Somme de deux carrés

(suite)

La primalité de 1 000 009

Léonhard EULER
(Utrum hic numerus 1000009 sit primus nec ne inquiritur
Nova Acta Academiae Scientarum Imperialis Petropolitinae 1797)

Tristan DERAY, Lycée Hilaire de Chardonnet, Chalon-sur-Saône

Comme le nombre est d'évidence somme de deux carrés ; à savoir 1000^2+3^2*, la question est donc de savoir s'il peut être décomposé en deux carrés de plus d'une façon* (voir le début de l'article dans la Feuille de Vigne n° 101, pages 15 à 19). *En effet, s'il ne peut l'être, il sera possible d'affirmer que le nombre est premier, par contre s'il existe une autre décomposition, il ne sera pas premier, et il sera alors possible de déterminer ses diviseurs. Si l'on considère le carré* x^2*, il faut donc rechercher s'il existe un autre carré, à savoir 1 000 009 -* x^2*, en dehors des cas* $x=3$ *et* $x=1000$*. Nous le ferons de la manière suivante :*

Si le carré choisi se termine par 9, l'autre carré doit nécessairement être divisible par 5, et même en réalité par 25. Par conséquent l'expression $1000009-x^2$ *doit être divisible par 25, et il est évident que l'on doit avoir* $x=25a+3$ *; on a alors l'expression* $1000000-6\times25a-25^2a^2$ *qui divisée par 25 donne* $40000-6a-25a^2$*, qui doit lui–même être également un carré.*

À ce stade deux cas peuvent être envisagés. Selon que a *est un nombre pair ou un nombre impair. Dans le premier cas, si* $a=2b$ *et en divisant par 4, l'expression qui en résulte doit également être un carré :* $A=10000-3b-25b^2$.
Dans l'autre cas, en prenant $a=4c+1$*, on est conduit à l'expression elle-même carrée d'un entier :* $B=39969-224c-400c^2$ *qui peut effectivement être un carré impair ; par ailleurs, si l'on prend, dans ce cas toujours,* $a=4d-1$*, la formule qui s'en déduit est* $C=39981+176d-400d^2$ *qui divisée par 8 donne pour reste 5 et qui ne peut en aucun cas être un carré. Nous devons donc étudier les deux expressions A et B.*

Décomposition de $B=39969-224c-400c^2$

Donnons ici à la lettre c successivement toutes les valeurs positives et négatives 0, 1, 2, 3, … et puisque l'expression $400c^2\pm224c$ *est soustraite de la valeur 39969 pour les différentes valeurs positives ou négatives de c, notons les différents nombres devant être soustraits dans deux colonnes et les différences successives entre ceux–ci.*

c	$400c^2-224c$	*Différence*	*c*	$400c^2+224c$	*Différence*
0	*0*		*0*	*0*	
1	*176*	*176*	*1*	*624*	*624*
2	*1152*	*976*	*2*	*2048*	*1424*
3	*2928*	*1776*	*3*	*4272*	*2224*
4	*5504*	*2576*	*4*	*7296*	*3024*

Il est évident d'après ce tableau que les différences augmentent, dans les deux cas, de 800.

Ces différences sont alors continuellement soustraites d'un nombre donné 39 969 ; par commodité on le fera sur deux colonnes ; de sorte que l'on pourra voir si le nombre résultant est un carré.

39969 176	*39969 624*
39793 976	*39345 1424*
38817 1776	*37921 2224*
37041 2576	*35697 3024*
34465 3376	*32673 3824*
31089 4176	*28849 4624*
26913 4976	*24225 5424*
21937 5776	*18801 6224*
16161 6576	*12577 7024*
9585 7376	*5553*
*2209**	

Parmi tous ces nombres, le seul carré qui apparaît est $2209 = 47^2$. *De là, on peut en déduire que le nombre proposé n'est pas premier mais possède des diviseurs, même s'il apparaît dans l'étude « table de nombres premiers jusqu'à un million et au-delà »* (Euler avait publié une étude conduisant à une table des nombres premiers inférieurs à 1 000 000). *Pour trouver ses diviseurs, il faut remarquer que ce carré est engendré par la valeur* $c = -10$ *; d'où l'on déduit celle de* $a = -39$ *; et évidemment celle de* $x = 25a + 3 = -972$ *; on a alors :* $1000009 - x^2 = 55225 = 235^2$.

Par conséquent, nous avons les deux décompositions $1000^2 + 3^2 = 972^2 + 235^2$ *; d'où* $1000^2 - 235^2 = 972^2 - 3^2$ *; d'où il résulte* $(1000 - 235)(1000 + 235) = (972 - 3)(972 + 3)$ *; c'est-à-dire* $1235 \times 765 = 969 \times 975$.

On a alors $\frac{1235}{975} = \frac{969}{765}$. *En simplifiant, il vient alors* $\frac{19}{15}$, *et alors il est possible de conclure que le nombre étudié possède un diviseur commun avec la somme des carrés* $19^2 + 15^2$, *à savoir 293. En fait, on trouvera que* $1000009 = 293 \cdot 3413$.

Il apparaît ainsi qu'une erreur avait été faite dans la table mentionnée précédemment, dans laquelle tous les nombres premiers entre 1000000 et 1002000 sont donnés, sans doute la raison de l'erreur est–elle que le diviseur 293 avait été oublié.

Décomposition de $A = 10000 - 3b - 25b^2$

Cette expression vaut le centième de $1000009 - x^2$, *et deux cas doivent être distingués dans l'étude de sa décomposition selon que b est un nombre pair ou impair. Dans le premier cas, il est évident que si b n'est pas lui–même "pairement pair" (c'est-à-dire de la forme* $2k$, *avec* k *pair) l'expression donnée ne peut pas être un carré. Il faut donc avoir* $b = 4c$ *; et l'expression qui vient après divisée par 4 est* $2500 - 3c - 100c^2$ *; et il n'est pas difficile de voir qu'il ne s'agit jamais d'un carré, sauf dans le cas où*

$c=0$. *Tout d'abord, il est clair que ce ne sera pas un carré si* $c=\pm 1$, *et de manière analogue, ce ne sera pas un carré si* $c=\pm 2$. *Pour* $c=\pm 3$, *notre expression donne* $2500-900\pm 9=1600\pm 9$ *; qui ne peut être un carré. De plus, si l'on suppose que* $c=\pm 4$, *on aura* $2500-1600\pm 12=900\pm 12$ *qui ne sera certainement pas un carré. Si l'on prend* $c=\pm 5$ *; on s'aperçoit vite qu'il ne s'agit pas d'un carré, car on obtient* $2500-2500\pm 15=0\pm 15$.

Dans le second cas, pour lequel b est un nombre impair, on prend tout d'abord $b=4d+1$ *; l'expression qui en résulte est* $9972-212d-400d^2$, *qui divisée par 4 donne* $2493-53d-100d^2$ *qui dans le cas* $d=0$ *; n'est d'évidence pas un carré. Si l'on prend ensuite* $d=\pm 1$ *qui donne* 2393 ± 53 *; on n'obtient pas de carré. Dans le cas* $d=\pm 2$, *il vient* 2093 ± 106. *Dans le cas* $d=\pm 3$, *il vient* 1593 ± 159 *; et aucun carré n'apparaît ; ni dans le cas* $d=\pm 4$ *; qui donne* 893 ± 212. *Dans le cas* $d=-5$, *il vient* $-7+265$. *Pour un nombre de la forme* $4d-1$, *on obtient* $9978+188d-400d^2$ *qui doit être un nombre pair ; mais comme il n'est pas divisible par 4, il ne peut donc être un carré.*

Suivant cette méthode, avec les nombreux calculs qui ont été faits, nous nous proposons d'examiner un autre nombre qui peut s'écrire comme somme de deux carrés, à savoir $1000081=1000^2+9^2$ *et nous cherchons à savoir s'il peut être décomposé en somme de deux carrés d'une autre manière. Comme dans le cas précédent, l'un ou l'autre de ces carrés doit être divisible par 5. Par conséquent l'un est posé égal à* x^2 *; et nous voyons que la différence* $1000081-x^2$ *doit être un carré divisible par 5 ou par 25.*

Posons $x=25y+9$, *ce qui mène à l'expression* $1000000-18\times 25y-25y^2$ *qui, une fois divisée par 25, donne* $40000-18y-25y^2$. *Si* y *est pair, alors il s'écrit* $y=2a$ *; en divisant à nouveau l'expression par 4, il vient :* $A=10000-9a-25a^2$. *Si* y *est impair ; il peut s'écrire soit* $y=4b+1$ *qui conduit à l'expression* $B=39957-272b-400b^2$ *qui est un nombre impair et donne alors un reste égal à 5 si on le divise par 8, elle ne peut donc pas être un carré, par conséquent la formule qui donne B est à laisser. Soit* y *est impair ; et peut encore s'écrire* $y=4c-1$, *l'expression à laquelle on arrive dans ce cas est* $B=39993+128c-400c^2$ *; le nombre 39993 donne pour reste 1 quand on le divise par 8 ; examinons ce cas maintenant.*

Décomposition de $C=39993+128c-400c^2$

Il est évident que les nombres de la forme $400c^2\pm 128c$ *doivent être retranchés du nombre 39993 ; et ces calculs sont simplifiés comme dans le cas précédent en prenant les différences entre les autres nombres ; pour les valeurs positives ou négatives de* c. *On les consigne dans le tableau suivant :*

c	$400c^2-128c$	*différence*	c	$400c^2+128c$	*différence*
0	*0*		*0*	*0*	
1	*272*	*272*	*1*	*528*	*528*
2	*1344*	*1072*	*2*	*1856*	*1328*
3	*3216*	*1872*	*3*	*3984*	*2128*

Par conséquent nous soustrayons ces différences, qui vont en croissant de 800, du nombre donné 39993. Le calcul nous donne :

39993	*39993*
272	*528*
39721	*39465*
1072	*1328*
38649	*38137*
1872	*2128*
36777	*36009*
2672	*2928*
34105	*33081*
3472	*3728*
30633	*29353*
4272	*4528*
26361	*24825*
5072	*5328*
21289	*19497*
5872	*6128*
15417	*13369*
6672	*6928*
8745	*6441*
7472	
1273	

Il est clair qu'aucun carré n'apparaît ici.

Décomposition de $A = 10000 - 9a - 25a^2$

A la place de a*, on introduit un nombre pair tel que* $a = 4e$ *; de sorte qu'en divisant l'expression par 4, nous obtiendrons* $2500 - 9e - 100e^2$*. Ainsi, les nombres de la forme* $100e^2 \pm 9e$ *devront être soustraits du nombre donné (2500) ; comme l'indique la table suivante ; dans laquelle le nombre* e *peut être soit positif soit négatif.*

e	$100e^2 - 9e$	*différence*	$100e^2 + 9e$	*différence*
0	*0*		*0*	
1	*91*	*91*	*109*	*109*
2	*382*	*291*	*418*	*309*
3	*873*	*491*	*927*	*509*

Ensuite nous devrons soustraire ces différences, qui vont croissantes de 200, du nombre donné 2500, de la manière suivante :

2500	*2500*
91	*109*
2409	*2391*
291	*309*
2118	*2082*
491	*509*
1627	*1573*
691	*709*
936	*864*
891	
45	

Aucun carré n'apparaît ; hormis 2500, qui conduit à un carré au delà de 1000^2.

Maintenant si a *est un nombre impair, tout d'abord de la forme* $4f+1$*, notre formule deviendra* $9966-236f-4f^2$*, qui n'est pas un multiple de quatre et ne peut donc être un carré. Si nous posons* $a=4f-1$*, l'expression obtenue est* $9984+164f-400f^2$ *qui est un multiple de quatre, et qui divisée par quatre donne* $2496+41f-100f^2$*. Les nombres de la forme* $100f^2\pm 41f$ *sont alors soustraits du nombre donné, et pour* f *positif ou négatif, on aura :*

f	$100f^2-41f$	*différence*	f	$100f^2+41f$	*différence*
0	*0*		*0*	*0*	
1	*59*	*59*	*1*	*141*	*141*
2	*318*	*259*	*2*	*482*	*541*
3	*777*	*459*	*3*	*3984*	*541*

Les différences sont ensuite nécessairement soustraites du nombre donné :

2496 *59*	*2496* *141*
2437 *259*	*2355* *341*
2178 *459*	*2014* *541*
1719 *659*	*1473* *741*
1060 *859*	*732*
201	

Comme dans tous ces calculs, aucun carré ne ressort ; il est certain que le nombre 1000081 ne peut être décomposé en carré que d'une unique manière, et est donc un nombre premier. Il est indiqué dans la table citée précédemment, et il est à remarquer la grande facilité des calculs par lesquels il a été possible d'établir la propriété.

Cependant, il est regrettable que cette méthode ne puisse pas être utilisée pour n'importe quel nombre ; mais est limitée aux nombres qui non seulement sont somme de deux carrés, mais qui se terminent par 1 ou 9 ; puisque alors l'autre carré sera divisible par 5.

Toutefois, il est clair que tous les nombres de la forme $4n+1$ *se terminant soit par 1, soit par 9 se prêtent parfaitement à cette méthode de recherche ; si nous savons qu'un tel nombre peut être décomposé en somme de deux carrés, l'un d'eux est nécessairement divisible par 5. En suivant alors la méthode décrite précédemment, si l'on montre que le nombre donné ne se laisse décomposer en somme de deux carrés que d'une seule façon, alors on pourra affirmer qu'il est premier ; mais si par contre il peut être décomposé en somme de deux carrés de diverses façons, il sera alors possible d'en trouver des diviseurs comme il a été vu plus haut. Cependant, s'il apparaît que le nombre donné ne peut pas être décomposé en somme de deux carrés, alors c'est une preuve qu'il n'est pas premier, même si ses facteurs ne peuvent être déterminés, et l'on peut conclure qu'il admet au moins deux diviseurs, dont l'un est de la forme* $4n-1$.

Si un nombre impair est de la forme $4n+1$, il admet toujours une décomposition en somme de deux carrés.

- Si cette décomposition est unique, il est premier.
- S'il existe plusieurs décompositions, il est composé (et l'on sait trouver des diviseurs grâce à la décomposition en somme de deux carrés)

Si un nombre impair est de la forme $4n-1$, et s'il n'admet pas de décomposition en somme de carrés, alors il est composé (même si l'on ne sait pas a priori trouver de diviseurs).

Comme Fermat ne s'était pas arrêté au problème de la représentation d'un entier en somme de deux carrés, mais s'était encore intéressé aux nombres du type x^2+3y^2 ; Euler reprit à son compte ces recherches sur la représentation de nombres par des « formules » X^2+NY^2 (ou plus généralement sous la forme mx^2+ny^2) posant la question de savoir quels sont les nombres premiers admettant une représentation sous la forme a^2+Nb^2 (*a* et *b* entiers) et plus généralement encore sur les valeurs entières pour lesquelles l'unicité de la représentation d'un entier premier avec $N=mn$, entraînait sa primalité.

En 1778, il écrivait à son collègue Béguelin de l'Académie de Berlin dont les travaux portaient sur la représentation des entiers comme somme de deux carrés :

« *… j'ai remarqué que plusieurs autres formules semblables de la forme* nx^2+y^2 *sont douées de la même propriété, & que, pourvu qu'on donne à la lettre n des valeurs convenables, telles que, par exemple 2, 3, 4, 5 , 6, 7, 8, 9, 10, 12, 13 &c. on en tire toujours des nombres premiers ; ou bien, qu'à l'exclusion des valeurs suivantes de n 11, 14, 17, 19, 20, 23, 26, 27 &c. La formule* nx^2+y^2 *donne toujours des nombres premiers ; car le nombre 15 par exemple quoique contenu d'une seule façon dans la formule* $11x^2+y^2$*, est un nombre composé. Il en est ainsi des autres nombres que je viens d'exclure ; au lieu que ceux que j'ai nommé valeurs convenables, donnent sûrement pour premier, tout nombre qui est contenu d'une seule façon dans la forme* nx^2+y^2*…* »

Il proposait alors une liste de 65 nombres entiers dits idoines répondant à la question.

Au soir de sa vie, Euler ne se contentait pas d'avoir découvert un nouveau continent, il y avait pris pied et invitait ses successeurs à poursuivre son oeuvre. Le fin sillon tracé par Fermat, devenait sous le labeur d'Euler un champ fertile dans lequel le jeune Lagrange allait faire une riche moisson, et ce dernier ne se méprenait pas recevant le legs, il écrivait au vieux mathématicien de Saint-Pétersbourg : « Il me semble qu'il n'y ait que Fermat et vous qui vous soient occupés avec succès de ces sortes de recherches, et si j'ai été assez heureux pour ajouter quelque chose à vos découvertes, je ne le dois qu'à l'étude que j'ai faite de vos excellents ouvrages. » Peu avant d'écrire ces lignes, Lagrange avait publié un mémoire *« Recherches Arithmétiques* » dans les Annales de l'Académie de Berlin (1773) ayant « …pour objet les nombres qui peuvent être représentés par la formule $Bt^2+Ctu+Du^2\ldots$ » Il donnait alors un cadre général aux nombreuses recherches d'Euler, celui de l'étude des formes quadratiques binaires que Gauss viendrait parachever avec l'excellence qui s'attache à son nom dans ses *Recherches Arithmétiques*.

…
Un trésor est caché dedans.
Je ne sais pas l'endroit ; mais un peu de courage
Vous le fera trouver : vous en viendrez à bout.
Remuez votre champ dès qu'on aura fait l'oût :
Creusez, fouillez, bêchez; ne laissez nulle place
Où la main ne passe et repasse.»