Les nombres premiers, une recherche active et très ancienne !

Les nombres premiers sont connus depuis l'Antiquité mais sont encore un sujet d'étude majeur !

L'actuel **plus grand nombre premier connu** a été calculé en décembre 2018. Il **possède plus de 24 millions de chiffres**, c'est le nombre : $2^{82\,589\,933} - 1$.

Le système de cryptographie **RSA** est une **base de la sécurité d'internet**. Il est basé sur la multiplication de deux très grands nombres premiers. Si une méthode de factorisation facile existait pour le produit de deux grands nombres premiers, cela poserait d'importants problèmes de sécurité pour Internet.

La conjecture de Goldbach. En 1742, une correspondance entre le mathématicien prusse Christian Goldbach et le suisse Leonhard Euler aboutit à la conjecture :

> *Tout nombre entier pair (supérieur à 3) peut s'écrire comme la somme de deux nombres premiers.*

Exemple : 4=2+2 ; 12 = 5+7 ; 20 = 3+17 ; 30 = 7+23, etc.

Petit exercice : donner des décompositions pour 24, 36 et 100.

De nos jours, ceci a été vérifié par ordinateur pour tous les 4 premiers milliards de milliards de nombres pairs... pourtant, 275 ans après son énonciation, cette proposition n'est toujours pas démontrée !

Les nombres premiers jumeaux. Ce sont deux nombres premiers qui diffèrent de 2. Pour commencer : (3;5), (5;7), (11;13), (17;19). Les deux plus grands nombres premiers jumeaux connus aujourd'hui possèdent 388 342 chiffres, ce sont $2\,996\,863\,034\,895 \times 2^{1\,290\,000} - 1$ et $2\,996\,863\,034\,895 \times 2^{1\,290\,000} + 1$.

Question : y a-t-il une infinité de nombres premiers jumeaux ? On pense que oui, mais personne n'a encore réussi à le démontrer. Seules des versions "allégées" de cette proposition ont été démontrées.

Autres questions irrésolues :
– Existe-t-il une infinité de nombres premiers qui soient supérieurs de 1 à un carré parfait (comme $17 = 4 \times 4 + 1$ ou $37 = 6 \times 6 + 1$ ou encore 101) ?
– Existe-il une formule qui donnerait les nombres premiers dans l'ordre ?

Les nombres premiers, une recherche active et très ancienne !

Les nombres premiers sont connus depuis l'Antiquité mais sont encore un sujet d'étude majeur !

L'actuel **plus grand nombre premier connu** a été calculé en décembre 2018. Il **possède plus de 24 millions de chiffres**, c'est le nombre : $2^{82\,589\,933} - 1$.

Le système de cryptographie **RSA** est une **base de la sécurité d'internet**. Il est basé sur la multiplication de deux très grands nombres premiers. Si une méthode de factorisation facile existait pour le produit de deux grands nombres premiers, cela poserait d'importants problèmes de sécurité pour Internet.

La conjecture de Goldbach. En 1742, une correspondance entre le mathématicien prusse Christian Goldbach et le suisse Leonhard Euler aboutit à la conjecture :

> *Tout nombre entier pair (supérieur à 3) peut s'écrire comme la somme de deux nombres premiers.*

Exemple : 4=2+2 ; 12 = 5+7 ; 20 = 3+17 ; 30 = 7+23, etc.

Petit exercice : donner des décompositions pour 24, 36 et 100.

De nos jours, ceci a été vérifié par ordinateur pour tous les 4 premiers milliards de milliards de nombres pairs... pourtant, 275 ans après son énonciation, cette proposition n'est toujours pas démontrée !

Les nombres premiers jumeaux. Ce sont deux nombres premiers qui diffèrent de 2. Pour commencer : (3;5), (5;7), (11;13), (17;19). Les deux plus grands nombres premiers jumeaux connus aujourd'hui possèdent 388 342 chiffres, ce sont $2\,996\,863\,034\,895 \times 2^{1\,290\,000} - 1$ et $2\,996\,863\,034\,895 \times 2^{1\,290\,000} + 1$.

Question : y a-t-il une infinité de nombres premiers jumeaux ? On pense que oui, mais personne n'a encore réussi à le démontrer. Seules des versions "allégées" de cette proposition ont été démontrées.

Autres questions irrésolues :
– Existe-t-il une infinité de nombres premiers qui soient supérieurs de 1 à un carré parfait (comme $17 = 4 \times 4 + 1$ ou $37 = 6 \times 6 + 1$ ou encore 101) ?
– Existe-il une formule qui donnerait les nombres premiers dans l'ordre ?