Des nombres remarquables

SOMMAIRE :

1) Nombres de Fermat

Ce sont les nombres de la forme $2^{2^n} + 1$, notés F_n, où n est un entier naturel.
Ils ne sont pas tous premiers, d'ailleurs on ne sait pas s'il y en a une infinité de premiers ni une infinité de non premiers.
de F_0 à F_4 premiers
de F_5 à F_{32} non premiers
F_{33} on ne sait pas encore

Si $n \neq n'$ Alors F_n *et* $F_{n'}$ sont premiers entre eux (théorème de Goldbach)

La conjecture de Goldbach, pas encore démontrée et énoncé en 1742 est :
« Tout nombre entier pair supérieur à 3 peut s'écrire comme la somme de 2 nombres premiers »

Soit k entier naturel $x=2^k + 1$ premier $\Rightarrow k=2^n$ où n est un entier naturel (réciproque fausse !)
$\Rightarrow$x est nombre de Fermat

Retour au sommaire

2) Nombre de Mersenne

Ce sont les nombres premiers de la forme 2^p-1 où p est premier.
On note M_k le k-ième nombre de Mersenne.
Si note $A_p=2^p-1$ alors
$M_1=A_2=3$
$M_2=A_3=7$
$M_3=A_5=31$
$M_4=A_7=127$
mais $M_5 \neq A_{11}$ car $A_{11}=2047=23x89$ donc non premier

On a aussi la propriété suivante :
2^n-1 premier$\Rightarrow$ n premier

Autrement dit, parmi les nombres de la forme 2^n-1 où n est un entier naturel, il y a 3 catégories :

n non premier et alors 2^n-1 n'est pas premier
n est premier et $2^n-1 = A_n$ n'est pas premier
n est premier et $2^n-1 = A_n$ est un nombre de Mersenne c'est à dire premier

Retour au sommaire

3) Nombres parfaits

Ce sont les entiers naturels qui sont égaux à la somme de leurs diviseurs propres positifs
Par exemple 6 est parfait car 6=1+2+3
où encore 2 305 843 008 139 952 128 (découvert par Leonhard Euler)
Voilà une méthode pour générer des nombres parfaits :

"Lorsque la somme d'une suite de nombres doubles les uns des autres est un nombre premier, il suffit de multiplier ce nombre par le dernier terme de cette somme pour obtenir un nombre parfait."

1+2=3 qui est premier donc 2x3=6 est parfait.
1+2+4=7 qui est premier donc 4x7=28 est parfait.
1+2+4+8=15 n'est pas premier.
1+2+4+8+16=31 est premier donc 16x31=496 est parfait.

En découle une formule qui porte aujourd'hui le nom de **Formule d'Euclide** :
$2^{p-1}(2^p - 1)$ est parfait si p et (2p - 1) sont premiers.

Actuellement, 40 nombres parfaits sont connus. Le plus grands possède 12 640 858 chiffres et est égal à :
$2^{20\,996\,010}(2^{20\,996\,011}-1)$.
Et on ne sait pas s'il y en a une infinité

Retour au sommaire

4) Nombres pseudo premiers

Un petit rappel sur le petit théorème de Fermat :
Soit p un nombre premier et a un entier premier avec p alors $a^{p-1} \equiv 1(p)$
ou encore p divise $a^{p-1}-1$
a est premier avec p quand a n'est pas un multiple de p, en particulier quand a est dans {2,3,.., p-1}

Mais attention, la réciproque est fausse !
(C'est bien dommage car sinon nous aurions eu un critère pour reconnaître si un nombre est premier.)
Les nombres qui contredisent la réciproque du petit théorème de Fermat sont les nombres de Carmichaël.
C'est-à-dire des nombres p non premiers tels que, pour tout a dans {2,3,.., p-1},
p divise $a^{p-1}-1$.
Le plus petit est 561=3x11x17.
Remarquez que la vérification risque d'être fastidieuse à cause des puissances à calculer.
Ils sont cependant rares, plus rares que les nombres premiers mais cependant il y en a une infinité (Théorème de Granville en 1994).
Il y a 245 nombres de Carmichael pour 78494 nombres premiers inférieurs à 10^6 (proportion de 3 pour 1000)

Maintenant changeons un peu la définition :
Considérons un nombre p non premier tel que p divise $a^{p-1}-1$ pour une valeur particulière de a dans {2,3,.., p-1}
(On a changé « pour tout a » par « un a particulier »
Ces nombres sont les nombres de Poulet ou a-pseudo premiers ou pseudo premiers de base a.
Par exemple 341 est le plus petit pseudo-premier de base 2.
Les nombres de Carmichaël et les nombres de Poulet sont les nombres pseudo premiers, c'est-à-dire des nombres qui ne sont pas premiers et qui « contredisent en partie » la réciproque du théorème de Fermat.
Un nombre de Carmichael est donc un pseudo premier de base a pour tout a dans {2,3,.., p-1}.

Mais pourquoi les appelle-t-on pseudo premier ?
Prenons le problème à l'envers, c'est-à-dire considérons un entier p dont on ne sait pas s'il est premier ou pas.
Effectuons les calculs a^{p-1}-1 pour a dans {2,3,.., p-1}.

- si, pour une valeur de a, p ne divise pas a^{p-1}-1 alors p n'est pas premier (c'est la contraposée du théorème de Fermat)
- sinon , pour tout a dans {2,3,.., p-1}., p divise a^{p-1}-1 alors soit p est premier soit p est un nombre de Carmichaël et comme la proportion de nombres de Carmichaël par rapport aux nombres premiers est très faible, il est fort probable qu'il soit premier (99,9..% de chance)

Bien sûr il y a trop de calculs à effectuer et on pourrait alors se contenter de prendre a=2 mais dans ce cas la probabilité diminue car la proportion de nombres pseudo premiers de base 2 par rapport aux nombres premiers est plus importante.

D'où l'idée d'un compromis entre précision et calcul en prenant 4 valeurs de a ou 4 témoins: 2, 3, 5,7 (Test de Fermat)
Ce test consiste à choisir un nombre p et à effectuer les 4 calculs : 2^{p-1}-1, 3^{p-1}-1 ,5^{p-1}-1 ,7^{p-1}-1
Si p divise ces 4 nombres il y aura une forte probabilité que p soit premier. Mais ce n'est pas certain !

Les nombres de Chernik sont des nombres de la forme (6n+1)(12n+1)(18n+1) dont les 3 facteurs 6n+1 , 12n+1 , 18n+1 sont premiers .
Ce sont des nombres de Carmichaël !

Retour au sommaire

5) Nombres premiers

Il y a des livres entiers consacrés aux nombres premiers et ce n'est pas quelques paragraphes qui pourront les résumer.
Les nombres premiers bien connus : 2, 3, 5, 7,11... sont essentiels.

Du point de vue théorique :
Ce sont les briques, les atomes qui permettent de reconstituer tous les autres entiers.
En effet un nombre premier n'est pas décomposable en produit de 2 entiers autres que 1 et lui-même.
Tout entier est soit premier soit décomposable en produit d'au moins 2 nombres premiers et cette décomposition est unique (nombre composé)
Par exemple 12=2x2x3
Autrement dit tout entier est soit premier soit composé (de nombres premiers).
On comprend l'importance de ces nombres.

Il y en a une infinité et le fait qu'ils ne soient pas décomposables leur confère tout un tas de propriétés intéressantes :
Deux nombres premiers distincts sont premiers entre eux.
Un nombre premier p est premier avec tout entier qui n'est pas un multiple de p.
Un nombre premier p divise a^{p-1}-1 ($a^{p-1}\equiv 1(p)$) pour tout a dans {2,3,.., p-1}.
L'ensemble des restes modulo p muni de + et x est un corps, en particulier,
soit a dans {1,2,3,.., p-1} il existe b dans {1,2,3,.., p-1} tel que $ab\equiv 1(p)$

(Remarque : les nombres premiers entre eux interviennent dans les théorèmes
de Gauss « si a divise bc et a premier avec b alors a divise c »
et de Bezout « a et b sont premiers entre eux si et seulement si il existe au moins un couple d'entiers (u,v) tel que au+bv=1 »)

On a une assez bonne idée de la répartition des nombres premiers.
En notant $\pi(x)$, le nombre de nombres premiers inférieurs ou égaux à x on a :
$\pi(x) \sim x/\ln(x)$, quand $x \to +\infty$
Par exemple pour x=100 000 000 il y a à peu près 5 428 681 nombres premiers inférieurs à x en utilisant cette formule (il y en a en fait 5 761 455)

On a aussi ce résultat par Felgner en 1990 : $0{,}91\, n \ln(n) < p_n < 1{,}7\, n \ln(n)$ où p_n désigne le n-ième nombre premier.

Du point de vue pratique :
Voici quelques exemples :

Cryptage RSA
L'idée est de coder un message (par exemple un nombre) en un autre message (un autre nombre).
Pour cela on dispose de 2 clés publiques dont une est n.
Tout le monde peut alors coder.
Mais personne peut décoder, c'est à dire retrouver le message d'origine à partir du message codé.
Cela vient du fait que n est le produit de 2 grands nombres premiers p et q distincts.
n est donné mais pas p ni q.
Pour décoder il faudrait connaître p et q or pour de très grands nombres on ne sait pas en un temps raisonnable décomposer n en pq même avec des machines puissantes.
Par exemple en prenant n constitué de 1024 chiffres binaires soit à peu près 308 chiffres décimaux, c'est impossible actuellement.
On a pu factoriser un entier de 768 bits en 2 ans et demi avec des ressources informatiques importantes.

Maintenant reste le problème de la création de ces clés donc de génération de grands nombres premiers.
C'est là qu'interviennent les pseudo premiers ou plus exactement des nombres dont il est fort probable qu'ils soient premiers et qui sont générés rapidement.

En cryptographie, les nombres premiers sont essentiels.

Clef de contrôle
Dans un numéro de sécurité sociale ou un numéro compte bancaire il y a 2 chiffres terminaux que l'on appelle la clef.
On la calcule en faisant 97 moins le reste de la division euclidienne par 97 du nombre avant ces 2 chiffres.
Cette clef permet de contrôler des erreurs (pas toutes) lors de la saisie informatique de ces numéros.
Quand il y a une erreur de saisie un message apparait et la signale.
L'efficacité repose sur le fait que 97 est le plus grand nombre premier inférieur à 100.

Retour au sommaire