ACTIVITÉ AUTOUR DES «IDENTITÉS REMARQUABLES» ET FACTORISATION DES ENTIERS: LA MÉTHODE DE FERMAT

Christian Aebi et John Steinig

Une collaboration entre un enseignant du Cycle d'orientation de Genève et un professeur de l'Université de Genève.

Fragment d'une lettre de Fermat

(Œuvres Complètes, éd.Tannery et Henry, tome 2, 1894, lettre de 1643, pp. 257-258)

Tout nombre impair non quarré est différent d'un quarré par un quarré, ou est la différence de deux quarrés, autant de fois qu'il est composé de deux nombres, et, si les quarrés sont premiers entre eux, les nombres compositeurs le sont aussi. Mais si les quarrés ont entre eux un commun diviseur, le nombre en question sera aussi divisible par le même commun diviseur, et les nombres compositeurs seront divisibles par le côté de ce commun diviseur.

Par exemple: 45 est composé de 5 et de 9, de 3 et de 15, de 1 et de 45. Partant, il sera trois fois la différence de deux quarrés: savoir de 4 et de 49, qui sont premiers entre eux, comme aussi sont les compositeurs correspondants 5 et 9; plus, de 36 et de 81, qui ont 9 pour commun diviseur, et les compositeurs correspondants, 3 et 15, ont le côté de 9, savoir 3, pour commun diviseur; enfin 45 est la différence de 484 et 529, qui ont 1 et 45 pour compositeurs correspondants.

Il est fort aisé de trouver les quarrés satisfaisants, quand on a le nombre et ses parties, et d'avoir les parties lorsqu'on a les quarrés. Cette proposition se trouve quasi tout par tout. On en pourrait quasi autant dire des pairements pairs, excepté 4, avec quelque petite modification.

Cela posé, qu'un nombre me soit donné, par exemple 2 027 651 281, on demande s'il est premier ou composé, et de quels nombres il est composé, au cas qu'il le soit. J'extrais la racine, pour connoître le moindre des dits nombres, et trouve 45 029 avec 40 440 de reste, lequel j'ôte du double plus 1 de la racine trouvée, savoir de 90 059: reste 49 619, lequel n'est pas quarré, parce que aucun quarré ne finit par 19, et partant je lui ajoute 90 061, savoir 2 plus que 90 059 qui est le double plus 1 de la racine 45029. Et parce que la somme 139 680 n'est pas encore quarrée, comme on le voit par les finales, je lui ajoute encore le même nombre augmenté de 2, savoir 90 063, et je continue ainsi d'ajouter tant que la somme soit un quarré, comme on peut voir ici. Ce qui n'arrive qu'à 1 040 400, qui est quarré de 1020, et partant le nombre donné est composé; car il est aisé, par l'inspection des dites sommes, de voir qu'il n'y a aucune qui soit nombre quarré que la dernière, car les quarrés ne peuvent souffrir les finales qu'elles ont, si ce n'est 499 944 qui néanmoins n'est pas quarré. Pour savoir maintenant les nombres qui composent 2 027 651 281, j'ôte le nombre que j'ai premièrement ajouté, savoir 90 061, du dernier ajouté 90 081. Il reste 20, à la moitié duquel plus 2, savoir à 12, j'ajoute la racine premièrement trouvée 45 029. La somme est 45 041, auquel nombre ajoutant et ôtant 1020, racine de la dernière somme 1 040 400, on aura 46 061 et 44 021, qui sont les deux nombres plus prochains qui composent 2 027 651 281. Ce sont aussi les seuls, pource que l'un et l'autre sont premiers.

Si l'on alloit par la voie ordinaire, pour trouver la composition d'un tel nombre, au lieu de onze additions, il eût fallu diviser par tous les nombres depuis 7 jusqu'à 44 021.

Activité autour des «identités remarquables»

L'activité décrite ci-dessous n'est ni une activité d'introduction, ni une activité de synthèse. Elle permet, avant tout, à chaque élève d'observer des «phénomènes numériques», d'essayer de les traduire dans un langage symbolique et d'exploiter les règles du calcul littéral pour les justifier. En outre, elle vise à donner du sens à l'introduction de l'écriture littérale et du calcul algébrique, tout particulièrement des identités remarquables, dans le but de prouver des affirmations universelles.

Énoncé:

Quels sont les entiers positifs pouvant s'écrire sous la forme d'une différence de deux carrés?

(Extrait du livre de John Mason, *L'esprit mathématique*, De Boeck Université 1994.)

Le problème a été testé à trois reprises: la première fois avec des gymnasiens genevois de première année en 1998 comme cours d'introduction. Quelle déception de constater leur difficulté d'entrer dans le problème, de l'explorer, d'avancer des conjectures et d'ébaucher des preuves. Aucune commune mesure lors de son deuxième passage dans une classe du cycle d'orientation de Genève de 9e Générale, en décembre 2000, puis dans une 9e A (classique/scientifique), en octobre 2003.

Ci-dessous est décrit en grande partie le déroulement de la séance en 9e G, avec en guise de conclusion l'argumentation développée par une élève de 9e A pour démontrer la troisième conjecture.

Comme il se doit, la première phase consiste à laisser les élèves prendre connaissance de l'énoncé, et surtout à fabriquer des exemples. Après deux minutes il n'est pas inutile de les interrompre et de faire rappeler par l'un d'eux ce qu'est une *différence*, ou un *carré*.

La première mise en commun des résultats se fait généralement de manière désordonnée:

$$5=3^2-2^2 \quad ; \quad 7=4^2-3^2 \quad ; \quad 12=4^2-2^2 \quad ; \quad 9=5^2-4^2.$$

Les exemples triviaux apparaissent ensuite: $1=1^2-0^2$; $4=2^2-0^2$; $9=3^2-0^2$.

Récapituler les résultats dans un tableau permet de clarifier légèrement:

$0=0^2-0^2$	$1=1^2-0^2$	$2=?$	$3=2^2-1^2$	$4=2^2-0^2$	$5=3^2-2^2$	$6=?$	$7=4^2-3^2$

Mais c'est surtout de faire construire la liste des carrés inférieurs à 100 qui permet aux élèves de déterminer plus rapidement les nombres *constructibles*, c'est-à-dire différence de deux carrés.

Comment justifier que 2 n'est pas constructible? et 6? La réponse naïve des élèves consiste à rétorquer «On a tout essayé!» L'argumentation est insuffisante, mais à ce stade de l'activité, tant qu'une conjecture n'émane pas de leur part, je conseillerais de les laisser poursuivre à compléter le tableau des nombres constructibles:

0	1	✗	3	4	5	✗	7	8
9	✗	11	12	13	✗	15	16	17
✗	19	20	21	✗	23	24	25	✗

Ce tableau récapitulatif permet de faire émerger généralement plusieurs conjectures que j'ai pris l'habitude de dénommer par le nom de l'auteur.

Conjecture Hedi: «La distance entre les nombres qu'on ne peut pas construire est de 4.»
Conjecture Malik: «Tous les impairs sont constructibles! Et je sais comment les obtenir!»

Démonstration de Malik par induction (au sens non mathématique):
«J'ai observé que dans les expressions

$$3=2^2-1^2 \;;\; 5=3^2-2^2 \;;\; 7=4^2-3^2 \;;\; 9=5^2-4^2 \;;\; 11=6^2-5^2 \qquad (*)$$

on voit que $2+1=3$; $3+2=5$; $4+3=7$ etc.»
Prof.: «Alors peux-tu nous prouver que 27 est constructible?»
Malik: «Ouais! Il suffit de prendre 14 et 13. Faites le calcul vous-même, ça marche!»

Remarque: Malgré l'étude des identités remarquables pendant les deux semaines précédentes, la première vérification se fait péniblement en calculant. Ce n'est qu'après avoir insisté lourdement sur le fait que *«nous sommes en présence d'une différence de la forme a^2–b^2»* qu'enfin une élève signale que

$$14^2-13^2=(14+13)(14-13)=27\cdot 1=27.$$

Ce déblocage jette un nouvel éclairage sur les égalités (*).
Prof. (toujours insatisfait): «Mais moi, j'aimerais une *formule générale* pour un *nombre impair quelconque*. Si l'on décrète que la forme générale d'un nombre pair est $2\cdot m$ alors un impair s'écrit comment?» «2·m+1». «D'accord!»
«Quelle sera alors la formule?»

$$2m+1=?^2-??^2$$

Après quelques dizaines de secondes un élève se jette à l'eau.
Au bout de deux, trois tentatives infructueuses on voit enfin apparaître $\boxed{2m+1=(m+1)^2-m^2}$
Deux démonstrations sont proposées:

1) $(m+1)^2-m^2=(m^2+2m+1)-m^2=2m+1$ par l'une des identités remarquables vue en classe,

2) $(m+1)^2-m^2=((m+1)-m)\cdot((m+1)+m)=2m+1$ par une autre identité remarquable.

Et la conjecture Hedi? Elle est reformulée ainsi: «Aucun entier de la forme $4m+2$ n'est constructible.» Mise de côté momentanément, nous attaquons les entiers de la forme $4m$.
Observons!

$$4=2^2-0^2 \;;\; 8=3^2-1^2 \;;\; 12=4^2-2^2 \;;\; 16=4^2-0^2=5^2-3^2.$$

Voyant que les élèves ne comprennent pas ce qui ce cache derrière ces identités, je les mets alors sous la forme suivante:

$$4\cdot 1=2^2-0^2 \;;\; 4\cdot 2=3^2-1^2 \;;\; 4\cdot 3=4^2-2^2 \;;\; 4\cdot 4=5^2-3^2.$$

Sous cette forme, les élèves parviennent à obtenir la formule $\boxed{4m=(m+1)^2-(m-1)^2}$
Une fois de plus, deux démonstrations sont proposées:

1) $(m+1)^2-(m-1)^2=(m^2+2m+1)-(m^2-2m+1)=4m$, et

2) $(m+1)^2-(m-1)^2=((m+1)-(m-1))\cdot((m+1)+(m-1))=4m$.

Démonstration de Jessica (9e A) de la dernière conjecture: aucun entier de la forme $4m+2$ n'est constructible. «Imaginons deux entiers a et b sur une droite avec $a<b$. Deux situations peuvent se produire: soit la distance entre a et b est paire, soit elle est impaire,
c'est-à-dire $b=a+2m$ ou $b=a+2m+1$. En calculant la différence de leurs carrés on obtient:
$b^2-a^2=(a+2m)^2-a^2=4am+4m^2=4\cdot(am+m^2)$, un multiple de 4, ou
$b^2-a^2=(a+2m+1)^2-a^2=(2m+1)\cdot(2(a+m)+1)=2\cdot(2am+2m^2+2m+a)+1$, un nombre impair.
Il est donc impossible d'obtenir un multiple de 4, plus 2.»

Une suite à donner à cette activité est proposée par l'exercice ci-dessous qui montre, à nouveau, une utilisation des identités remarquables.

Exercice (La première partie peut aisément se faire oralement.)

a) Décompose en produit de facteurs premiers les entiers ci-dessous en t'inspirant de l'exemple et en utilisant la liste des carrés 1 ; 4 ; 9 ; 16 ; 25... 121 ; 144 ; 196 ; 225 ; 256 ; 289 ; 324 ; 361 ; 400... 10'000

Exemple:

$$143 = 144 - 1 = 12^2 - 1^2 = (12-1)(12+1) = 11 \cdot 13$$

1) 399	2) 221	3) 391
4) 117	5) 9991	6) 9919

b) De combien de façons différentes peut-on écrire un nombre premier impair sous la forme d'une différence de deux carrés ?

c) Vérifie l'identité suivante, $(a^2 - b^2) \cdot (c^2 - d^2) = (ac - bd)^2 - (ad - bc)^2$ qui entre autres, signifie que «*le produit de deux entiers s'écrivant sous la forme d'une différence de deux carrés est encore une différence de deux carrés*».

d) De combien de façons différentes peut-on écrire 105 sous la forme d'une différence de 2 carrés ?

De tels problèmes de recherche ne doivent pas laisser croire que des exercices d'entraînement touchant au développement et à la factorisation d'expressions polynomiales sont à éviter : chaque enseignant a cette délicate tâche d'équilibrer au mieux les exercices de « drill » et de « découverte ». Ce qui nous importait prioritairement était d'essayer de montrer en quoi des questions élémentaires d'arithmétique peuvent servir de levier à l'exploration du monde algébrique. Nous pensons comme G. H. Hardy que : « La théorie élémentaire des nombres doit être la discipline la mieux adaptée à un enseignement primaire des mathématiques. Elle ne requiert que très peu de connaissances préalables, et le sujet de son étude est concret et familier ; les méthodes de raisonnement employées sont simples, générales et peu nombreuses ; et elle est unique parmi les diverses branches des mathématiques pour la curiosité humaine qu'elle suscite.» (Bull. Amer. Math. Soc. 35 (1929) p. 818)

Les différences de deux carrés : un commentaire historique

L'activité proposée aux élèves de 9e, «Quels sont les entiers positifs qu'on peut écrire comme la différence de deux carrés ? », est plus qu'un simple passe-temps.

Elle est liée à une des préoccupations principales de la théorie des nombres : comment reconnaître, d'un entier positif donné, s'il est premier ou composé ; et comment l'écrire comme produit de nombres premiers, s'il est composé.

En 1643, le R.P. Mersenne mit Fermat au défi de décider, «dans l'espace d'un jour», si l'entier 100 895 598 169 est premier ou non.

Fermat lui répondit le 7 avril 1643 que «(...) ce nombre est composé et se fait du produit de ces deux : 898 423 et 112 303, qui sont premiers».

La méthode inventée par Fermat pour factoriser de grands entiers est détaillée dans une autre de ses lettres, qui n'a survécu qu'à l'état de fragment, recopié de l'original. La date ni le destinataire n'en sont connus ; on suppose qu'elle aurait pu être écrite en 1643, à Mersenne ou à Frenicle. Cette méthode est fondée sur l'identité.

$$x^2 - y^2 = (x-y)(x+y).$$

Une des découvertes des élèves de 9e est que tout entier impair peut s'écrire sous la forme $x^2 - y^2$, avec x et y entiers ; ce qui implique que la méthode de Fermat permet de décider,

au sujet de n'importe quel entier positif impair, «s'il est premier ou composé, et de quels nombres il est composé, au cas qu'il le soit».

On trouvera ci-dessous un exposé de la méthode de Fermat et quelques énoncés de problèmes suggérés par son procédé.

Factorisation d'entiers: la méthode de Fermat

Supposons qu'on veuille savoir si un certain entier $n>1$ est premier ou composé; et s'il est composé, qu'on veuille le décomposer en produit de facteurs premiers. On peut se limiter au cas où n est impair (dans le cas d'un entier pair, on a immédiatement un facteur premier; et les entiers pairs se reconnaissent au premier coup d'oeil). Si n est composé, il admet un facteur premier $p \le \sqrt{n}$. On pourrait donc essayer de diviser n par chacun des nombres premiers $p \le \sqrt{n}$. Si une des divisions se fait sans reste, alors n est composé et on en connaît un facteur premier. Sinon, n est premier.

C'est une méthode peu pratique. Si n a 31 chiffres en base 10 (c'est-à-dire, si $10^{30} \le n < 10^{31}$), le nombre de divisions (dans le cas le moins favorable) est supérieur au nombre de nombres premiers de l'intervalle $(1, 10^{15})$. Il y a environ $29844 \cdot 10^9$ nombres premiers $p < 10^{15}$. Un ordinateur qui ferait 10^9 divisions par seconde mettrait plus de 29844 secondes (plus de 8 heures) pour les effectuer toutes.

La méthode de Fermat, décrite dans une lettre (peut-être envoyée en 1643 à Mersenne), repose sur l'identité $x^2 - y^2 = (x-y)(x+y)$. Elle permet de déterminer si n est premier ou composé; s'il est composé, elle en livre un diviseur d non-trivial $(1 < d < n)$.

Soit $n > 1$, impair. Si on écrit n comme produit de deux entiers positifs (impairs), disons

$n = ab$, avec $a \ge b \ge 1$ (a et b impairs),

alors

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2,$$

avec $\frac{a \pm b}{2}$ entiers et $\frac{a+b}{2} > \frac{a-b}{2} \ge 0$;

toute factorisation de n livre une écriture $n = x^2 - y^2$ avec $x > y \ge 0$, entiers. Un entier impair positif composé peut s'écrire de plusieurs manières distinctes comme le produit de deux entiers positifs; il peut donc s'écrire de plusieurs manières distinctes comme la différence de deux carrés d'entiers non-négatifs. Autrement dit, un entier impair supérieur à 1, qui s'écrit d'une seule manière comme la différence de deux carrés d'entiers non-négatifs, est un nombre premier.

Et si $n = x^2 - y^2$ avec des entiers $x > y \ge 0$, alors $\sqrt{n} \le x \le \frac{1}{2}(n+1)$. En effet, on a d'une part $n = x^2 - y^2 \le x^2$; d'autre part, $n = x^2 - y^2 \ge x^2 - (x-1)^2 = 2x - 1$.

D'où la méthode: on prend le plus petit entier t tel que $t \ge \sqrt{n}$, puis on calcule $x^2 - n$ pour $x = t,\ t+1,\ t+2, \ldots$ pour voir si on obtient un carré. Le cas le plus favorable se présente si n est un carré d'entier; on aura alors $t^2 - n = 0$. Sinon, on obtient un carré au plus tard pour $x = \frac{1}{2}(n+1)$, puisque

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2;$$

mais ceci ne livre que la factorisation triviale

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = n \cdot 1.$$

Si n est composé on trouvera un entier $x < \frac{1}{2}(n+1)$ pour lequel $x^2 - n$ est un carré, disons $x^2 - n = y^2$, et on pourra factoriser $n = (x-y)(x+y)$, avec $1 < x - y < n$.

Et si on n'obtient, par ces essais successifs, que la factorisation $n = n \cdot 1$, alors n est premier.

Fermat ajoute deux idées qui abrègent les calculs. La première est de construire une table de carrés en utilisant l'identité

$m^2 + (2m + 1) = (m + 1)^2$; il suffit de faire des additions, sans faire de multiplications (on fera ensuite $2m + 3 = (2m + 1) + 2$, etc.).

Ainsi, on commencera par calculer $t^2 - n$, puis on additionnera, successivement $2t + 1, 2t + 3, 2t + 5,\ldots$ pour calculer $(t + 1)^2 - n$, $(t + 2)^2 - n$, $(t + 3)^2 - n,\ldots$

La seconde idée est que le dernier chiffre d'un carré d'entier ne peut pas être 2, 3, 7 ou 8. De même, certaines paires d'entiers (par exemple 35) ne peuvent pas être les deux derniers chiffres («les finales», comme les appelle Fermat) d'un carré. Donc si $x^2 - n$ se termine d'une de ces manières, on passera de suite à $(x + 1)^2 - n$.

Dans le pire des cas, celui où n est premier et n'admet donc que la factorisation triviale $n = n\cdot 1$, on doit essayer tous les entiers de $x = t$ à $x = \frac{1}{2}(n+1)$, donc faire environ $\frac{1}{2}(n+1) - \sqrt{n}$ tentatives.

Par contre, la méthode aboutit rapidement si n admet une factorisation comme produit de deux entiers «proches» (car ces entiers sont alors proches de $\sqrt{n}$).

Fermat illustre sa méthode avec l'exemple $n = 2\,027\,651\,281$, qui est de ce dernier type.

Commençons les calculs pour cet exemple. Le plus petit entier $t \geq \sqrt{n}$ est $t = 45030$.

On a

$$\begin{array}{lcll}
t^2 - n & = & 49\,619 & \\
\underline{2t+1} & = & \underline{90\,061} & \\
(t+1)^2 - n & = & 139\,680 & \text{: n'est pas un carré (un carré ne se termine pas par 80)} \\
\underline{2t+3} & = & \underline{90\,063} & \\
(t+2)^2 - n & = & 229\,743 & \text{: n'est pas un carré (un carré ne se termine pas par 3)} \\
\underline{2t+5} & = & \underline{90\,065} & \\
(t+3)^2 - n & = & 319\,808 & \text{: n'est pas un carré (un carré ne se termine pas par 8)} \\
\ldots\ldots & & &
\end{array}$$

En continuant de cette manière on trouve $(t + 11)^2 - n = 1\,040\,400 = 1020^2$. Puisque $t + 11 = 45041$, on a $n = 45041^2 - 1020^2 = (45041 - 1020)(45041 + 1020)$, soit $n = 44021 \cdot 46061$.

La décomposition s'arrête sur ces deux diviseurs, «pource que l'un et l'autre sont premiers». Comme l'observe Fermat, il a suffi de faire 11 additions, au lieu d'essayer de diviser n par tous les nombres premiers jusqu'à $\sqrt{n}$, c'est-à-dire jusqu'à 44029.

La méthode de factorisation de Fermat : quelques problèmes

1. Quelles sont les paires d'entiers susceptibles d'être les deux derniers chiffres (en base 10) d'un carré d'entier?
2. (A faire «à la main», comme l'aurait fait Fermat.)

(a) L'entier 139 854 276 est-il un carré d'entier?
(b) L'entier 194 489 672 241 689 est-il la quatrième puissance d'un entier?

3. Employer la méthode de Fermat pour factoriser l'entier 119 143.
4. Quels entiers peut-on écrire d'une seule manière sous la forme $x^2 - y^2$, avec x et y entiers, $x \geq 0$ et $y \geq 0$?