Les nombres premiers

Définition

Un entier $n \geqslant 2$ est un nombre premier ssi n admet exactement deux diviseurs 1 et lui-même.

Remarque : un nombre non premier est dit composé.

Les premiers nombres premiers sont :
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...

Il n'existe pas de machine à générer des nombres premiers. Par contre, on dispose de résultats concernant la densité des nombres premiers (hors programme)

Le plus grand nombre premier connu à ce jour (2016) est le nombre de Mersenne suivant :

$2^{74\,207\,281} - 1$ qui comporte 22 338 618 chiffres !

Test de primalité ou critère d'arrêt

Théorème : Soit $n \geqslant 2$:

- n admet un diviseur premier.
- Si n n'est pas premier alors il admet un diviseur premier p tel que : $2 \leqslant p \leqslant \sqrt{n}$.

Pour montrer qu'un nombre n est premier, on utilise la contraposée de ce théorème. Si n n'admet pas de diviseur premier $p \leqslant \sqrt{n}$ alors n est premier.

Exemple : montrons que 109 est premier.

- On calcule $\sqrt{109} \approx 10,4$.
- On teste tous les nombres premiers inférieur à 10 : 2, 3, 5 et 7
- Ces nombres ne divisent pas 109. Donc 109 est premier.

À la recherche des nombres premiers

- Pour obtenir une liste de nombres premiers inférieurs à un entier n donné, on peut utiliser le **crible d'Ératosthène**.

  On procède par élimination des multiples stricts des nombres premiers p_i inférieur ou égal à $\sqrt{n}$ sur la liste des entiers de 2 à n.

- **Les nombres de Mersenne** : On pose $M_n = 2^n - 1$.

  Proposition (exos bac) : Si M_n est premier alors n est premier.

  ⚠ La réciproque est fausse malheureusement. Contre-exemple : Si $n = 11$ alors n est premier, mais $M_{11} = 2047 = 23 \times 89$ n'est pas premier.

Infinité des nombres premier

ROC : Il existe une infinité de nombres premiers.

Démonstration par l'absurde, proche de celle d'Euclide en son temps. On suppose qu'il existe un nombre fini n de nombres premiers, on établit alors que le nombre $N = p_1 p_2 \dots p_n + 1$ est aussi premier ce qui est contradictoire avec l'hypothèse de départ.

Théorème de Gauss sur les nombres premiers

Divisibilité : Soit p un nombre premier.

Si p divise ab alors p divise a ou p divise b.

En particulier :

si p divise a^n alors p divise a et donc p^n divise a^n

Théorème fondamental de l'arithmétique

Tout entier naturel $n \geqslant 2$ peut se décomposer en produits de puissances de nombres premiers (à l'ordre des facteurs près).

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_m^{\alpha_m}$$

Exemple : $120 = 2^3 \times 3 \times 5$.

Remarque : Les nombres premiers apparaissent comme des briques élémentaires de l'arithmétique.

Diviseurs et nombres de diviseurs

- Tout diviseur d de n admet comme décomposition :
  $d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_m^{\beta_m}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$
- Le nombre N de diviseurs de n est égal à :
  $N = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$

Exemple : 120 a $N = (3+1)(1+1)(1+1) = 16$ diviseurs.

Retour au pgcd et ppcm

- Le pgcd de 2 entiers naturels s'obtient en effectuant le produit de tous les facteurs premiers communs aux 2 décompositions affectés du plus petit exposant.

$$\begin{cases} 126 = 2 \times 3^2 \times 7 \\ 735 = 3 \times 5 \times 7^2 \end{cases} \Rightarrow \text{pgcd}(126, 735) = 3 \times 7 = 21$$

- Le ppcm de 2 entiers naturels s'obtient en effectuant le produit de tous les facteurs premiers contenus dans l'une au moins des décompositions des 2 entiers affectés du plus grand exposant.

$$\text{ppcm}(126, 735) = 2 \times 3^2 \times 5 \times 7^2 = 4410.$$

Ce qui sert parfois dans les exercices

1) Interpréter astucieusement une hypothèse : soit n un nombre premier $\geqslant 5$.

On en déduit que $n \neq 3$ et comme n est premier, il n'est pas divisible par 3.
Ainsi $n \equiv 1\ (3)$ ou $n \equiv 2\ (3)$.
Cela aide parfois à débuter un exercice.

2) Éduquer son œil : somme des termes d'une suite géométrique $S_n = \dfrac{1-q^{n+1}}{1-q}$

- $2^n - 1 = \dfrac{2^n-1}{2-1} = \dfrac{1-2^n}{1-2} = 1+2+2^2+\cdots+2^{n-1}$
- $\dfrac{4^n-1}{3} = \dfrac{4^n-1}{4-1} = \dfrac{1-4^n}{1-4} = 1+4+4^2+\cdots+4^{n-1} \quad \Leftrightarrow$
  $4^n - 1 = 3(1+4+4^2+\cdots+4^n)$.
  Donc 3 divise $4^n - 1$ et donc non premier si $n \neq 1$
- Plus généralement $\dfrac{2^{pq}-1}{2^p-1} = 1+2^p+2^{2p}+\cdots+2^{p(q-1)} \quad \Leftrightarrow$
  $(2^p)^q - 1 = (2^p-1)\left(1+2^p+2^{2p}+\cdots+2^{p(q-1)}\right)$

Culture : le système RSA

Le système R.S.A., provient des initiales des noms de ses inventeurs américains en 1977 : Ronald Rivest, Adi Shamir et Leonard Adleman.

Le chiffrement RSA est asymétrique : il utilise une paire de clés (des entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. Les deux clés sont créées par une personne, Alice, qui souhaite que lui soient envoyées des données confidentielles. Alice rend la clé publique accessible. Cette clé est utilisée par ses correspondants (Bob, etc.) pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à Alice, et lui permet de déchiffrer ces données. La clé privée peut aussi être utilisée par Alice pour signer une donnée qu'elle envoie, la clé publique permettant à n'importe lequel de ses correspondants de vérifier la signature.

Une condition indispensable est qu'il soit « calculatoirement impossible » de déchiffrer à l'aide de la seule clé publique, en particulier de reconstituer la clé privée à partir de la clé publique (produit de deux nombres premiers suffisamment grands pour qu'il ne soit pas cassé).

Le petit théorème de Fermat

(Théorème désormais hors programme)

Soit un nombre premier p et un naturel a non multiple de p alors : $a^{p-1} \equiv 1\ (p)$

Exemple : Très utilise pour la divisibilité
Prouver que : $\forall n \in \mathbb{N},\ 3^{6n} - 1$ est divisible par 7.

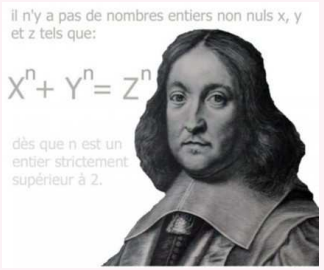
7 est premier et 3 non divisible par 7 donc $3^{7-1} \equiv 1\ (7) \Leftrightarrow 3^6 \equiv 1\ (7) \Leftrightarrow$
$(3^6)^n \equiv 1^n\ (7) \Leftrightarrow 3^{6n} - 1 \equiv 0\ (7)$.

Et le « Grand théorème de Fermat » : « Étant donné un entier $n \geqslant 3$, il est impossible de trouver 3 entiers naturels x, y et z non nuls tels que $x^n + y^n = z^n$. »

Pendant trois siècles, ce résultat a résisté aux mathématicien ou mathématicienne (Sophie Germain) les plus brillant(e)s jusqu'en 1994 où Andrew Wiles fit de la conjecture de Fermat un « vrai » théorème.

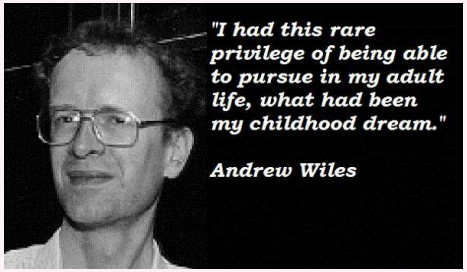
Pour le cas $n = 2$, connu depuis la plus haute l'antiquité, on connaît les entiers 3, 4, 5 qui donne $3^2 + 4^2 = 5^2$. Ces entiers particuliers sont connus sous le nom de triplets pythagoriciens qui sont en nombre infini.

Quelques portraits



Pierre de Fermat (1601-1665)

Sophie Germain (1776-1831)



Andrew Wiles (né en 1953)