure momentanément encore hors de portée de la connaissance humaine. Citons trois exemples célèbres : le problème  $3n+1$ , l'existence d'une infinité de premiers jumeaux et la conjecture de Goldbach.

Je me propose ici d'exposer une expérience pédagogique portant sur les sommes de carrés et d'inverses. Bien souvent il suffit de partir d'un exercice classique, puis d'effectuer une légère perturbation sur les hypothèses de départ pour faire apparaître un problème défiant les experts actuels en théorie des nombres. Une de mes plus grandes joies dans mon métier d'enseignant consiste justement à montrer à mes élèves que nos préoccupations mathématiques sont très proches de celles des chercheurs d'aujourd'hui, que la grande quête à démystifier l'inconnu ne cesse de gagner du terrain et qu'ils pourront peut-être, qui sait, un jour y contribuer.

## UNE ACTIVITÉ ARITHMÉTIQUE POUR SECONDAIRE I ET II

Rien de tel que de soumettre à des élèves de 11<sup>e</sup> année (14-15 ans) un problème d'arithmétique comme ci-dessous, en ap-

parence très innocent<sup>1</sup>, pour susciter leur curiosité et les amener à se questionner sur les généralisations possibles.

**Question 1.** Est-il vrai que la somme des carrés des entiers de même parité compris strictement entre deux multiples de 5 consécutifs est encore un multiple de 5 ?

Souvent, il leur faut quelques minutes pour bien comprendre la question, maîtriser le vocabulaire en jeu, comme « parité », voire même « somme ». Mais ensuite, un peu d'expérimentation les convainc rapidement qu'il semble que la réponse soit affirmative. Deux types de preuves peuvent être trouvées :

a) Observer les résultats pour les nombres plus petits que 10 :  $1^2+3^2 = 10$  ;  $2^2+4^2 = 20$  ;  $6^2+8^2 = 100$  et  $7^2+9^2 = 120$ . Puis, l'algorithme de multiplication implique que pour deux entiers supérieurs ou égaux à 10 la somme de leurs carrés est divisible même par 10.

b) Sinon, une preuve classique consiste à regarder les nombres en question « modulo 5 » :

$$\begin{aligned} &(5n+1)^2+(5n+3)^2 \\ &= 50n^2+40n+10 \\ &= 5(10n^2+8n+2) \in M_5 \end{aligned}$$

et

$$\begin{aligned} &(5n+2)^2+(5n+4)^2 \\ &= 50n^2+60n+20 \\ &= 5(10n^2+12n+4) \in M_5 \end{aligned}$$

A la leçon suivante, je n'ai pu m'empêcher de leur proposer une petite extension :

**Question 2.** Est-il vrai que la somme des carrés des entiers de même parité compris strictement entre deux multiples de 7 consécutifs est encore un multiple de 7 ?

Cette fois-ci, je leur ai demandé d'obtenir une réponse sans mon aide et évidemment de prouver leur conjecture. A ma grande satisfaction, tout le monde a investi rapidement la recherche et un tout petit nombre est même arrivé jusqu'au bout. Par ailleurs, l'approche « modulo 7 » semble indispensable. A force de développer des expres-

<sup>1</sup> Car ne nécessitant essentiellement que l'identité  $(a+b)^2=a^2+2ab+b^2$ .

sions comme ci-dessous

$$(7n+1)^2+(7n+3)^2+(7n+5)^2$$

les élèves réalisent peu à peu que la réponse ne dépend que de  $1^2+3^2+5^2$  dans ce cas, puisque tous les autres termes sont des multiples de 7. Impossible alors de ne pas leur dire de se comporter comme « de vrais mathématiciens en herbe » en généralisant leur conjecture : *Est-il vrai que la somme des carrés des entiers de même parité compris strictement entre deux multiples de 9 consécutifs est encore un multiple de 9 ?* Et là, déception dès le premier essai  $1^2+3^2+5^2+7^2=84 \notin M_9$ . Mais, comme le résultat est vrai pour 5 et 7, des nombres premiers et que 9 est composé, l'on peut encore espérer que pour 11, voire même 13, la propriété de divisibilité se remanifeste. Et en un rien de temps, le simple calcul

$$1^2+3^2+5^2+7^2+9^2 = 165 = 11 \times 15$$

$$2^2+4^2+6^2+8^2+10^2 = 220 = 11 \times 20$$

permet de s'en assurer. A mon plus grand regret, je n'ai pu aller plus loin avec les élèves du C.O., qui en sont restés provisoirement sur leur faim, en s'imaginant que le résultat n'est vrai que pour des premiers > 3. J'ai donc poursuivi la recherche avec mes élèves de 3<sup>e</sup> année du gymnase qui avaient déjà démontré par récurrence en début d'année scolaire l'identité,

$$\sum_{k=1}^m k^2 = \frac{1}{6} m(m+1)(2m+1) \quad (1)$$

Je n'ai pas hésité à leur faire part du résultat obtenu par mes 11<sup>e</sup>, afin de leur soumettre directement la question :

**Question 3.** Quels sont les entiers impairs  $n$  qui divisent chacune des sommes  $1^2+3^2+5^2+\dots+(n-2)^2$  et  $2^2+4^2+6^2+\dots+(n-1)^2$  ?

Rapidement, à l'aide de leur calculatrice, ils ont obtenu la conjecture : *n ne doit pas être un multiple de 3.* Malgré le fait d'avoir étudié la formule (1), ils ont mis du temps pour factoriser la deuxième somme par  $2^2$  et à la réduire correctement. Malheureusement, il me semble que le fait d'avoir très peu exercé l'arithmétique de base dans leur cursus scolaire leur rend la tâche difficile et j'ai dû me résoudre à leur présenter un argument qui se résume ainsi :

Démonstration. La seconde équivalence peut s'écrire sous la forme :

$$4 \cdot (1^2 + 2^2 + 3^2 + \dots + (\frac{n-1}{2})^2) = \frac{1}{6} (n-1)(n+1)n.$$

Or, ces trois derniers facteurs sont premiers entre eux. Alors pour que  $n$  divise le produit, il est nécessaire et suffisant que  $(6, n) = 1$ , c'est-à-dire dans ce cas que  $3 \nmid n$ . D'autre part, si l'on soustrait à

$$\sum_{i=1}^{n-1} i^2$$

la somme

$$\sum_{i=1}^{(n-1)/2} (2i)^2$$

l'on obtient alors

$$\sum_{i=1}^{(n-1)/2} (2i-1)^2$$

qui se factorise en l'expression

$$\frac{1}{6} n(n-1)(n-2)$$

De manière similaire, les trois derniers facteurs étant premiers entre eux, on obtient la même conclusion.  $\diamond$

### VARIATION ET PROLONGEMENT

Un problème en apparence élémentaire et un peu du même type que celui précédemment présenté consiste à considérer un entier naturel  $n > 1$  et à observer le numérateur de la fraction irréductible de la somme des inverses des entiers de 1 à  $n-1$ .

**Question 4.** Quels sont les entiers naturels  $n$  qui divisent le numérateur de la fraction irréductible ci-dessous ?

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n-1}$$

En calculant à la main l'on voit aisément :

(1) pour  $n = 3$ , on a  $1 + \frac{1}{2} = \frac{3}{2}$  Oui !

(2) pour  $n = 4$ , on a  $1 + \frac{1}{2} + \frac{1}{3} = \frac{11}{6}$  Non

(3) pour  $n = 5$ , on a  $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12}$  Oui !

(4) pour  $n = 6$ , on a  $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} = \frac{137}{60}$  Non

(5) pour  $n = 7$ , on a

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \frac{49}{20} \quad \text{Oui!}$$

Si l'on manque de patience alors à l'aide d'une calculatrice programmable ou d'un logiciel de mathématique il est facile d'obtenir les entiers inférieurs à 100 qui vérifient la propriété de divisibilité : 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. De prime abord, une réponse semble évidente :

Lemme 1. Si  $p \geq 3$  est premier alors le numérateur de

$$\sum_{i=1}^{p-1} \frac{1}{i}$$

est divisible par  $p$ .

Démonstration.

Comme dans la preuve obtenue certainement par Gauss, concernant la somme d'entiers consécutifs, il suffit d'utiliser la « symétrie centrale du calcul » pour faire apparaître la propriété recherchée.

$$\sum_{i=1}^{p-1} \frac{1}{i} = \sum_{i=1}^{(p-1)/2} \frac{1}{i} + \frac{1}{p-i} = p \sum_{i=1}^{(p-1)/2} \frac{1}{i(p-i)}$$

Le dénominateur commun de la dernière somme ne contient que des nombres premiers  $< p$  dans sa décomposition en facteurs premiers. Il ne peut donc y avoir de simplification possible avec le facteur  $p$  devant la somme.  $\diamond$

Une autre propriété élémentaire que l'on peut aisément prouver concerne les nombres pairs.

Lemme 2. Si  $n$  est pair alors il ne peut diviser le numérateur de

$$\sum_{i=1}^{p-1} \frac{1}{i}$$

Démonstration. Voici encore un argument classique : considérer la plus grande puissance de 2 parmi les dénominateurs, que l'on notera  $2^m$ . Il va de soi qu'il ne peut y en avoir qu'une seule. Lorsqu'on met toute la somme au même dénominateur, il n'y a que des numérateurs pairs à l'exception du numérateur de  $\frac{1}{2^m}$  qui est impair.

La somme des numérateurs est donc forcément impaire.  $\diamond$

Les deux preuves ci-dessus peuvent être exposées aisément aux élèves du C.O. à condition de faire comme l'aurait suggéré Nicolas Rouche, en effectuant des preuves paradigmatiques<sup>2</sup>.

Si l'on observe plus précisément les numérateurs du lemme alors l'on constate qu'à partir de  $p = 5$  la divisibilité est même par  $p^2$ . Ce résultat est un grand classique de la théorie des nombres. La preuve donnée ci-dessous, qui démarre exactement de la même manière que dans celle du lemme, utilise le fait que la fonction  $\text{inv} : x \rightarrow x^{-1}$  est un isomorphisme de  $\mathbb{Z}^*_p$ , que

$$\frac{1}{k^2} \equiv \frac{1}{(p-k)^2} \pmod{p}$$

et se termine en appliquant (1).

Théorème (de Wolstenholme, 1862). Si  $p > 3$  est premier alors le numérateur de

$$\sum_{i=1}^{p-1} \frac{1}{i}$$

est divisible par  $p^2$ .

Démonstration.

$$\begin{aligned} \sum_{i=1}^{p-1} \frac{1}{i} &= \sum_{i=1}^{(p-1)/2} \frac{1}{i} + \frac{1}{p-i} \equiv (-p) \sum_{i=1}^{(p-1)/2} \frac{1}{i^2} \equiv \frac{(-p)}{2} \sum_{i=1}^{p-1} \frac{1}{i^2} \\ &\equiv \frac{(-p)}{2} \sum_{j=1}^{p-1} j^2 \equiv \frac{-1}{12} (p-1)p^2(2p-1) \end{aligned}$$

$\diamond$

Pour amener les élèves sur le terrain de la recherche actuelle, il suffit de poser la question de la réciproque du lemme ou du théorème précédent. En fait, si l'on se base sur les résultats que fournit un logiciel tel que Mathematica ou Maple il est même très tentant d'affirmer :

Conjecture 1. Si  $n$  est un entier composé alors le numérateur de

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n-1}$$

n'est pas divisible par  $n$ .

ou d'une manière moins risquée :

Conjecture 2. Si  $n$  est un entier composé alors le numérateur de

<sup>2</sup> Illustrer le mécanisme général sous-jacent sur un ou des exemples particuliers.

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n-1}$$

n'est pas divisible par  $n^2$ .

Le plus petit contre-exemple que j'ai obtenu à la conjecture 1 est 283'686'649, qui n'est autre que le carré du nombre premier  $p=16843$ . Ce dernier a été identifié lors de la recherche de nombres premiers irréguliers (Johnson 1975). Une propriété qui le caractérise est qu'il est le plus petit nombre premier qui divise le numérateur du nombre de Bernoulli  $B_{p-3}$ . Le lien avec les sommes harmoniques a été explicité par Gardiner (1988). En revanche, je n'ai aucune idée s'il existe un plus petit contre-exemple.

Concernant la deuxième conjecture, après avoir passé plusieurs semaines à m'échiner dessus, je me suis permis d'envoyer un e-mail au Prof. Richard Guy, en lui demandant son avis sur la question. Moins de trois jours après il me répondait : « I'd like to know the answers myself ! » tout en transférant mon message à Richard McIntosh, autre grand spécialiste en la matière. Ce dernier m'a surtout souhaité bien du courage à poursuivre l'exploration, en me signalant les derniers articles parus à ce sujet.

### Références

Gardiner A. (1988). Four problems on prime power divisibility, *Amer. Math. Monthly* 95, no. 10, 926–931.

McIntosh, R. J. (1995). On the converse of Wolstenholme's theorem, *Acta Arithmetica* 71 (4): 381-389

Johnson W. (1975). Irregular Primes and Cyclotomic Invariants, *Mathematics of Computation*, Vol. 29, Number 129, (1975), 113–120