Somme et produit

Daniel PERRIN

1 Le problème de l'APM

1.1 La question

Le problème abordé ici est posé dans le numéro 543 de *Au fil des maths* (problème 543-2) :

J'ai décidé de faire deviner l'âge de mes enfants à mes élèves en leur précisant qu'ils avaient entre 2 *et* 20 *ans. J'ai écrit sur un bout de papier la somme des deux âges et sur un autre leur produit. J'ai donné au hasard un papier à Sophie et l'autre à Germain :*

1) **Sophie** – *En tout cas, je suis sûre que j'ai la somme.*

2) **Germain** – *Merci pour le renseignement, mais j'hésite quand même entre plusieurs solutions.*

3) **Sophie** – *Dans ce cas, moi je la connais.*

4) **Germain** – *Alors moi aussi.*

Et vous ?

Appelons a et b les deux âges, avec $2 \leq a, b \leq 20$ et posons $s = a + b$ et $p = ab$. On a $4 \leq a + b \leq 40$ et $4 \leq p \leq 400$. Dans tout le problème on postule implicitement que toute personne (en particulier Sophie et Germain) entendant les assertions des protagonistes est apte à mener les raisonnements appropriés pour résoudre le problème et notamment ceux qui suivent.

1.2 Conséquences de la première assertion de Sophie

1.1 Lemme. *L'assertion 1) implique que le nombre que détient Sophie (et qui est s) est premier, supérieur ou égal à* 5 *et que les deux âges sont l'un pair et l'autre impair.*

Démonstration. Soit S le nombre détenu par Sophie. Comme elle est sûre d'avoir la somme on a $S \leq 40$ (sinon S serait le produit). Si S n'était pas premier on aurait $S = mn$ avec $m, n \geq 2$ et les nombres m et n seraient ≤ 20 (sinon S serait plus grand que 40). Sophie ne pourrait donc pas savoir que S n'est pas le produit des âges m et n. Il est clair alors que $S = s$ est ≥ 5, donc premier impair et cela impose que les âges ne sont pas de même parité.

1.3 Conséquences de la première assertion de Germain

Grâce à l'assertion de Sophie, Germain sait qu'il détient p et que s est premier ≥ 5. Le lemme 1.1 montre que $p = ab$ est pair et nous supposerons que a est pair et b impair. Cela conduit à la définition suivante :

1.2 Définition. *Soit p un entier positif.*

1) Une **décomposition convenable** *de p est une écriture $p = ab$ avec a pair, b impair, $2 \leq a, b \leq 20$ et $s = a + b$ premier.*

2) On dit que p est un **nombre de Germain** *s'il admet au moins deux décompositions convenables distinctes.*

(Puisque Germain ne peut conclure avec le p qu'il détient c'est qu'il y a plusieurs décompositions convenables possibles, donc que p est un nombre de Germain.)

Le lemme suivant permet de préciser p :

1.3 Lemme. *Soit p un nombre de Germain écrit sous la forme $p = 2^\alpha q$ avec $\alpha \geq 1$ et $q \geq 3$ impair et soit $p = ab$ une décomposition convenable de p.*

1) On a $a = 2^\alpha a'$ avec a' impair et $q = a'b$.

2) On a $\alpha \leq 2$.

3) Le nombre q n'est pas premier, ses facteurs premiers sont parmi $3, 5, 7$.

4) Le nombre q n'est pas une puissance de $3, 5$ ou 7 ; les nombres 5 et 7 sont à une puissance au plus un dans q ; le nombre 3 est au plus au carré.

5) Les nombres de Germain sont 30, 42, 60, 70 et 90.

Démonstration.

1) Comme b est impair, 2^α est premier avec b donc divise a. On a donc $a = 2^\alpha a'$ d'où $q = a'b$, de sorte que a' est impair.

2) Il est clair qu'on a $\alpha \leq 4$ car a est ≤ 20. Si α est ≥ 3, comme $a = 2^\alpha a'$ avec a' impair et $a \leq 20$ on a $a' = 1$, donc l'unique décomposition convenable de p est ab avec $a = 2^\alpha$, $b = q$. Ce n'est donc pas un nombre de Germain.

3) Si q était premier, comme $q = a'b$ avec $b \geq 2$, on aurait $q = b$ et la seule décomposition convenable serait $a = 2^\alpha$ et $b = q$, de sorte que p ne serait pas un nombre de Germain. Il reste à voir que q n'a pas de facteur premier > 10. Si r était un tel facteur, $q = rq'$ avec q' impair ≥ 3, l'unique décomposition convenable de p en ab serait $a = 2^\alpha q'$, $b = r$. En effet, si r n'est pas le seul facteur de a ou b, il est accompagné d'un entier $k \geq 2$ mais kr est > 20, donc exclu.

4) Si q est, par exemple, une puissance de 3, il n'y a pas d'autre solution convenable que $a = 2^\alpha$, $b = q$. En effet, tout autre solution aurait à la fois a et b multiples de 3, ce qui contredit le fait que la somme $s = a + b$ est un nombre premier. Si 5 ou 7 sont au moins au carré, ils ne peuvent être dans

le même facteur a ou b (qui serait alors ≥ 25), ils sont donc à la fois dans a et b ce qui contredit encore le fait que s est un nombre premier. L'argument est le même pour le facteur 3.

5) En définitive, on a $2^\alpha = 2$ ou 4 et q est un diviseur de $3^2 \times 5 \times 7$ contenant au moins deux nombres premiers, donc un des nombres 3×5, 3×7, 5×7, $3 \times 5 \times 7$, $3^2 \times 5$, $3^2 \times 7$ ou $3^2 \times 5 \times 7$. Le cas $q = 3^2 \times 5 \times 7 = 315$ est impossible car p serait plus grand que 400, le cas $3 \times 5 \times 7 = 105$ aussi car il imposerait $2^\alpha = 2$ et il n'y aurait qu'une solution convenable $a = 14$, $b = 15$. Enfin le cas $q = 3^2 \times 7$ est impossible car il donne les solutions $a = 14, b = 9, s = 23$ et $a = 18, b = 7, s = 25$ qui n'est pas premier. On a donc $q = 15, 21, 35$ ou 45. De plus, seul le cas $q = 15$ permet d'avoir $2^\alpha = 4$ (dans les autres cas il y a unicité de la solution, soit parce qu'il n'y a qu'un diviseur impair de q qui soit ≤ 20, soit dans le cas $q = 3^2 \times 5 = 45$, que seule la décomposition $a = 20$, $b = 9$ donne $s = 29$ premier, l'autre $a = 12$, $b = 15$ donnant $s = 27$).

1.4 Corollaire. *Pour chaque nombre p de Germain voici la liste des décompositions convenables $p = ab$ et les sommes $s = a + b$ correspondantes :*

$$p = 30, a = 2, b = 15, s = 17;\ p = 30, a = 6, b = 5, s = 11;\ p = 30, a = 10, b = 3, s = 13;$$

$$p = 42, a = 6, b = 7, s = 13;\ p = 42, a = 14, b = 3, s = 17;$$

$$p = 60, a = 4, b = 15, s = 19;\ p = 60, a = 12, b = 5, s = 17;\ p = 60, a = 20, b = 3, s = 23;$$

$$p = 70, a = 10, b = 7, s = 17;\ p = 70, a = 14, b = 5, s = 19;$$

$$p = 90, a = 10, b = 9, s = 19;\ p = 90, a = 18, b = 5, s = 23.$$

1.4 Conséquences de la deuxième assertion de Sophie

Sophie, qui a évidemment fait tous les calculs précédents de tête et ainsi a déterminé tous les nombres de Germain et leurs décompositions convenables, affirme qu'avec le s qu'elle connaît il n'y a plus d'ambiguïté. Or les s obtenus ci-dessus sont $11, 13, 17, 19$ et 23 et, hormis 11, tous correspondent à plusieurs p. On en déduit qu'elle détient le nombre $s = 11$ et Pierre le nombre $p = 30$ donc que les âges sont 5 et 6 ans.

On notera que la deuxième assertion de Germain ne nous apporte rien de plus : il connaît la solution, mais nous aussi !

2 Le problème classique

2.1 L'énoncé

Le problème classique sur ce même thème de la somme et du produit est un peu différent. En voici une version trouvée sur Internet :

Deux mathématiciens, Serge et Pierre, descendent l'escalier de l'immeuble où ils habitent. Leur concierge, qui rève de mettre en défaut ces esprits brillants, les attend.

– Tenez, dit-elle à Pierre en lui tendant un morceau de papier, j'ai écrit le produit de deux nombres entiers compris entre 2 et 100, saurez-vous les trouver ? Pour vous, j'ai écrit leur somme, continue-t-elle en tendant un second morceau de papier à Serge.

1) Je ne peux pas déterminer ces nombres avec leur seul produit, annonce Pierre.

2) Je le savais, dit Serge.

3) Ah, bon ? Alors, je les connais, dit Pierre.

4) Dans ce cas, moi aussi, rétorque Serge.

Quels sont ces deux nombres ?

On note a et b les nombres cherchés et p et s leur produit et leur somme. Si quelqu'un connaît p et s il connaît a et b (par exemple parce que ce sont les racines de l'équation $X^2 - sX + p = 0$). On a $p, s \geq 4$, $s \leq 200$ et $p \leq 10000$. On note que p n'est pas un nombre premier.

2.2 Conséquences de l'assertion 1)

Pierre connaissant le produit p peut en déduire les nombres a et b s'il n'y a qu'une écriture $p = ab$ avec $2 \leq a, b \leq 100$. Appelons P^+ (resp. P^-) les nombres qui vérifient cette propriété (resp. les autres), de sorte que le nombre p détenu par Pierre est dans P^-. On a le lemme suivant :

2.1 Lemme. *1) L'ensemble P^+ contient les produits de deux nombres premiers ≤ 100.*

2) Si p a un facteur premier > 50 il est dans P^+.

3) Si p est ≥ 9800, p est dans P^+

Démonstration. Le point 1) est évident. Pour 2), si q est un facteur premier de p avec $q > 50$, et si $p = ab$, q divise a ou b donc lui est égal puisque les nombres sont ≤ 100 et l'unique décomposition convenable est donc $p = q \times (p/q)$. Enfin, pour 3), si $p = ab$ avec $a \leq b$, comme $97 \times 100 < 9800$ on a $a \geq 98$. Si $a = 98$, on a $b = 100$ car $98 \times 99 = 9702 < 9800$. Les seules possibilités sont donc $p = 98 \times 100 = 9800$, $p = 99 \times 99 = 9801$, $p = 99 \times 100 = 9900$

et $p = 100 \times 100 = 10000$. Dans tous les cas, p détermine a et b de manière unique.

2.2 *Remarque.* Il y a d'autres p que ceux évoqués au lemme 2.1 dans P^+, par exemple les $p = uvw$ avec u, v, w premiers, $u \leq v \leq w \leq 100$ et $uv \leq 100$ mais $uw > 100$, comme $3 \times 5 \times 37$.

2.3 Conséquences de l'assertion 2)

Ce que dit Serge c'est qu'il savait que Pierre ne pouvait pas conclure. Cela signifie exactement que s n'est pas somme de deux nombres a, b avec $2 \leq a, b \leq 100$ tels que ab soit dans P^+, sinon il ne pourrait pas affirmer cela. Appelons S^+ (resp. S^-) les nombres compris entre 4 et 200 qui sont sommes de deux nombres a, b avec $2 \leq a, b \leq 100$ tels que ab soit dans P^+ (resp. les autres). Le nombre s détenu par Serge est donc un nombre de S^- et on a le lemme :

2.3 Lemme. *L'ensemble S^- (les "nombres de Serge") est contenu dans l'ensemble des nombres* $11, 17, 23, 27, 29, 35, 37, 41, 47, 51, 53$.

Démonstration. Si s est ≥ 55 il est dans S^+. En effet, si s est ≥ 198, on a nécessairement l'une des décompositions $198 = 98 + 100 = 99 + 99$ ou $199 = 99 + 100$ ou $200 = 100 + 100$ et on conclut par 2.1.3. Si l'on a $99 \leq s \leq 197$ on écrit $s = a + b$ avec $b = 97$ et $a = s - 97$ donc $2 \leq a \leq 100$ et on conclut par 2.1.2. Si l'on a $55 \leq s \leq 98$ on écrit $s = a + b$ avec $b = 53$ et $a = s - 53$ et on conclut de la même manière.

Il reste à examiner les nombres $s \leq 54$. Si s est un nombre pair, il est somme de deux nombres premiers ≤ 100 (c'est l'hypothèse de Goldbach, évidemment vérifiée pour des nombres de cette taille), donc s est dans S^+.

Enfin, les nombres de la forme $s = 2 + q \leq 54$ avec q premier impair sont évidemment dans S^+. Les nombres de S^- sont donc parmi les nombres s impairs ≤ 53 tels que $s - 2$ ne soit pas premier. On obtient la liste annoncée.

2.4 *Remarques.* 1) Attention, les nombres de S^- sont parmi les nombres ci-dessus, mais la réciproque n'est pas vraie. Ainsi 51 est dans S^+. En effet, il s'écrit $51 = 17 + 34$ et le produit $17 \times 34 = 2 \times 17 \times 17$ n'a qu'une décomposition convenable en produit ab. Le lecteur courageux vérifiera que tous les autres sont bien dans S^-, mais c'est sans importance pour ce qui suit.

2) Une conséquence de 2.3 est que l'un des nombres a et b est pair et l'autre impair. Appelons a le nombre pair et b l'impair.

2.3.1 Les ensembles P_s^-

Rappelons que si s est dans S^- alors pour toute décomposition $s = a + b$ avec $2 \leq a, b \leq 100$, le nombre $p = ab$ est dans P^-. Pour un tel s on appelle P_s^- l'ensemble des $p = ab$ avec $a + b = s$ et $a, b \geq 2$ (la condition $a, b \leq 100$ est automatique car les s de S^- sont ≤ 100).

Il est facile de déterminer P_s^-. Par exemple, pour $s = 11$, les décompositions possibles sont $11 = 9 + 2 = 3 + 8 = 4 + 7 = 5 + 6$ qui donnent les produits $18, 24, 28$ et 30 dont on vérifie qu'ils sont dans P^- : $18 = 2 \times 9 = 3 \times 6$; $24 = 3 \times 8 = 2 \times 12 = 4 \times 6$; $28 = 4 \times 7 = 2 \times 14$; $30 = 5 \times 6 = 2 \times 15 = 3 \times 10$. On a donc $P_{11}^- = \{18, 24, 28, 30\}$.

Le lecteur trouvera en annexe la liste de tous les P_s^- pour $s \in S^-$.

2.4 Conséquences de l'assertion 3)

Bien entendu, Pierre a dressé la liste des nombres de s possibles après l'assertion 2). Pour conclure, voilà comment il peut raisonner. Supposons par exemple qu'il détienne le nombre : $p = 50 = 2 \times 5 \times 5$. Les décompositions convenables en ab sont 2×25 et 10×5 avec les valeurs de s : 27 et 15. Parmi celles-ci, seule 27 est dans la liste de Serge, de sorte que si $p = 50$, Pierre peut conclure que la solution est $a = 2$ et $b = 25$.

Cela nous conduit à la définition suivante :

2.5 Définition. *Soit $p \in P^-$. On dit que p est* **orphelin** *s'il est dans un unique ensemble P_s^- pour $s \in S^-$.*

Le fait que Pierre puisse conclure signifie exactement que le p qu'il détient est orphelin.

2.5 Conséquences de l'assertion 4)

Comme Serge peut conclure, c'est qu'il a pu déterminer, en connaissant seulement s, le p orphelin détenu par Pierre et pour cela, il faut et il suffit qu'il n'y ait qu'un seul orphelin dans P_s^-. Une méthode brutale (mais qui ne pose pas de problème avec un ordinateur) consiste à faire la liste exhaustive de tous les ensembles P_s^- (voir l'annexe ci-dessous). Un examen attentif de cette liste montre que seul P_{17}^- contient un unique orphelin, à savoir 52. On a donc $p = 52$ et $s = 17$, $a = 4$ et $b = 13$.

Pour ceux que rebuterait l'emploi d'un tel rouleau compresseur, on peut s'épargner d'écrire toute les listes : un s est éliminé dès que P_s^- contient au moins deux orphelins. Dans certains cas c'est facile à vérifier : si les éléments sont petits (comme dans P_{11}^-) ou grands (comme dans P_{53}^-) ...

2.5.1 Annexe : la liste des P_s^-

Les nombres indiqués en rouge sont les nombres orphelins.

$$P_{11}^- = \{18, 24, 28, 30\}, \quad P_{17}^- = \{30, 42, 52, 60, 66, 70, 72\}.$$

$$P_{23}^- = \{42, 60, 76, 90, 102, 112, 120, 126, 130, 132\}.$$

$$P_{27}^- = \{50, 72, 92, 110, 126, 140, 152, 162, 170, 176, 180, 182\}.$$

$$P_{29}^- = \{54, 78, 100, 120, 138, 154, 168, 180, 190, 198, 204, 208, 210\}.$$

$$P_{35}^- = \{66, 96, 124, 150, 174, 196, 216, 234, 250, 264, 276, 286, 294, 300, 304, 306\}.$$

$$P_{37}^- = \{70, 102, 132, 160, 186, 210, 232, 252, 270, 286, 300, 312, 322, 330, 336, 340, 342\}.$$

$$P_{41}^- = \{78, 114, 148, 180, 210, 238, 264, 288, 310, 330, 348, 364, 378, 390, 400, 408, 414, 418, 420\}.$$

$$P_{47}^- = \{90, 132, 172, 210, 246, 280, 312, 342, 370, 396, 420, 442, 462, 480, 496, 510, 522, 532, 540, 546, 550, 552\}.$$

$$P_{53}^- = \{102, 150, 196, 240, 282, 322, 360, 396, 430, 462, 492, 520, 546, 570, 592, 612, 630, 646, 660, 672, 682, 690, 696, 700, 702\}.$$

2.5.2 Conclusion

Le problème de l'APM est tout à fait intéressant et différent du problème classique, avec le petit défaut que la quatrième assertion n'est pas nécessaire au spectateur pour conclure.