

Les nombres premiers s'arrêtent-ils un jour ?

Divisibilité · Nombres premiers ·
Raisonnement logique

Les nombres premiers commencent par 2, 3, 5, 7, 11, 13, ... On peut continuer à en chercher et en trouver beaucoup d'autres. Mais trouver toujours plus d'exemples ne répond pas à la question essentielle : comment savoir que cette liste ne finira jamais ? Ce problème propose de repartir de calculs très simples, puis de faire peu à peu apparaître une idée générale jusqu'à obtenir une véritable démonstration.

Vous pouvez vous lancer si...

Vous savez effectuer les opérations élémentaires sur les nombres entiers. Une calculatrice peut être utilisée pour les calculs : l'essentiel du problème est ailleurs. Les mots *diviseur*, *multiple*, *nombre premier*, *nombre composé* et *factorisation* seront remis en place au moment où ils deviennent utiles.

I Retrouver quelques repères

On dit qu'un entier a **divise** un entier n lorsqu'on peut écrire

$$n = a \times k$$

avec k entier. Par exemple, $18 = 3 \times 6$, donc 3 divise 18. On peut dire la même chose dans l'autre sens : 18 est un **multiple** de 3.

- 1 Parmi les nombres 2, 3, 4, 5, 6, lesquels divisent 18 ? Pour chacun de ceux que vous retenez, écrivez 18 sous la forme d'un produit qui justifie votre réponse.

Un **nombre premier** est un entier strictement supérieur à 1 qui n'a que deux diviseurs positifs : 1 et lui-même. Ainsi, 7 est premier.

Un entier strictement supérieur à 1 qui n'est pas premier est appelé **composé**. Par exemple, $12 = 3 \times 4$, donc 12 est composé. Écrire un nombre sous la forme d'un produit s'appelle une **factorisation**.

- 2 Parmi 7, 12, 17, 21, repérez les nombres premiers et les nombres composés. Pour chaque nombre composé, donnez une factorisation qui le montre immédiatement.

II Un nombre premier finit toujours par apparaître

Nous allons établir un petit résultat qui sera utilisé plusieurs fois ensuite.

Prenons un entier strictement supérieur à 1. Pour parler de n'importe quel entier de ce type sans en choisir un en particulier, nous allons utiliser une lettre et l'appeler N .

IDÉE La lettre N ne représente pas un nombre mystérieux : elle signifie simplement « un entier strictement supérieur à 1, quel qu'il soit ». Utiliser une lettre permet de raisonner en une seule fois sur tous les entiers concernés. Par exemple, si $N = 35$, le plus petit diviseur de N strictement supérieur à 1 est 5.

Parmi les diviseurs de N strictement supérieurs à 1, choisissons le plus petit et appelons-le d .

- 3 (a) Pourquoi est-on certain qu'il existe au moins un diviseur de N strictement supérieur à 1 ?

- (b) Imaginons que d soit composé. Il pourrait alors s'écrire $d = a \times b$ avec $1 < a < d$. Comme d divise N , on peut également écrire $N = d \times k$ pour un certain entier k . En remplaçant d par $a \times b$, montrez que a divise lui aussi N .
- (c) Pourquoi cela est-il incompatible avec le choix de d comme plus petit diviseur de N strictement supérieur à 1 ? Concluez : tout entier strictement supérieur à 1 possède au moins un diviseur premier.

III Une expérience qui fonctionne... puis qui nous piège

Commençons avec seulement trois nombres premiers :

$$2, \quad 3, \quad 5.$$

Multiplions-les, puis ajoutons 1 :

$$2 \times 3 \times 5 + 1 = 31.$$

- 4 On a $31 = 30 + 1$ et $30 = 2 \times 3 \times 5$. Expliquez pourquoi 2, 3 et 5 ne peuvent pas diviser 31.

IDÉE Pour vous orienter : la différence de deux multiples d'un même entier est encore un multiple de cet entier. Ainsi, si un même entier divisait 30 et 31, il devrait aussi diviser $31 - 30 = 1$. Demandez-vous si cela est possible pour 2, 3 ou 5.

- 5 Le nombre 31 est strictement supérieur à 1. D'après la partie II, il possède donc au moins un diviseur premier. Pourquoi ce diviseur premier ne peut-il être ni 2, ni 3, ni 5 ? Qu'est-ce que cette construction nous a donc permis de découvrir à partir de la liste 2, 3, 5 ?

Dans cet exemple, 31 est lui-même premier. On pourrait être tenté d'en déduire la règle suivante :

« Si l'on multiplie plusieurs nombres premiers et que l'on ajoute 1, le résultat est toujours premier. »

Ce serait faux. En effet,

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$$

et

$$30031 = 59 \times 509.$$

Le nombre 30031 est donc composé.

- 6 (a) Pourquoi cet exemple suffit-il à réfuter la règle proposée ci-dessus ?
- (b) Pourtant, quelque chose d'essentiel dans notre première expérience reste vrai. Reprenez le raisonnement de la question 4 en observant que $30031 = 30030 + 1$. Expliquez pourquoi aucun des nombres 2, 3, 5, 7, 11, 13 ne divise 30031.
- (c) 30031 possède au moins un diviseur premier. Que pouvez-vous affirmer sur ce diviseur premier par rapport aux six nombres premiers de la liste ?
- (d) Reformulez avec vos propres mots ce que la construction « produit des nombres premiers de la liste +1 » permet réellement d'obtenir.

IV La même expérience, quelle que soit la liste

Avant de passer à un raisonnement complètement général, faisons encore un essai.

- 7 Choisissez quatre nombres premiers. Si vous préférez ne pas choisir, vous pouvez prendre 2, 3, 5, 7. Multipliez-les puis ajoutez 1. Sans chercher à savoir si le nombre obtenu est premier, reprenez le mécanisme de la question 4 : le produit et le nouveau nombre différent de 1. Pourquoi aucun des quatre nombres premiers de départ ne divise-t-il le nouveau nombre ? Que peut-on alors affirmer sur au moins un de ses diviseurs premiers ?

Nous avons maintenant répété la même expérience avec plusieurs listes particulières. Il est temps de faire disparaître les valeurs numériques.

Imaginons **n'importe quelle liste finie non vide de nombres premiers**. Appelons simplement P le produit de tous les nombres premiers présents dans cette liste.

IDÉE La lettre P permet de ne plus choisir une liste particulière. Le raisonnement qui suit doit fonctionner pour quatre nombres premiers, pour cent, ou pour n'importe quel nombre fini d'entre eux. C'est le passage des exemples à une affirmation générale.

- 8 (a) On construit $P + 1$. Prenez n'importe quel nombre premier de la liste : il divise P puisque P est le produit de tous les nombres de la liste. Supposons, pour vous aider à raisonner, qu'il divise aussi $P + 1$. Que devrait-il alors diviser en considérant la différence $(P + 1) - P$? Pourquoi est-ce impossible ?
- (b) Pourtant, $P + 1 > 1$. Que nous garantit la partie II ?
- (c) Que pouvez-vous en conclure sur au moins un diviseur premier de $P + 1$? Complétez finalement l'idée suivante : « À partir de n'importe quelle liste finie non vide de nombres premiers, on peut toujours... »

V Peut-il alors exister un dernier nombre premier ?

Supposons maintenant, pour voir où cette hypothèse nous conduit, qu'il n'existe qu'un **nombre fini** de nombres premiers.

Ils pourraient être très nombreux, peut-être tellement nombreux qu'il serait irréaliste de les écrire tous effectivement. Mais le mot *fini* signifie qu'il y en aurait malgré tout un nombre déterminé.

- 9 Expliquez pourquoi, sous cette hypothèse, on pourrait au moins en principe imaginer une liste finie contenant tous les nombres premiers sans exception. Reprenez alors le résultat obtenu à la question 8. Que se passe-t-il si on applique la construction précédente à cette liste supposée complète ? Menez le raisonnement jusqu'à l'impossibilité.
- 10 Reformulez maintenant l'ensemble du raisonnement sous la forme d'une démonstration autonome, compréhensible par quelqu'un qui n'a pas lu les questions précédentes. Votre texte doit expliquer ce que l'on suppose au départ, quel nombre on construit, pourquoi aucun nombre premier de la liste supposée complète ne le divise, pourquoi il possède pourtant un diviseur premier, puis pourquoi cela conduit à une contradiction. Concluez clairement.

Un très ancien raisonnement

L'idée mathématique que vous venez de reconstruire apparaît dans les *Éléments* d'Euclide, écrits il y a plus de deux millénaires. Sa présentation n'est pas exactement celle que l'on rencontre souvent aujourd'hui : Euclide part lui aussi d'une collection finie de nombres premiers et montre qu'elle ne peut jamais constituer une liste définitive. Le passage des exemples particuliers à une liste arbitraire est donc véritablement au cœur du raisonnement.

Une dernière surprise

Le résultat obtenu signifie qu'il y aura toujours d'autres nombres premiers, aussi loin que l'on aille. Cela ne signifie pourtant pas qu'ils apparaissent à intervalles réguliers : on peut rencontrer des suites de nombres composés consécutifs aussi longues que l'on veut.

IDÉE Ce phénomène peut sembler contradictoire, mais il ne l'est pas. « Il existe une infinité de nombres premiers » signifie qu'il n'y en a pas de dernier ; cela n'empêche pas que deux zones contenant des nombres premiers puissent être séparées par une très longue suite d'entiers composés. Un autre problème pourra montrer comment fabriquer explicitement de telles suites.