CORRIGÉ

Reprendre les maths · CORRIGÉ

Les nombres premiers s'arrêtent-ils un jour ?

CHAPITRES

Divisibilité · Nombres premiers · Raisonnement logique

Ce corrigé reprend le raisonnement étape par étape. Les encadrés « À retenir » isolent les résultats essentiels, et les encadrés « Idée » mettent en évidence les mécanismes qui seront réutilisés plus loin.

I Retrouver quelques repères

1

Dire que a divise 18 signifie qu'il existe un entier k tel que

$$18 = a \times k.$$

Autrement dit, la division de 18 par a doit « tomber juste » : le quotient doit être un entier, ou, si l'on effectue une division euclidienne, le reste doit être nul.

Pour 2, 3 et 6, on trouve immédiatement

$$18 = 2 \times 9, \qquad 18 = 3 \times 6, \qquad 18 = 6 \times 3.$$

Les nombres 2, 3 et 6 divisent donc 18.

Regardons maintenant 4 et 5. Les divisions euclidiennes donnent

$$18 = 4 \times 4 + 2, \qquad 18 = 5 \times 3 + 3.$$

Dans le premier cas, le quotient est 4 et le reste est 2 ; dans le second, le quotient est 3 et le reste est 3. Les restes ne sont pas nuls. Cela signifie qu'il n'existe pas d'entier k tel que $18 = 4k$, ni d'entier k tel que $18 = 5k$.

On peut dire la même chose avec la division ordinaire : $18/4 = 4{,}5$ et $18/5 = 3{,}6$ ne sont pas des entiers.

À retenir — 2, 3 et 6 divisent 18 ; 4 et 5 ne divisent pas 18.

IDÉE Trois formulations disent ici la même chose : « a divise n », « n/a est un entier », « dans la division euclidienne de n par a, le reste est 0 ». Suivant la situation, on peut utiliser la formulation la plus pratique.

2

Commençons par distinguer deux types de vérification.

- Pour montrer qu'un entier est **composé**, il suffit de trouver *une seule* factorisation en deux entiers strictement supérieurs à 1.
- Pour montrer qu'un entier $n > 1$ est **premier**, il faut au contraire vérifier qu'aucun entier de 2 à $n - 1$ ne le divise. C'est une vérification finie : il n'y a qu'un nombre fini de candidats à tester.

Pour 7, les seuls candidats autres que 1 et 7 sont $2, 3, 4, 5, 6$. On peut effectuer les divisions euclidiennes :

$$7 = 2 \times 3 + 1, \quad 7 = 3 \times 2 + 1,$$
$$7 = 4 \times 1 + 3, \quad 7 = 5 \times 1 + 2,$$
$$7 = 6 \times 1 + 1.$$

Aucun reste n'est nul. Aucun des entiers $2, 3, 4, 5, 6$ ne divise donc 7. Ses seuls diviseurs positifs sont 1 et 7 : 7 est premier.

Pour 12, une seule égalité suffit :

$$12 = 3 \times 4.$$

Comme $3 > 1$ et $4 > 1$, 12 possède des diviseurs autres que 1 et lui-même : il est composé.

Pour 17, on pourrait de la même manière tester successivement les divisions de 17 par

$$2, 3, 4, \ldots, 16.$$

Aucune ne donne un quotient entier, c'est-à-dire qu'aucune division euclidienne n'a un reste nul. Il n'y a donc pas de diviseur positif de 17 autre que 1 et 17 : 17 est premier. Nous ne recopions pas ici les quinze divisions, mais c'est bien cette vérification finie qui justifie l'affirmation.

Enfin,

$$21 = 3 \times 7,$$

donc 21 est composé.

À retenir — 7 et 17 sont premiers ; 12 et 21 sont composés.

IDÉE Il existe des méthodes qui réduisent fortement le nombre de divisions nécessaires pour tester si un entier est premier. Pour le raisonnement présent, il suffit de savoir que la vérification porte sur un nombre fini de candidats.

II Un nombre premier finit toujours par apparaître

3

(a) Nous devons d'abord justifier deux choses : qu'il existe bien au moins un diviseur de N strictement supérieur à 1, puis que l'on peut parler du plus petit d'entre eux.

Puisque N est un entier strictement supérieur à 1, on a

$$N = N \times 1.$$

Ainsi N divise N. Le nombre N lui-même est donc un diviseur de N strictement supérieur à 1 : la liste que nous considérons n'est pas vide.

Ensuite, un diviseur positif d de N ne peut pas être plus grand que N. En effet, si d divise N, alors il existe un entier positif k tel que

$$N = d \times k.$$

Comme $k \geq 1$, on a nécessairement $d \leq N$.

Tous les diviseurs positifs de N sont donc pris parmi la liste finie

$$1, 2, 3, \ldots, N.$$

Les diviseurs strictement supérieurs à 1 forment ainsi une liste **finie et non vide**. Dans une liste finie non vide de nombres entiers, on peut toujours repérer le plus petit élément. C'est ce plus petit diviseur que nous appelons d.

IDÉE Exemple : si $N = 35$, les diviseurs positifs sont $1, 5, 7, 35$. Ceux qui sont strictement supérieurs à 1 sont $5, 7, 35$, et le plus petit est 5. Le raisonnement précédent garantit que cette situation — une liste finie non vide avec un plus petit élément — existe pour tout entier $N > 1$.

(b) Supposons maintenant que d soit composé. Cela signifie qu'il peut s'écrire comme un produit de deux entiers strictement supérieurs à 1 :

$$d = a \times b.$$

Le sujet nous place dans le cas $1 < a < d$.

Comme d divise N, il existe un entier k tel que

$$N = d \times k.$$

En remplaçant d par $a \times b$, on obtient

$$N = (a \times b) \times k.$$

Par associativité de la multiplication,

$$N = a \times (bk).$$

Or b et k sont des entiers, donc leur produit bk est encore un entier. Nous avons donc écrit N sous la forme

$$N = a \times (\text{un entier}).$$

C'est exactement la définition de « a divise N ». Ainsi a divise N.

IDÉE On vient d'utiliser une propriété très naturelle : si a divise d et si d divise N, alors a divise N. L'égalité $N = a(bk)$ permet de la retrouver directement.

(c) Nous avons trouvé un diviseur a de N tel que

$$1 < a < d.$$

Mais d avait précisément été choisi comme le *plus petit* diviseur de N strictement supérieur à 1. Il ne peut donc pas exister un autre diviseur de N strictement compris entre 1 et d.

Nous obtenons une contradiction. L'hypothèse « d est composé » est donc impossible. Comme $d > 1$, la seule possibilité restante est que d soit premier.

À retenir — Tout entier strictement supérieur à 1 possède au moins un diviseur premier.

IDÉE Ce résultat est essentiel pour la suite. Nous n'aurons jamais besoin de savoir à l'avance si le nombre construit est premier. Il suffira de savoir qu'étant strictement supérieur à 1, il possède quelque part au moins un diviseur premier.

III Une expérience qui fonctionne… puis qui nous piège

4

On a

$$30 = 2 \times 3 \times 5 \qquad \text{et} \qquad 31 = 30 + 1.$$

Les nombres 2, 3 et 5 divisent donc tous 30.

Il y a deux manières complémentaires de voir qu'ils ne divisent pas 31.

Première lecture : les divisions euclidiennes

Effectuons les divisions euclidiennes de 31 par 2, 3 et 5 :

$$31 = 2 \times 15 + 1, \qquad 31 = 3 \times 10 + 1, \qquad 31 = 5 \times 6 + 1.$$

Pour la division par 2, le quotient est 15 et le reste est 1 ; pour la division par 3, le quotient est 10 et le reste est 1 ; pour la division par 5, le quotient est 6 et le reste est 1.

Dans les trois cas, le reste vaut 1 et non 0. Par le critère rappelé à la question 1, cela signifie que 2, 3 et 5 ne divisent pas 31.

Deuxième lecture : la différence de deux multiples

Cette seconde lecture est celle qui sera utile pour généraliser.

Prenons par exemple 2. Nous savons que 2 divise 30. Supposons, pour voir ce qui se passerait, que 2 divise aussi 31. Il existerait alors deux entiers u et v tels que

$$30 = 2u \qquad \text{et} \qquad 31 = 2v.$$

En soustrayant les deux égalités,

$$31 - 30 = 2v - 2u = 2(v - u).$$

Donc $1 = 2(v-u)$. Comme $v-u$ est un entier, cela signifierait que 2 divise 1, ce qui est impossible : aucun multiple entier de 2 ne vaut 1.

Le même raisonnement vaut avec 3 ou 5 à la place de 2.

À retenir — 2, 3 et 5 ne divisent pas 31.

IDÉE Le mécanisme général est maintenant explicite : si un entier $m > 1$ divise un nombre A, il ne peut pas diviser en même temps $A + 1$. S'il divisait les deux, alors il diviserait leur différence $(A + 1) - A = 1$, ce qui est impossible.

5

Comme $31 > 1$, le résultat de la partie II garantit que 31 possède au moins un diviseur premier. Appelons ce diviseur premier q.

La question 4 nous a montré que 2, 3 et 5 ne divisent pas 31. Le nombre premier q, qui lui divise 31, ne peut donc être ni 2, ni 3, ni 5. Il s'agit nécessairement d'un nombre premier absent de la liste de départ.

Dans cet exemple particulier, le nombre 31 est lui-même premier. Comment pourrait-on le vérifier si on voulait le faire complètement ? On testerait les divisions de 31 par tous les entiers

$$2, 3, 4, \ldots, 30.$$

Aucune ne donne un quotient entier, donc aucun de ces entiers ne divise 31 ; ses seuls diviseurs positifs sont alors 1 et 31. Cette vérification n'est toutefois *pas nécessaire* au raisonnement principal : l'existence d'au moins un diviseur premier de 31 suffit.

À retenir — À partir de la liste $2, 3, 5$, la construction fait apparaître au moins un nombre premier qui n'était pas dans la liste.

6

(a) La règle proposée disait : « le produit de plusieurs nombres premiers, puis $+1$, est toujours premier ». Pour réfuter une affirmation contenant le mot *toujours*, un seul contre-exemple suffit. Or

$$30031 = 59 \times 509.$$

Les deux facteurs 59 et 509 sont strictement supérieurs à 1, donc cette égalité est une factorisation non triviale de 30031. Le nombre 30031 est composé. La règle « toujours premier » est donc fausse.

IDÉE Attention : Il ne faut pas remplacer la bonne idée par une règle fausse. La construction ne garantit pas que le nombre obtenu soit premier ; elle garantit que les nombres premiers déjà présents dans la liste ne le divisent pas.

(b) On a

$$30030 = 2 \times 3 \times 5 \times 7 \times 11 \times 13,$$

donc chacun des six nombres $2, 3, 5, 7, 11, 13$ divise 30030 : chacun apparaît comme facteur du produit.

Prenons l'un quelconque de ces nombres et appelons-le p. Comme p divise 30030, il existe un entier u tel que

$$30030 = pu.$$

Supposons que p divise aussi 30031. Il existerait alors un entier v tel que

$$30031 = pv.$$

En soustrayant,

$$1 = 30031 - 30030 = p(v - u).$$

Cela signifierait que p divise 1. Or p est un nombre premier, donc $p \geq 2$, et aucun entier supérieur à 1 ne divise 1.

Cette contradiction montre que p ne divise pas 30031. Comme p pouvait désigner n'importe lequel des six nombres de la liste, aucun des six ne divise 30031.

(c) $30031 > 1$. La partie II garantit donc l'existence d'au moins un diviseur premier de 30031 ; appelons-le q. Or aucun des six nombres premiers de la liste ne divise 30031. Le diviseur premier q ne peut donc être aucun d'eux :

$$q \notin \{2, 3, 5, 7, 11, 13\}.$$

Il existe donc au moins un nombre premier nouveau par rapport à la liste de départ.

La factorisation $30031 = 59 \times 509$ sert seulement à montrer que 30031 est composé. Pour conclure à l'existence d'un diviseur premier nouveau, nous n'avons pas besoin de déterminer lequel : le résultat de la partie II s'en charge.

(d) La formulation correcte de la construction est donc la suivante.

À retenir — Si l'on multiplie les nombres premiers d'une liste finie puis que l'on ajoute 1, le nombre obtenu possède au moins un diviseur premier qui n'appartient pas à la liste de départ.

IV La même expérience, quelle que soit la liste

7

Prenons par exemple les quatre nombres premiers

$$2, 3, 5, 7.$$

Leur produit vaut

$$2 \times 3 \times 5 \times 7 = 210,$$

et nous construisons

$$211 = 210 + 1.$$

Chacun des nombres $2, 3, 5, 7$ divise 210. Prenons l'un d'eux, noté p. Si p divisait aussi 211, alors, comme dans la question 4, p diviserait la différence

$$211 - 210 = 1,$$

ce qui est impossible puisque $p > 1$. Aucun des quatre nombres premiers de départ ne divise donc 211.

Comme $211 > 1$, la partie II garantit que 211 possède au moins un diviseur premier q. Ce q ne peut être aucun des quatre nombres premiers de départ, puisqu'aucun d'eux ne divise 211.

À retenir — La liste $2, 3, 5, 7$ n'était donc pas « terminée » : la construction garantit l'existence d'au moins un nombre premier absent de cette liste.

IDÉE Le nombre construit n'a toujours pas besoin d'être premier. Avec la liste $3, 5, 7, 11$, on obtient $3 \times 5 \times 7 \times 11 = 1155$, puis $1156 = 34^2 = 2^2 \times 17^2$. Le nombre obtenu est composé, mais ses facteurs premiers 2 et 17 sont absents de la liste de départ.

8

Nous passons maintenant du cas numérique au cas général. Imaginons une liste finie non vide quelconque de nombres premiers, et appelons P le produit de tous les nombres de cette liste.

(a) Prenons un nombre premier quelconque de la liste et appelons-le p. Puisque p apparaît comme l'un des facteurs du produit P, on peut écrire

$$P = p \times M,$$

où M est le produit des autres facteurs de la liste ; en particulier, M est un entier. Cela montre directement que p divise P.

Supposons maintenant que p divise aussi $P + 1$. Il existerait alors un entier K tel que

$$P + 1 = pK.$$

Comme $P = pM$, on peut soustraire les deux égalités :

$$(P + 1) - P = pK - pM = p(K - M).$$

Le membre de gauche vaut 1, donc

$$1 = p(K - M).$$

Or $K - M$ est un entier. Cette égalité dirait donc que p divise 1, ce qui est impossible puisque p est premier et donc $p \geq 2$.

Ainsi p ne divise pas $P+1$. Comme p était *n'importe quel* nombre premier de la liste, aucun nombre premier de la liste ne divise $P + 1$.

IDÉE Les lettres ne changent rien au mécanisme. Dans la question 4, P valait 30, $P+1$ valait 31 et p pouvait être 2, 3 ou 5. Ici, les lettres permettent simplement de refaire le même raisonnement sans choisir une liste particulière.

(b) Le nombre P est un produit de nombres premiers positifs, donc $P \geq 2$. En particulier,

$$P + 1 > 1.$$

La partie II s'applique : $P+1$ possède au moins un diviseur premier. Appelons ce diviseur premier q.

(c) Nous savons deux choses :

- q divise $P+1$;
- aucun nombre premier de la liste de départ ne divise $P+1$.

Si q appartenait à la liste de départ, il serait précisément l'un des nombres premiers que nous venons de montrer incapables de diviser $P+1$. C'est impossible. Donc q n'appartient pas à la liste.

À retenir — À partir de n'importe quelle liste finie non vide de nombres premiers, on peut toujours trouver au moins un nombre premier qui n'est pas dans cette liste.

Cette phrase est la clé du problème : aussi longue soit-elle, une liste finie de nombres premiers peut toujours être dépassée.

V Peut-il alors exister un dernier nombre premier ?

9

Supposons qu'il n'existe qu'un nombre fini de nombres premiers.

Le mot *fini* signifie qu'il existe un entier r donnant leur nombre total. On pourrait alors, au moins en principe, tous les ranger dans une liste

$$p_1, p_2, \ldots, p_r.$$

Cette notation ne dit pas que nous connaissons effectivement ces nombres ni que la liste est courte ; elle exprime seulement l'hypothèse selon laquelle il y en aurait un nombre fini et que la liste serait complète.

Appliquons la question 8 à cette liste supposée contenir *tous* les nombres premiers. Posons

$$P = p_1 p_2 \cdots p_r$$

et considérons $P+1$.

La question 8 montre que $P+1$ possède un diviseur premier q qui n'appartient pas à la liste $p_1, \ldots, p_r$.

Mais la liste avait été supposée complète. Dire qu'elle contient tous les nombres premiers signifie précisément que tout nombre premier, donc q, devrait appartenir à cette liste.

Nous sommes donc forcés d'affirmer simultanément :

- q est un nombre premier, donc il devrait être dans la liste complète ;
- q n'est pas dans cette liste, d'après la construction.

Ces deux affirmations sont incompatibles. C'est la contradiction recherchée.

À retenir — L'hypothèse « il n'existe qu'un nombre fini de nombres premiers » est impossible. Il existe donc une infinité de nombres premiers.

IDÉE Une contradiction n'est pas un calcul faux : c'est le signe que l'hypothèse de départ ne peut pas être vraie, parce qu'elle conduit logiquement à deux conclusions incompatibles.

10

Voici une rédaction autonome possible, suivie d'une lecture détaillée.

Supposons, par l'absurde, qu'il n'existe qu'un nombre fini de nombres premiers. On peut alors les écrire tous dans une liste finie

$$p_1, p_2, \dots, p_r.$$

Considérons leur produit

$$P = p_1 p_2 \cdots p_r$$

et le nombre

$$N = P + 1.$$

Pour chaque nombre premier p_i de la liste, p_i divise P puisque p_i est l'un des facteurs du produit P.

Supposons que p_i divise aussi $N = P + 1$. Il existe alors des entiers A et B tels que

$$P = p_i A \qquad \text{et} \qquad N = p_i B.$$

En soustrayant,

$$1 = N - P = p_i(B - A).$$

Comme $B - A$ est entier, cela signifierait que p_i divise 1, ce qui est impossible puisque $p_i > 1$. Ainsi aucun nombre premier de la liste ne divise N.

Or $N = P + 1 > 1$. D'après le résultat démontré à la partie II, tout entier strictement supérieur à 1 possède au moins un diviseur premier. Il existe donc un nombre premier q qui divise N.

Puisqu'aucun nombre premier de la liste ne divise N, le nombre premier q n'appartient pas à la liste. Nous avons donc construit un nombre premier absent de la liste supposée contenir tous les nombres premiers. C'est une contradiction.

Par conséquent, il n'existe pas de liste finie contenant tous les nombres premiers. Il existe donc une infinité de nombres premiers.

Comment lire cette preuve sans perdre le fil ?

La démonstration comporte cinq mouvements.

- On suppose le contraire du résultat recherché : il n'y aurait qu'un nombre fini de nombres premiers.
- Cette hypothèse permet d'imaginer une liste finie complète $p_1, \dots, p_r$.
- On fabrique le produit P de tous les nombres de la liste, puis le nombre voisin $P + 1$.
- Aucun nombre premier de la liste ne divise $P + 1$, mais $P + 1 > 1$ possède malgré tout un diviseur premier q.
- Ce q devrait être dans la liste parce qu'elle est supposée complète, et il ne peut pas y être parce qu'il divise $P + 1$. Contradiction.

IDÉE Attention : La contradiction ne vient jamais de l'affirmation « $P + 1$ est premier ». Cette affirmation est fausse en général. La preuve utilise seulement le fait, démontré en partie II, que $P + 1 > 1$ possède au moins un diviseur premier.

Un exemple miniature avant de relire les lettres

Imaginons, à tort, que les seuls nombres premiers soient 2, 3 et 5. Leur produit vaut 30, puis on construit $31 = 30 + 1$.

Les divisions euclidiennes

$$31 = 2 \times 15 + 1, \qquad 31 = 3 \times 10 + 1, \qquad 31 = 5 \times 6 + 1$$

montrent qu'aucun des trois nombres de la prétendue liste complète ne divise 31. Pourtant $31 > 1$ possède un diviseur premier. Ce diviseur premier est nécessairement hors de la liste $2, 3, 5$: la liste ne pouvait donc pas être complète.

La preuve générale fait exactement la même chose. Elle remplace simplement $2, 3, 5$ par une liste finie quelconque $p_1, \ldots, p_r$ et 30 par leur produit P.

Un très ancien raisonnement

La preuve moderne est souvent présentée sous forme de raisonnement par l'absurde. Le texte d'Euclide, au livre IX, proposition 20 des *Éléments*, est organisé un peu différemment : il part d'une collection donnée de nombres premiers et montre directement qu'on peut en trouver davantage. Le coeur mathématique est le même : une collection finie ne peut jamais épuiser tous les nombres premiers.

La dernière surprise du sujet

Une infinité de nombres premiers ne signifie pas qu'ils apparaissent à intervalles réguliers. Par exemple,

$$24, 25, 26, 27, 28$$

sont cinq nombres composés consécutifs, car

$$24 = 2 \times 12, \quad 25 = 5 \times 5, \quad 26 = 2 \times 13, \quad 27 = 3 \times 9, \quad 28 = 4 \times 7.$$

Pour chacun d'eux, une factorisation non triviale suffit à montrer qu'il est composé.

Il n'y a aucune contradiction avec l'infinité des nombres premiers. « Il existe une infinité de nombres premiers » signifie qu'il n'existe pas de dernier nombre premier. Cette affirmation n'impose pas qu'ils soient régulièrement espacés. Un autre problème pourra montrer comment construire des suites de nombres composés consécutifs aussi longues que l'on veut.

SOURCES

Euclide, *Éléments*, livre IX, proposition 20, traduction anglaise de T. L. Heath, Perseus Digital Library — Lien direct

Euclide, *Éléments*, livre VII, proposition 31, traduction anglaise de T. L. Heath — Lien direct