Nombres premiers

David Delhoumeau

Juin 2018

Critères de divisibilité

Critères de divisibilité

Critère de divisibilité par 2 : Un nombre est divisible par 2 s'il se termine par un chiffre pair (0 ; 2 ; 4 ; 6 ; ou 8).

Critères de divisibilité

Critère de divisibilité par 2 : Un nombre est divisible par 2 s'il se termine par un chiffre pair (0 ; 2 ; 4 ; 6 ; ou 8).

Critère de divisibilité par 3 : Un nombre est divisible par 3 si la somme de ses chiffres est divisible par 3.

Critères de divisibilité

Critère de divisibilité par 2 : Un nombre est divisible par 2 s'il se termine par un chiffre pair (0 ; 2 ; 4 ; 6 ; ou 8).

Critère de divisibilité par 3 : Un nombre est divisible par 3 si la somme de ses chiffres est divisible par 3.

Critère de divisibilité par 5 : Un nombre est divisible par 5 s'il se termine par un 0 ou 5.

Critères de divisibilité

Critère de divisibilité par 2 : Un nombre est divisible par 2 s'il se termine par un chiffre pair (0 ; 2 ; 4 ; 6 ; ou 8).

Critère de divisibilité par 3 : Un nombre est divisible par 3 si la somme de ses chiffres est divisible par 3.

Critère de divisibilité par 5 : Un nombre est divisible par 5 s'il se termine par un 0 ou 5.

Critère de divisibilité par 9 : Un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9.

Critères de divisibilité

Critère de divisibilité par 2 : Un nombre est divisible par 2 s'il se termine par un chiffre pair (0 ; 2 ; 4 ; 6 ; ou 8).

Critère de divisibilité par 3 : Un nombre est divisible par 3 si la somme de ses chiffres est divisible par 3.

Critère de divisibilité par 5 : Un nombre est divisible par 5 s'il se termine par un 0 ou 5.

Critère de divisibilité par 9 : Un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9.

Critère de divisibilité par 10 : Un nombre est divisible par 10 s'il se termine par un 0.

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; ... ont un point commun lequel ?

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; ... ont un point commun lequel ?

Définition

On appelle nombre premier tout entier positif qui admet exactement deux diviseurs positifs : 1 et lui-même.

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; ... ont un point commun lequel ?

Définition

On appelle nombre premier tout entier positif qui admet exactement deux diviseurs positifs : 1 et lui-même.

Remarque

1 n'est pas un nombre premier.

Un peu d'histoire : A l'Antiquité

Euclide (grec, environ 300 av JC)

Livre VII des Éléments.

1e définition : Un nombre premier comme "étant celui qui n'est mesuré par aucun autre sinon l'unité"

Livre VII des Éléments.

1e définition : Un nombre premier comme "étant celui qui n'est mesuré par aucun autre sinon l'unité"

Livre IX des Éléments.

Théorème fondamental de l'arithmétique : Unicité de la décomposition d'un nombre en facteurs premiers.

Livre VII des Éléments.

1e définition : Un nombre premier comme "étant celui qui n'est mesuré par aucun autre sinon l'unité"

Livre IX des Éléments.

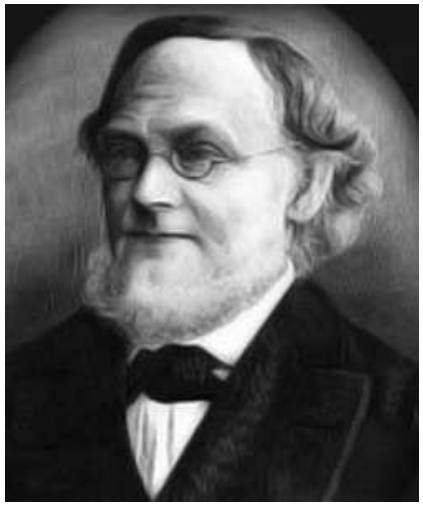
Théorème fondamental de l'arithmétique : Unicité de la décomposition d'un nombre en facteurs premiers.

L'ensemble des nombres premiers est infini.

Eratosthène de Cyrène (-276 Cyrène ; -194 Alexandrie)

Le renouveau de la pensée scientifique

Pierre de Fermat
(1601 - 1665)



Christian Goldbach
(1690 - 1764)

Leonhard Euler
(1707 - 1783)

Factoriser un nombre

Factoriser un nombre c'est décomposer ce nombre en produits de facteurs premiers.

$35 = ?$

$1591 =$

Factoriser un nombre

Factoriser un nombre c'est décomposer ce nombre en produits de facteurs premiers.

$35 = ?$

$1591 = 37 \times 43$

Factoriser un nombre

Factoriser un nombre c'est décomposer ce nombre en produits de facteurs premiers.

$35 = ?$

$1591 = 37 \times 43$

Mersenne, en 1643, avait donné à Fermat, comme un défi, de factoriser le nombre 100895598169 .

Factoriser un nombre

Factoriser un nombre c'est décomposer ce nombre en produits de facteurs premiers.

$35 = ?$

$1591 = 37 \times 43$

Mersenne, en 1643, avait donné à Fermat, comme un défi, de factoriser le nombre 100895598169 .

Vous me demandez si le nombre 100 895 598 169 est premier ou non, et une méthode pour découvrir, dans l'espace d'un jour, s'il est premier ou composé. À cette question, je réponds que ce nombre est composé et se fait du produit de ces deux : 898 423 et 112 303, qui sont premiers.

Factoriser un nombre

Factoriser un nombre c'est décomposer ce nombre en produits de facteurs premiers.

$35 = ?$

$1591 = 37 \times 43$

Mersenne, en 1643, avait donné à Fermat, comme un défi, de factoriser le nombre 100895598169 .

Vous me demandez si le nombre 100 895 598 169 est premier ou non, et une méthode pour découvrir, dans l'espace d'un jour, s'il est premier ou composé. À cette question, je réponds que ce nombre est composé et se fait du produit de ces deux : 898 423 et 112 303, qui sont premiers.

Cependant, le record absolu de factorisation date du 12 décembre 2009

Cependant, le record absolu de factorisation date du 12 décembre 2009

Voila ces nombres :

$$1230186684530117755130494958384962720772853569$$
$$595347921973224$$
$$52151726400507263657518745202199786469389956474942774063845925 1$$
$$92557326303453731548268507917026122142913461670429214311602221 2$$
$$40479274737794080665351419597459856902143413 =$$
$$33478071698956898786044169848212690817704794983713768568 91$$
$$24313889828837938780022876147116525317430877378144679994 89 \times$$
$$36746043666799590428244633799627952632279158164343087642676 0$$
$$3228381573966651127 92 \; 33373417143396810270092798736308917$$

La cryptographie

La cryptographie

La cryptographie (grec ancien kruptos « caché » et graphein « écrire ») est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

Chiffrement RSA (1978)

Rivest (américain) - Shamir (israélien) - Adleman (américain)

Chiffrement RSA (1978)

Rivest (américain) - Shamir (israélien) - Adleman (américain)

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres.

Chiffrement RSA (1978)

Rivest (américain) - Shamir (israélien) - Adleman (américain)

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres.
- Les multiplier.

Chiffrement RSA (1978)

Rivest (américain) - Shamir (israélien) - Adleman (américain)

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres.
- Les multiplier.
- Pour des nombres de cette taille (400 chiffres) on ne sait pas retrouver p et q à partir de leur produit pq.

Chiffrement RSA (1978)

Rivest (américain) - Shamir (israélien) - Adleman (américain)

- On sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres.
- Les multiplier.
- Pour des nombres de cette taille (400 chiffres) on ne sait pas retrouver p et q à partir de leur produit pq.
- Pour coder un message il suffit de connaître le produit pq (public), pour le décoder il faut connaître p et q (secrets).

Et aujourd'hui ?

Et aujourd'hui ?

- 30 ans$\rightarrow$ 50 milliards d'années = 150 chiffres.

  Les banques $\rightarrow$ 300 chiffres
  Les militaires $\rightarrow$ 600 chiffres

Et aujourd'hui ?

- 30 ans$\rightarrow$ 50 milliards d'années = 150 chiffres.

  Les banques $\rightarrow$ 300 chiffres
  Les militaires $\rightarrow$ 600 chiffres

- Quelques conjectures non démontrés à ce jour.

  Conjecture de Golbach - Euler (1742) : Tout nombre pair plus grand que 4 est somme de deux nombres premiers.

  Conjecture des nombres premiers jumeaux : Il existe une infinité de nombre premiers jumeaux.

Et aujourd'hui ?

- 30 ans$\rightarrow$ 50 milliards d'années = 150 chiffres.

  Les banques $\rightarrow$ 300 chiffres
  Les militaires $\rightarrow$ 600 chiffres

- Quelques conjectures non démontrés à ce jour.

  Conjecture de Golbach - Euler (1742) : Tout nombre pair plus grand que 4 est somme de deux nombres premiers.

  Conjecture des nombres premiers jumeaux : Il existe une infinité de nombre premiers jumeaux.

- Le plus grand nombre premier connu à ce jour possède 22 millions de chiffres soit plus de 5000 pages. (janvier 2016)