N° : 05 / PGS-2004 / MT

République Algérienne Démocratique et Populaire

Université des Sciences et de la Technologie Houari Boumediene

Faculté des mathématiques

Mémoire de Post-Graduation Spécialisée en Mathématiques

Spécialité : Cryptologie

Présenté par

Monsieur : Mustapha Mohamed

Sujet :

Quelques Aspects sur Les Nombres Premiers

Soutenu le : 25 / 03 / 2004

Devant le jury composé de :

M r : BENTINA Kamel, professeur, USTHB — **Président**

M r : ZITOUNI Mohamed, Professeur, USTHB — **Directeur du mémoire**

M r : HACHAICHI Mohamed .S, Maître de Conférences, USTHB — **Examinateur**

M r : HAMITI Hassan, D.G.S.C.T, — **Examinateur**

Table des Matières

Nombres Premiers et Applications

1. Introduction

Il s'agit des nombres premiers de l'anneau Ù des entiers rationnels.

Par convention, les ensembles de nombres sont désignés par les symboles :

ô = ensemble des nombres entiers naturels .

Ù = anneau des nombres entiers rationnels .

Ð = corps des nombres rationnels.

Ñ = corps des nombres réels.

Â = corps des nombres complexes.

Les entiers naturels forment un sous ensemble ô de Ù , qui n'est ni un sous anneau, ni un sous groupe de Ù ; c'est un monoïde.

La divisibilité et l'arithmétique classent les entiers rationnels en deux parties :

Les nombres premiers et **les nombres composés**

Définition 1 : *Un nombre premier dans l'anneau Ù , est un entier divisible seulement par 1 et lui-même.*

Un nombre composé est un entier qui admet, au moins, un diviseur premier autre que 1 et lui-même.

Exemples : 2,3,5,7,11 et 13 sont premiers tandis que 4,6,8,9 et 10 sont composés .

Proposition 1 : *L'ensemble des nombres premiers est infini*

Preuve : On utilise un raisonnement par l'absurde

Supposons que l'ensemble Ï des nombres premiers est fini (1)

Donc 2 est le plus petit élément de Ï, par l'ordre naturel de ô; soit p le plus grand élément de Ï :

$2 < 3 < 5 < 7 < 11 < 13 < \ldots < p$ (2)

Considérons le nombre entier N égal à la somme de 1 et du produit de tous les éléments de Ï :

$N=1+2\times3\times5\times7\times11\times\ldots\times p$, (3)

L'arithmétique implique que N n'est divisible par aucun nombre premier contenu dans Ï.

Il en résulte que N est premier (4).

La relation (3) implique l'inégalité $p < N$, donc N est premier non contenu dans Ï, (5).

(5) est en **contradiction** avec la supposition (1),

Il en résulte que cette supposition (1) est absurde ; donc

L'ensemble des **nombres premiers est infini.**

□

Corollaire

Dans l'anneau Ù □ des entiers rationnels, tout entier n se factorise, de façon unique à l'ordre prés des facteurs sous forme :

$n = \pm p_1^{n1} \times \ldots \times p_r^{nr}$,

Où $p_1, \ldots p_r$ sont des nombres premiers et $n_1, \ldots n_r$, des exposants entiers positifs .

C'est le théorème fondamental de l'arithmétique.

□

La détermination des nombres premiers de 2, 3 et 4 chiffres s'obtient par la méthode du crible :

On barre successivement les multiples de 2, 3, 5, 7,…

Il reste des nombres non barrés ; ce sont des nombres premiers.

Pour des nombres de plus de 10 chiffres, il faut trouver un algorithme applicable à un ordinateur puissant ; ce sont en général des équipes qui s'attaquent à ces calculs.

Exemple : crible d' Eratosthène

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Les nombres non barrés :

2,3,5,7,11,13.17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97 sont des **nombres premiers**

2 Distribution des nombres premiers

La distribution des nombres premiers, dans l'ensemble ô , est irrégulière.
Elle est mesurée par la fonction arithmétique pi de x, pour tout nombre réel x >2.

$\Pi(x) = \sum_{p \leq x} 1$, pour tout nombre premier $p \leq x$

Cette fonction pi de x, évalue le nombre de nombres premiers p ≤ x.

La fonction arithmétique [x] : " plus grand entier d'un nombre réel x "
Satisfait plusieurs relations ; en voici quelques unes :

(1) [x] ≤ x < [x+1]

(2) x-1 < [x] ≤ x

(3) [x]+[y] ≤ [x+y] ≤ [x] + [y] +1

(4) [x] + [-x] = 0 si x est entier, -1 si non

Exemples :

[3,52] = 3 ; [-3.52] = -4, d'après (1)

[6,387]+ [-6,387] = 6-7 = -1, d'après (4)

[7,86]+ [12,53]= 7+12 = 19 et [7,86 + 12,53] = [20,39] = 20 d'où

[7,86] + [12,53] + 1 = [7,86+12,86] , d'après (3)

Cette fonction arithmétique permet de calculer la plus grande puissance p^h , d'un nombre premier p,qui divise un entier N.

Théorème

Soit p^h , la plus grande puissance d'un nombre premier p, qui divise factorielle n ! = N.
Alors, la fonction arithmétique : " plus grand entier [x] d'un nombre réel x satisfait "

$h = [\frac{n}{p}] + [\frac{n}{P^2}] + \ldots + [\frac{n}{P^r}]$

Exemple :

Algorithme de calcul de la plus grande puissance 7^h qui divise N = 1000 !

Calcul de [1000/7]= a_1 ; je trouve $a_1 = 142$

Calcul de [a_1 / 7] = a_2 ; je trouve $a_2 = 20$

Calcul de [a_2 / 7] = a_3 ; je trouve $a_3 = 2$

Calcul de [a_3 / 7] = a_4 ; je trouve $a_4 = 0$

Par application du Théorème, je trouve la plus grande puissance 7^h , qui divise 1000 !

C'est $7^{142+20+2} = 7^{164}$

Le calcul montre que 7^{165} ne divise pas 1000 !

Cet algorithme de calcul de l'exposant h dans la puissance maximale p^h qui divise N = n ! , peut être utilisé pour l'inégalité de Tchebicheff

Proposition 2 :

Il existe deux constantes a et b positives qui satisfont, pour un nombre réel x fini, la double inégalité

$$\frac{ax}{\log x} < \Pi(x) < \frac{bx}{\log x}$$

C'est un théorème de Tchebicheff (1850)

Preuve :

Considérons le coefficient du binôme

$$N = \left[\begin{matrix} 2n \\ n \end{matrix} \right] = \frac{2n\,(2n-1)\ldots(n+1)}{n\,!} = \frac{(2n)\,!}{(n\,!)(n\,!)} \quad ; \quad (1)$$

Soit un nombre premier p, et $p^{h(p)}$ la plus grande puissance de p qui divise N ; (2)

(1) et le Théorème précédent impliquent l'exposant h (p) :

$$h(p) = \sum_{i \geq 1} \left(\left[\frac{2n}{p^i} \right] - 2 \left[\frac{n}{p^i} \right] \right) ; \quad (3)$$

L'entier 2n est encadré par les puissances de p

$$p^{r(p)} \leq 2n \leq p^{r(p)+1} \quad ; \quad (4)$$

(3) et (4) impliquent l'inégalité

$$h(p) \leq r(p) \quad ; \quad (5)$$

Il en résulte que $\binom{2n}{n}$ divise le produit $\prod_{p \leq 2n} p^{r(p)}$ (6)

Considérons l'inégalité double $n < p \leq 2n$; alors

p divise (2n) ! et p ne divise pas n ! (7)

Il en résulte que $\left(\prod_{n<p \leq 2n} p\right)$ divise $\binom{2n}{n}$ et que le coefficient du binôme $\binom{2n}{n}$

est encadré par :

$$\prod_{n<p \leq 2n} p \leq \binom{2n}{n} \leq \prod_{p \leq 2n} p^{r(p)} \leq \prod_{p \leq 2n} (2n) \quad (8)$$

Remplaçons p par n dans (8) ; nous obtenons l'encadrement :

$$n^{\Pi(2n) - \Pi(n)} \leq \binom{2n}{n} \leq (2n)^{\Pi(2n)} \quad (9)$$

Le coefficient du binôme $\binom{2n}{n}$ satisfait les deux inégalités

$\binom{2n}{n} \leq (1+1)^{2n} = 2^{2n}$, (10-1) et

$$\binom{2n}{n} = \frac{(2n)(2n-1)\ldots(n+1)}{n!} = \prod_{1 \leq i \leq n} \frac{n+i}{i} \geq \prod_{i} 2 = 2^n \; ; \; (10\text{-}2)$$

Ces deux inégalités dans (9) et les logarithmes des deux nombres impliquent les deux inégalités :

$$\Pi(2n) - \Pi(n) \leq \frac{2n.\log 2}{\log n} \text{ et } \Pi(2n) \geq \frac{n.\log 2}{\log 2n} \qquad (11)$$

Pour tout nombre réel x encadré par : $2n \leq x < 2n+2$, ces inégalités (10) impliquent :

$$\Pi(x) \geq \Pi(2n) \geq \frac{n.\log 2}{\log 2n} \geq \frac{n.\log 2}{\log x} > \frac{\log 2}{4} \frac{x}{\log x} \quad ; \quad (12)$$

Pour la borne b du Théorème de **Tchebicheff,** nous prenons les valeurs :
$2n = 2^r$, pour $r \geq 3$; alors :

$$\Pi(2^r) - \Pi(2^{r-1}) \leq \frac{2^r}{r-1} \qquad (13)$$

Remplaçons r par les entiers r= 2i, 2i-1,…,3 et additions les inégalités (13) ainsi obtenues, pour $i \geq 2$

$$\Pi(2^{2i}) < \frac{2^{2i+2}}{i} \quad \text{soit} \quad \frac{\Pi(2^{2i})}{2^{2i}} < \frac{4}{i} \qquad (14)$$

Pour tout réel x encadré par : $2^{2i-2} < x \leq 2^{2i}$, (14) implique :

$$\frac{\Pi(x)}{x} \leq \frac{\Pi(2^{2i})}{2^{2i-2}} = \frac{4\Pi(2^{2i})}{2^{2i}} , \quad (15)$$

D'où les inégalités :

$$\frac{4}{i} \leq \frac{8\log 2}{\log x} \quad \text{et}$$

$$\frac{\Pi(x)}{x} < \frac{16}{i} \leq \frac{32\log 2}{\log x} \quad ; \quad (16)$$

Nous en déduisons l'encadrement

$$\frac{\log 2}{4} \cdot \frac{x}{\log x} < \Pi(x) < 32 . \log 2 . \frac{x}{\log x}$$

□

L'approximation asymptotique de $\Pi(x)$ est la :

Proposition 3 :

La fonction arithmétique $\Pi(x)$ *satisfait*

$$\lim_{x \to \infty} \Pi(x) . \frac{\log(x)}{x} = 1$$

C'est un théorème prouvé par **: Hadamard et lavallée Poussin en 1896.**

□

On en déduit le corollaire

Corollaire

1) la fonction $\Pi(N)$, pour un nombre N, satisfait

$$\Pi(N) \approx \frac{N}{\log(N)}$$, où ≈ signifie " proche de "

C'est le théorème des nombres premiers

2) la probabilité d'un entier a<N d'être premier est égale à

$$p(a) = \frac{1}{\log(N)}$$

□

Signalons que les valeurs de la fonction Π (x) ont été tabulées
pour de grande valeur de x

Exemples :

1) Π (100) = 25

2) Π (2^{25}) = 2063689

3) Π (10^{10}) = 455052511

4) Π (3^{21}) = 475023803

5) Π (7^{10}) = 15353323

6) Π (5^{18}) = 136575061279

7) Π (7^{15}) = 168650876819

8) Π (11^{10}) = 1131108518

9) Π (17^{11}) = 1137480672389

10) Π (10^{21}) = 21127269486018731928 (nombre de 20 chiffres)

3 Nombres entiers pourvus de propriétés particulières

Ils sont nombreux et portent souvent les noms de mathématiciens qui les ont étudiés : **Fermat, Mersenne Carmichael, Lucas, Fibonacci**, etc.…

3.1 Nombres de Fermat (1637)

Définition 2 :

Le n-ème nombre de Fermat est l'entier naturel

$$F_n = 2^{2^n} + 1$$

Exemples :

$F_1 = 5$, $F_2 = 17$, $F3 = 257$, $F4 = 65537$, $F_5 = 4294967297$

$F_5 = 641 \times 6700417$, $F_6 = 274177 \times 67280421310721$

$F_7 = 59649589127497217 \times 5704689200685129054721$

Proposition 4 :

Si le nombre $2^n + 1$ *est premier impair, alors n est une puissance de 2 et*

$$2^n + 1 = 2^{2^s} + 1 = F_s$$

est le s-ème nombre de Fermat.

□

Proposition 5 (Euler) :

Pour tout entier $n \geq 2$, *tout facteur premier p du n-ème nombre de Fermat*

$$F_n = 2^{2^n} + 1$$

satisfait la congruence $p \equiv 1 \bmod 2^{n+2}$.

□

Il existe un test de reconnaissance des nombres de Fermat qui sont premiers.

Proposition 6 *: Pour tout entier n≥1, le nombre de Fermat*

$$F_n = 2^{2^n} + 1$$

est premier si et seulement si il satisfait la congruence :

$$3^{(F_n-1)/2} \equiv -1 \bmod F_n$$

□

La notion de "nombre pseudo premier " s'applique aux nombres de Fermat

Définition 3 *Un nombre composé n est pseudo premier de Fermat de base a s'il satisfait la congruence*

$$a^n \equiv a \bmod n$$

Cette congruence, pour n premier, implique la :

Proposition 7 (petit théorème de Fermat) :

Si p est premier, alors tout entier a premier à p satisfait la congruence

$$a^{p-1} \equiv 1 \bmod p .$$

□

Exemple1 :

$3^{91} \equiv 3 \bmod 91$, et " 91 est composé " impliquent que le nombre composé 91 est un **pseudo premier de Fermat** de base 3

Exemple2 :

$2^{340} \equiv 1 \bmod 341$, et " 341 est composé " impliquent que le nombre composé 341 est un **pseudo premier de Fermat** de base 2.

Corollaire : Pour chaque entier a, il existe une infinité de pseudo premiers de Fermat de base a

□

3.2 Nombres de Mersenne (1640)

Définition 4 :

Le k-ème nombre de Mersenne, pour tout entier naturel k≥1 est l'entier

$$M_k = 2^k - 1$$

Exemples :

$M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15$, $M_5 = 31$

$M_6 = 63$, $M_7 = 127$, $M_8 = 255$, $M_{10} = 1025$

$M_{97} = 11447 \times 13842607235828485645766393$

$M_{151} = 18121 \times 55871 \times 165799 \times 2332951 \times 7289088383388253664437433$

Proposition 8 : Pour *k=2n, le k-ème nombre de Mersenne* M_k *est décomposé*

Preuve :

$M_k = 2^k - 1 = 2^{2n} - 1$, est une différence de deux carrés.

On en déduit : $M_k = (2^n+1) \times (2^n-1)$

□

Les nombres premiers de Mersenne donnent des nombres parfaits

Définition 5 : *Un nombre parfait est un entier naturel n égal à la demi somme de ses diviseurs*

Exemples :

1) a= 6 admet les diviseurs 1, 2, 3, 6 ; leur somme est égale à :
$o(6) = 12 = 2 \times 6$; Donc 6 est un nombre parfait.

2) n=28 admet les diviseurs 1, 2, 4, 7, 14, 28 ; leur somme est égale à

$\sigma(28) = 56 = 2 \times 28$; Donc 28 est un nombre parfait.

3) b=496 admet les diviseurs 1, 2, 4, 8, 16, 31, 62, 124, 248, 496 ; leur somme est égal à :

$\sigma(496) = 992 = 2 \times 496$; Donc 496 est un nombre parfait.

Proposition 9 :

Si le nombre de Mersenne $M_k=2^k-1$ *est premier, alors le nombre* $M= 2^{k-1} \times M_k$ *est parfait.*

Preuve :

On détermine les diviseurs de M.
Ensuite on applique la définition 5 d'un nombre parfait.

□

Proposition 10 :

Soit un nombre n parfait pair, alors il existe un nombre de Mersenne M_k *premier, qui satisfait :* $n=2^{k-1} \times M_k$.

□

Proposition 11 :

Si un nombre $M_k = 2^k - 1$ *de Mersenne est premier, alors k est premier.*

□

Corollaire :

Tout facteur premier p d'un nombre de Mersenne M_k , pour k premier , satisfait les congruences :

$p \equiv 1 \mod k$ et $p \equiv \pm 1 \mod 8$

□

Exemple1 :

Soit k = 3 alors $M_3 = 2^3 - 1 = 7$.

Ce nombre est premier, il satisfait les deux congruences :

$$7 \equiv 1 \mod 3 \quad \text{et } 7 \equiv -1 \mod 8.$$

Exemple2 :

Soit k = 11 ; alors $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$.

Le diviseur premier p = 23 satisfait les congruences

$23 \equiv 1 \mod 11$ et $23 \equiv -1 \mod 8$.

Le diviseur premier p = 89 satisfait les congruences :

$89 \equiv 1 \mod 11$ et $89 \equiv 1 \mod 8$.

3.3 Nombres de Carmichael

Définition 6 :

Un nombre de Carmichael est un nombre composé $N > 0$ *sans facteur carré tel que, pour tout entier positif* a *premier à* N, *il satisfait la congruence :*

$$a^{N-1} \equiv 1 \bmod N.$$

Ces nombres sont caractérises par la :

Proposition 12 :

Un entier composé $N > 0$ *est un nombre de Carmichael*
si et seulement si N *est le produit de nombres premiers distincts impairs* $p_1, p_2, \ldots p_k$, *(*$k > 3$*) , et* $N \equiv 1 \bmod p_i - 1$ *pour* $i = 1,2,\ldots k$

Preuve : On peut la trouver dans :

Chernick dans "on Fermat 's simple théorème", Bull Amer. Math .Soc 45(1938) p 268-274

□

Exemples :

Nombre de Carmichael avec 13 facteurs premiers

$N = 5 \times 13 \times 17 \times 19 \times 29 \times 37 \times 43 \times 67 \times 97 \times 113 \times 129 \times 317$

$M = 7 \times 11 \times 17 \times 19 \times 31 \times 37 \times 53 \times 61 \times 73 \times 79 \times 97 \times 131 \times 10369.$

Avec 14 facteurs premiers

$N = 11 \times 13 \times 17 \times 19 \times 29 \times 37 \times 41 \times 61 \times 71 \times 73 \times 113 \times 127 \times 20161$

$M = 5 \times 13 \times 17 \times 19 \times 37 \times 67 \times 73 \times 89 \times 97 \times 109 \times 113 \times 127 \times 139 \times 2437$

Voici un test de reconnaissance d'un nombre de Carmichael :

Proposition13 :

Un nombre composé N>0, sans facteur carré est de Carmichael
si et seulement si pour tout diviseur premier p de N, alors p-1 divise N-1.

□

3.4 Nombres de Lucas

Définition7 :

Les nombres de Lucas sont les nombres U_n définis par la relation de récurrence ternaire :

$U_{n+1}=U_n+U_{n-1}$ *et de premiers termes* $U_1=1$ $U_2=3$.

Les nombres consécutifs de Lucas jusqu' à 32 sont :

n	3	4	5	6	7	8	9	10	11	12
U_n	4	7	11	18	29	47	76	123	199	322
n	13	14	15	16	17	18	19	20	21	22
U_n	521	843	1364	2207	3571	5778	9349	15127	22476	39603
n	23	24	25	26	27	28	29	30	31	32
U_n	62079	101682	163761	265443	429204	694647	1123851	1818498	2942349	4760847

Définition 8 :

Un pseudo premier de Lucas est un nombre composé n qui satisfait les conditions suivantes :

Pgcd(n,2b Δ) =1 et $U_{n-(\frac{\Delta}{n})} \equiv 0 \bmod n$

Où f(x)= x^2-ax+b, Δ =a^2-4b, $\left(\frac{\Delta}{n}\right)$ = symbole de Legendre - Jacobi

$U_k = U_k(a, b) = \dfrac{x^k - (a-x)^k}{2x - a}$; $U_0 = 0$, $U_1=1$, $U_k=a \times U_{k-1} - b \times U_{k-2}$.

3.5 Nombres de Fibonacci

Définition 9 :

Les nombres de Fibonacci sont les termes de la récurrence ternaire

$U_{n+1}=U_n+U_{n-1}$ *et de premiers termes* $U_0=0$, $U_1=1$.

Exemple :

Les nombres consécutifs de Fibonacci jusqu' à 100 sont :

n	U_n	Factorisation de U_n
0	0	0
1	1	1
2	1	1
3	2	P, où p signifie premier
4	3	P
5	5	P
6	8	2×4
7	13	P
8	21	3×7
9	34	2×17
10	55	5×11
11	89	P
12	144	$2^4\times3^2$
13	233	P
14	377	13×29
15	610	$2\times5\times61$
16	987	$3\times7\times47$
17	1 597	P
18	2 584	$2^3\times17\times19$
19	4 181	P
20	6 765	$3\times5\times11\times41$
…		
23	28 657	P
29	514 229	P
31	1 346 269	557×2417
43	433 494 437	P
47	2 971 215 073	P
83	99 194 853 094 755 497	P
100	354 224 848 179 261 915 075	$3\times5^2\times11\times41\times101\times151\times401\times3001\times570601$

Proposition 14 :

Les nombres de Fibonacci satisfont les relations :

1) $\lim_{n \to \infty} \frac{U_{n+1}}{U_n} = \frac{1+\sqrt{5}}{2}$

2) $U_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$

3) $U_1 + U_2 + U_3 + \ldots + U_n = U_{n,+2} - 1$.

4) $U_{n+1}\ U_{n-1} = U_n{}^2 + (-1)^n$; pour tout entier $n \geq 1$.

5) $U_{m+n} = U_{m-1}\ U_n + U_m\ U_{n+1}$; pour toute paire d'entiers {m, n}.

□

Les nombres de Fibonacci satisfont la

Proposition15 :

Soit les nombres de Fibonacci $U_0=0$, $U_1=1$ et $U_{n+1}=U_n+U_{n-1}$

Alors ils satisfont la relation matricielle :

$$\begin{pmatrix} U_{n+1} & U_n \\ U_n & U_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

Preuve :

Avec la définition des nombres de Fibonacci et les propriétés des matrices carrées

□

Définition 10 :

Un nombre composé n est un pseudo premier de Fibonacci s'il satisfait la congruence ,

$U_{n-t_n} \equiv 0 \bmod n$, *où*

$$t_n = \begin{cases} 1 \text{ quand } n \equiv \pm 1 \bmod 5 \\ -1 \text{ quand } n \equiv \pm 2 \bmod 5 \\ 0 \text{ quand } n \equiv 0 \bmod 5 \end{cases}$$

donc t_n est le symbole de Legendre $(\frac{n}{5})$.

Exemple :

$n = 323 = 17 \times 19$, $t_{323} = -1$ impliquent $U_{n-tn} = U_{324}$

U_{324}=230414835855241682622209064896420180751016174667804967905736902899 68

$U_{324} \equiv 0 \bmod 323$, donc n= 323 est pseudo premier de Fibonacci.

4 Fonctions arithmétiques

4.1 Définition 11 :

Une fonction arithmétique est une application de l'ensemble ô *des entiers naturels dans l'ensemble* Â *des nombres complexes :*

$h : ô^{*} \rightarrow Â$

Une fonction h est additive si elle satisfait la formule

$h(m + n) = h(m) + h(n)$.

La fonction h est multiplicative si elle satisfait la formule

$h(m \times n) = h(m) \times h(n)$ *et* $h(1) \neq 0$.

Pour tout paire d'entiers m et n positifs et premiers entre eux.

Il y a des fonctions arithmétiques associées aux diviseurs d'un entier n : $\tau(n)$, $\sigma(n)$, $\sigma_k(n)$, …

4.2 Exemples

1) $\tau(n)$ est le nombre de diviseurs positifs de n

2) $\sigma(n)$ est la somme des diviseurs positifs de n

3) $\sigma_k(n)$ est la somme des puissances k-èmes des diviseurs positifs de n

Tableau de quelques valeurs :

n	1	2	3	4	5	6	7	8	9	10
$\tau(n)$	1	2	2	3	2	4	2	4	3	4
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18
$\sigma_2(n)$	1	5	10	21	26	50	50	85	91	130

Nous ferons un exposé bref de la fonction **Möbius**, de la fonction **d'Euler** et de la fonction **Zêta** de Riemann.

4.3 Fonction de Möbius

Définition 12 :

La fonction de ***Möbius*** *est la fonction arithmétique* $\mu(n)$
définie par ses valeurs

$$\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si n a un facteur carré} \\ (-1)^r \text{ si } n = p_1 \times p_2 \ldots \times p_r = \text{ produit de r facteurs premiers} \end{cases}$$

Cette fonction μ est multiplicative

Tableau de quelques valeurs $\mu(n)$

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

La fonction de Möbius possède plusieurs propriétés

Proposition 16 :

La fonction arithmétique $\mu(n)$ *de Möbius satisfait*

$\sum_{d/n} \mu(d) = 0$, pour $n > 1$ où le symbole d/n signifie" d divise n "

Preuve :

Soit un entier $n= p_1^{e1} \times \ldots \times p_r^{er}$, on en déduit l'ensemble des

diviseurs d de n, d= 1, p_1 ,…, p_r ,p_1^2 …, p_r^{er},…

La fonction de Möbius est nulle pour les diviseurs contenant un carré

Pour un facteur premier μ (p)=-1, il faut donc un raisonnement par récurrence sur le nombre de facteurs premiers pour démontrer la formule $\sum_{d/n} \mu(d) = 0$

□

Proposition 17 :

Soit une fonction arithmétique f (n) et la fonction associée

F (n) = $\sum_{d/n}$ *f (d), pour tout entier naturel n*

Alors : *f (n) =* $\sum_{d/n}$ *μ (d).F (n/d)*

Preuve :

C'est la formule d'inversion de Möbius

□

4.4 Fonction arithmétique d'Euler

Définition 13 :

La fonction φ (n) ***d'Euler*** *est la fonction* ***arithmétique qui compte le nombre des entiers a premiers à n*** *et inférieurs à n, et qui vaut* φ (1) =1 *pour* n=1.

Tableau de quelques valeurs de φ (n)

n	2	3	4	5	6	7	8	9	10	25
φ(n)	1	2	2	4	2	6	4	6	4	20

Proposition 18 :

La fonction φ (n) *d'Euler satisfait* :

1) $\varphi(m \times n) = \varphi(m) \times \varphi(n)$ si m et n sont premiers entre eux

2) $\varphi(p^e) = p^e - p^{e-1} = (p-1) \times p^{e-1}$ pour tout nombre premier p et $e \geq 1$

3) $\varphi(2^e) = 2^{e-1}$ pour $e \geq 1$ et $\varphi(2.n) = \varphi(n)$, pour tout entier impair n

4) pour tout entier $n>1$ $\varphi(n) = n \times \prod_{p/n} (1 - \frac{1}{p})$, où p décrit les facteurs premiers de n

5) $\sum_{d/n} \varphi(d) = n$

□

Corollaire : pour tout entier $n \geq 3$, $\varphi(n)$ est pair

□

4.5 Fonction Zêta de Riemann

Définition 14 : *La fonction* ***Zêta de Riemann*** *est la fonction de la variable complexe s*

z : Â → Â , de valeur

$$\mathbf{z}(s) = \mathbf{S}_{n \geq 1} \frac{1}{n^s}$$ où *n* parcourt les entiers naturels.

Cette fonction Zêta se met sous la forme d'un produit infini

Proposition 19

La fonction Zêta de Riemann se met sous la forme du produit eulérien

$\zeta(s) = \prod_{p} (1-p^{-s})^{-1}$, où p *parcourt l'ensemble des nombre premiers* Ï

Preuve :

On utilise la factorisation de l'entier naturel $n = p_1^{n_1} . p_2^{n_2} \ldots . p_r^{n_r}$

$$n^s = \left(p_1^{n_1} . p_2^{n_2} \ldots . p_r^{n_r} \right)^s = p_1^{s\,n_1} . p_2^{s\,n_2} \ldots . p_r^{s\,n_r}$$

□

Riemann a calculé quelques zéros de la fonction $\zeta(s)$; il a conjecturé que tous les zéros non triviaux de $\zeta(s)$ ont une partie réelle Re(*s*) = 1/2

Cette droite x = 1/2 est la ligne critique de $\zeta(s)$
et l'hypothèse de Riemann est la conjecture de Riemann.
Cette fonction $\zeta(s)$ de la variable complexe *s* est liée à la fonction Gamma de *s* et aux nombres de Bernoulli.

$$\Gamma(s) = \int_0^{\infty} e^{-x} x^{s-1} dx \quad .$$

Dans les ouvrages spécialises (EDWARDS, Riemann's Zêta Function),
(TITCHMARCH, the Riemann Zêta Function)
On peut trouver une équation fonctionnelle de Riemann de la forme.

$$\zeta(s) = 2^s . \pi^{s-1} . \Gamma(1-s) . \zeta(1-s) . \sin(\pi s/2)$$

Et la formule de duplication de Legendre

$\Gamma(s).\ \Gamma(s+1/2) = 2^{1-2s}.\ \pi^{1/2}.\ \Gamma(2s)$

La fonction $\Gamma(s/2)$ admet pour zéros les entiers négatifs :-2, -4, -6,…
Ces zéros sont aussi zéros de la fonction Zêta **z** (s)

Définition 15 :

Les zéros triviaux de ***z*** *(s) sont les entiers pairs négatifs –2, -4, -6,…*
Pour calculer des zéros non triviaux de ***z*** *(s), on utilise un algorithme basé sur la forme du nombres complexes* ***z*** *(s) = a+ i b .*

A l'heure actuelle, cette conjecture de Riemann sur les zéros non triviaux de **z** (s) , n'est pas résolue
La fonction **z** (s) est liée à des fonctions arithmétiques comme μ (n)
Elle a été prolongée aux corps de nombres par la fonction Zêta de Dedekind.

4.6 Congruences dans l'anneau Ù

Définition 16 :

Soit un entier m ≥ 0, qui divise la différence a-b de deux entiers rationnels a et b.
Alors a et b sont ***congrus modulo*** *m.*
La relation $a \equiv b \bmod m$ *est une congruence de module m.*
Si a-b n'est pas divisible par m, alors a et b ne sont pas congrus module m :

$$a \not\equiv b \bmod m$$

Certaines propriétés des congruences modulo *m* sont rassemblées dans la

Proposition 20 :

Soient des entiers rationnels a, b, c, d, x, y et m > 0

1) a ≡ b mod m implique les congruences b ≡ a mod m et a-b ≡ 0 mod m .

2) a ≡ b mod m et b ≡ c mod m impliquent a ≡ c mod m

3) a ≡ b mod m et c ≡ d mod m impliquent ax + cy ≡ bx + dy mod m et ac ≡ bd mod m

4) pour tout diviseur p de m, a ≡ b mod m implique a ≡ b mod p .

5) ax ≡ ay mod m et a premier à m implique x ≡ y mod m .

□

La théorie des congruences dans l'anneau Z admet des applications ; nous en citons quelques unes

Théorème d'Euler 1

Si deux entiers a et b sont premiers entre eux, alors

$a^{\varphi(b)} \equiv 1 \bmod b$, où $\varphi(b)$ = fonction arithmétique d'Euler.

□

Théorème de Wilson 2

Tout nombre premier p satisfait la congruence

$(p-1)! \equiv -1 \bmod p$, où (p-1) ! = 1.2.3.4… (p-1)

□

Théorème 3

Pour tout nombre premier p la congruence $x^2 \equiv -1 \bmod p$

admet des solutions si et seulement si p =2 ou $p \equiv 1 \bmod 4$.

□

La congruence quadratique $x^2 \equiv a \bmod p$, p premier permet de définir le symbole de Legendre $\left(\frac{a}{p}\right)$

Définition 17 :

Toute solution a de la congruence quadratique $x^2 \equiv a \bmod p$, *p premier, est un* ***reste quadratique modulo p.***

Exemples

1) Les restes quadratiques mod 5 sont 1 et 4

2) Les restes quadratiques mod 17 sont 1, 2, 4, 8, 9, 13, 15, 16 ; il y en a huit (8).

3) Les restes quadratiques mod 29 sont 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25 et 28, il y en a 14.

Ces résultats se généralisent

Proposition 21

Soit un nombre premier p, alors le nombre de restes quadratiques mod p est égal à

$$\frac{p-1}{2} = \frac{\varphi(p)}{2}.$$

Le nombre de non restes quadratiques mod p est aussi égal à $\frac{p-1}{2}$

Preuve : les entiers a premiers à un nombre premier *p* sont les éléments non nuls du corps $Å_p$ fini.

Les restes quadratiques forment les carrés dans F_p ; l'ensemble quotient

$F_p^* / \{ x^2 , x \in F_p^* \}$, est d'ordre 2

□

Définition 18 :

Le symbole de ***Legendre*** $(\frac{a}{p})$ *d'un nombre premier p >2 est défini par ses valeurs*

$(\frac{a}{p})$ = *+1 si a est un reste quadratique modulo p.*

$(\frac{a}{p})$ = *-1 si a est non reste quadratique modulo p.*

$(\frac{a}{p})$ = *0 si a est multiple de p.*

Pour p =2, le symbole $(\frac{a}{2})$ *n'est pas défini.*

Proposition 22 :

Soit un nombre premier impair p et le symbole de Legendre $(\frac{a}{p})$; *alors* :

1) $(\frac{a}{p})(\frac{b}{p}) = (\frac{a.b}{p})$, $(\frac{a^2}{p}) = 1$, $(\frac{a^2.b}{p}) = (\frac{b}{p})$

2) $(\frac{-1}{p}) = (-1)^{(p-1)/2}$, et $(\frac{2}{p}) = (-1)^e$, avec $e = (p^2 -1) / 8$

3) $(\frac{a}{p}) \equiv a^{(p-1)/2} \bmod p$

Loi de réciprocité quadratique

Les symboles de Legendre modulo deux nombres premiers impairs p et q satisfont :

$(\frac{p}{q})(\frac{q}{p}) = (-1)^e$, avec $e = (p-1)(q-1)/4$.

□

Le symbole de **Legendre** se prolonge au symbole de **Jacobi** pour deux nombres entiers A et B premiers entre eux, $B = p_1^{e1} \ldots . p_r^{er}$ impair et positif.

Définition 19

Soit deux nombres A *et* B *premiers entre eux, et* $B = p_1^{e1} \ldots . p_r^{er}$ *, impair et positif*

Le symbole de **Jacobi** $\left(\frac{A}{B} \right)$ *est égal au produit des symboles de Legendre* :

$$\left(\frac{A}{B} \right) = \left(\frac{A}{P_1} \right)^{e_1} \ldots . \left(\frac{A}{p_r} \right)^{e_r} = \prod_i \left(\frac{A}{p_i} \right)^{e_i}$$

Proposition 23

Soit deux entiers impairs positifs B *et* B′ *et deux entiers rationnels A et* A′ *satisfaisant* pgcd (A × A′ , B × B′) =1 *alors les symboles de Jacobi satisfont les relations :*

1) $\left(\frac{A}{B} \right) \times \left(\frac{A}{B'} \right) = \left(\frac{A}{B.B'} \right)$ et $\left(\frac{A}{B} \right) \times \left(\frac{A'}{B} \right) = \left(\frac{A.A'}{B} \right)$

2) $\left(\frac{A^2}{B} \right) = \left(\frac{A}{B^2} \right) = 1$ et $\left(\frac{A.A'^2}{B.B'^2} \right) = \left(\frac{A}{B} \right)$

3) $\left(\frac{-1}{B} \right) = (-1)^{(B-1)/2}$ et $\left(\frac{2}{B} \right) = (-1)^{(B^2-1)/8}$

Loi de réciprocité quadratique

Soit deux entiers A et B impairs, positifs et premiers entre eux.

Alors les symboles de Jacobi satisfont :

$\left(\frac{A}{B} \right) \times \left(\frac{B}{A} \right) = (-1)^e$ avec e = (A-1). (B-1) / 4

□

Exemple Calcul du symbole de Jacobi $\left(\frac{105}{317}\right)$

105 = 3.5.7, est un nombre composé ; 317 est un premier. (1)

Loi de réciprocité $\left(\frac{105}{317}\right).\left(\frac{317}{105}\right) = (-1)^{104.317/4} = +1.$ (2)

Multiplions (2) par $\left(\frac{317}{105}\right)$

$\left(\frac{105}{317}\right).\left(\frac{317}{105}\right)^2 = \left(\frac{317}{105}\right)$ d'où $\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right)$ (3)

(3) implique $\left(\frac{317}{105}\right) = \left(\frac{317 - 3.105}{105}\right) = \left(\frac{2}{105}\right)$ (4)

Le symbole de Jacobi et (1) impliquent

$\left(\frac{2}{105}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{2}{7}\right) = (-1)(-1)(+1) = +1$

Par suite $\left(\frac{105}{317}\right) = +1.$

Théorème des restes chinois

Soient r entiers positifs $m_1,\ldots,m_r$ premiers entre eux 2 à 2, et r entiers rationnels $a_1,\ldots,a_r$
Alors le système de r congruences

$$x \equiv a_i \bmod m_i \quad \text{pour } i = 1, 2, 3 ,..., r .$$

admet une solution mod $m = m_1 . m_2 \ldots m_r$.

□

Corollaire

Une solution de r congruences $x \equiv a_i \bmod m_i$ est de la forme :

$$c = \sum_{1 \le i \le r} \frac{m}{m_i} b_i \times a_i \bmod m \quad avec \quad \frac{m}{m_i} \times b_i \equiv 1 \bmod m_i \quad pour \quad 1 \le i \le r$$

□

Exemple1 : résoudre le système de congruences

$$\begin{cases} x \equiv 2 \bmod 4 \\ x \equiv 3 \bmod 5 \\ x \equiv 4 \bmod 21 \end{cases}$$

Les 3 modules $m_1 = 4$, $m_2 = 5$, $m_3 = 21$ sont premiers entres eux 2 à 2 ; donc le théorème des restes chinois s'applique

On trouve la solution :

$c \equiv 2818 = 358 \bmod 420.$

Exemple2 : résoudre le système de congruences

$$\begin{cases} x \equiv 3 \bmod 17 \\ x \equiv 4 \bmod 11 \\ x \equiv 5 \bmod 6 \end{cases}$$

Les 3 modules $m_1=17$, $m_2=11$, $m_3=6$ sont premiers entre eux 2 à 2 ; donc le théorème des restes chinois s'applique

On trouve la solution :

$c = 66.8.3 + 102.\ 5.\ 4 + 187.\ 1.\ 5 \equiv 785 \bmod 1122$.

5 Tests de primalité

Pour savoir si un entier naturel *n* est premier il y a plusieurs méthodes.

Certaines sont simples lorsque l'entier n possède 4 ou 5 chiffres au plus, les résultats sont tabulés.

Dans ce cas, on effectue les divisions de l'entier *n* par les nombres premiers $p < \sqrt{n}$.

(Table de Druck Van Tafel H, Grominger, Holland,(1953), dans laquelle les entiers de 1 à 11197 sont indiqués avec leur factorisation).

D'autres méthodes sont nécessaires pour des entiers de plus 20 chiffres.
Les plus grands nombres premiers sont obtenus par les spécialistes avec des programmes exécutés par ordinateurs pendant plusieurs jours.

Exemple :

Le plus grand nombre premier connu est $2^{13466917}-1$
Ce nombre comporte 4 053 946 chiffres. Il s'agit du 39e nombre premier de Mersenne $M_{13466917}$ découvert le 14 novembre 2001.
Le nombre premier précédent est $2^{6972593}-1$
Ce nombre comporte 2 098 960 chiffres, et est aussi un nombre premier de Mersenne, découvert le 1 juin 1999.

Ici, nous considérons quelques méthodes "élémentaires" .

5.1 Théorème 5 (Atkin et Berstein 1999)

On considère l'ensemble des entiers *n* premiers à 12 et sans facteur carré, et les 3 sous ensembles :

$$K_1(n) = card \left\{ (u,v) : u > v > 0 \; ; \; n = u^2 + v^2 \equiv 1, 5 \mod 12 \right\}$$

$$K_2(n) = card \left\{ (u,v) : u > 0, v > 0 \; ; \; n = 3 \times u^2 + v^2 \equiv 7 \mod 12 \right\}$$

$$K_3(n) = card \left\{ (u,v) : u > v > 0 \; ; \; n = 3 \times u^2 - v^2 \equiv 11 \mod 12 \right\}$$

Alors *n* est premier si et seulement si l'un des *K (n)* est impair.

□

Exemple :

Soit *n* =149, le nombre de représentations d'un entier *n* comme somme de 2 carrés, $n = u^2 + v^2$ est égal à

$$r_2(n) = 4 \times \sum_{d/n-1} (-1)^{(d-1)/2}, \; d \quad impair$$

$$n = 149 \equiv 5 \mod 12$$

L'équation $n = 149 = u^2 + v^2$ admet une solution unique

$u > v > 0$ qui est u=10 et v=7

Il en résulte K_1=1 est impair, donc n =149 est premier par le théorème d'Atckin-Bretein .

Exemple :

Soit n = 1241, implique n = 1241 ≡ 5 mod 12.

L'équation n = 1241 = $u^2 + v^2$ admet deux solutions u> v qui sont u = 35, 29 et v = 4, 20, il en résulte $K_1 = 2$ est pair, donc n= 1421 n'est pas premier et plus précisément n= 17.73

5.2 Théorème 6 (Lucas-Lehmer)

Si les entiers a et n satisfont les congruences

$a^{(n-1)} \equiv 1 \bmod n$ et $a^{(n-1)/p} \neq 1 \bmod n$ pour tout diviseur premier p de n-1 , alors n **est premier**

Exemple

Soit n = 2003 et a = 5

Alors les diviseurs premiers de n-1 = 2002 sont : 2, 7, 11, 13

On a: $a^{(n-1)} = 5^{2002} \equiv 1 \bmod 2003,$ (1)

Pour p =2 on a: $a^{(n-1)/p} = 5^{1001} \equiv -1 \bmod 2003,$ (2)

Pour p =7 on a: $a^{(n-1)/p} = 5^{286} \equiv 874 \bmod 2003,$ (3)

Pour p =11 on a: $a^{(n-1)/p} = 5^{182} \equiv 886 \bmod 2003,$ (4)

Pour p = 13 on a : $a^{(n-1)/p} = 5^{154} \equiv 633 \bmod 2003$, (5)

(1), (2), (3), (4) et (5) impliquent que n =2003 est premier.

□

Théorème 7

Soit un entier n >1 impair qui satisfait les congruences

$a^{(n-1)/2} \equiv -1 \bmod n$ et $a^{(n-1)/2p} \neq -1 \bmod n$ pour tout diviseur premier p de n-1 , alors n est premier.

Réciproquement, soit un nombre premier impair p , alors toute **racine primitive** *a* modulo p satisfait ces 2 relations

□

Exemple

Soit n = 401 et a = 3, impliquent :

Les diviseurs premiers de n-1 = 400 sont 2 et 5

$3^{(400)/2} = 3^{200} \equiv -1 \bmod 401$, (1)

Pour p = 2 : $3^{(400)/2.2} = 3^{100} \equiv 20 \bmod 401$, (2)

Alors p = 2 satisfait la congruence

Pour p = 5 : $3^{(400)/2.5} = 3^{40} \equiv 83 \bmod 401$, (3)

Alors p = 5 satisfait la congruence

(1), (2) et (3) impliquent que n= 401 est premier.

Pour les nombres de Mersenne $M_n = 2^n - 1$ on dispose du test

Théorème 8 (Lucas- Lehmer)

On considère la suite d'entiers (v_k) , pour k = 0,1,… définie par le premier terme $v_0 = 4$ et la récurrence linéaire $v_{k+1} = v_k^2 - 2$

Soit un nombre premier p. Alors, le nombre de Mersenne $M_p = 2^p - 1$ est premier si et seulement si $v_{p-2} \equiv 0 \bmod M_p$

□

Exemple 1 :

Pour p =5.

Alors $M_5 = 2^5 - 1 = 31$, $v_0 = 4$, $v_1 = 14$, $v_2 = 194$, $v_3 = 37634$

v_3 satisfait la congruence $37634 = 31 \times 1214$.

Il en résulte que $M_5 = 31$ est premier.

Exemple 2 :

Pour p = 7

Alors $M_7 = 2^7 - 1 = 127$, $v_0 = 4$, $v_1 = 14$, $v_2 = 194$, $v_3 = 37634$, $v_4 = 1416317954$

$v_5 = 2005956546822746114 = 127 \times 157949334959182$

v_5 satisfait la congruence.

Il en résulte que $M_7 = 127$ est premier

Exemple 3 :

Pour p = 11

Alors $M_{11}= 2^{11} -1 = 2047$, $v_0 = 4$, $v_1 =14$, $v_2= 194$, $v_3 = 37634$, $v_4= 1416317954$

$V_5= 2005956546822746114$, $v_6=4023861667741036022825635656102100994$

$V_7=1619146272111567178177755907012051366495859012549915855143293087409757880 34$

$V_8=2621634650492785145260593695575630392136478775595245459119060053495557738312369350159562818489334269993079824186649432769439016089193966072975851 54$

$V_9=6872968240664427723883748622317475309242471541086466717521926185830884874057909579647328830691025610434367796639355951720423573065949163446060745647128680782876080552030246583594390175808839109786661858757174155410844949265004751673811685059273781818997538392606094522653652748509018798812037 14$

$v_9 \equiv 1736 \bmod 2047$, v_9 ne satisfait pas la congruence implique que

$M_{11} = 2047$ n'est pas premier.

5.3 Test de Miller – Rabin

Petit Théorème de Fermat

Pour tout nombre premier p, tout entier a < p satisfait la congruence

$$a^{p-1} \equiv 1 \bmod p$$

Pour un entier n, de nature inconnue, la congruence

$$a^{n-1} \equiv 1 \bmod n$$

ne suffit pas pour que n soit premier.

Il faut que les congruences : $a^{(n-1)/q} \not\equiv 1 \bmod n$, soient satisfaites pour tous les diviseurs premiers q de n-1 pour que n soit un nombre premier.

Considérons une autre variante du Petit Théorème de Fermat

Théorème 9 :

Soit un entier premier impair p et la décomposition : $p-1 = 2^s d$, où d est impair.

Alors, tout entier a non divisible par p satisfait l'une des deux condition :

$a^d \equiv 1 \bmod p$, où bien $a^{2^r d} \equiv -1 \bmod p$

pour un certain entier r avec $0 \leq r \leq s-1$

□

Ce Théorème implique le Test suivant

Algorithme

Considérons un nombre impair $n > 3$

Représentation $n = 1+ 2^s d$, avec d impair

Soit un entier a, avec $1< a < n-1$

[Partie impaire de n-1] ; $b = a^d \bmod n$.

Si $b = 1$ ou $b = -1$, alors n est fort probablement premier de base a

[Les puissances de 2 dans n-1] ; $b = b^2 \bmod n$.

Si $b = -1 \bmod n$, alors n est fort probablement premier de base a.

Sinon n est composé et on appelle a un témoin de non primalité

Exemple 1 :

Soit $n = 53$, alors $n-1 = 52 = 2^2.13$

Pour $a = 2$, $2^{13} \equiv 30 \bmod 53$

$2^{2.13} = 30^2 \equiv -1 \bmod 53$

$2^{4.13} = -1^2 \equiv 1 \bmod 53$

Il n'y pas de contradiction donc 53 passe le test pour la base 2

Exemple 2 :

Soit n = 561, alors n-1 = 560 = 2^4.35

Pour a = 2, $2^{35} \equiv 263 \bmod 561$

$2^{2.35} = 263^2 \equiv 166 \bmod 561$

$2^{2^2.35} = 166^2 \equiv 67 \bmod 561$

$2^{2^3.35} = 67^2 \equiv 1 \bmod 561$

Nous avons rencontré une contradiction donc 561 ne passe pas le test donc ; il n'est pas premier

Le témoin de non -primalité est le nombre a = 2.

Exemple 3 :

Soit n = 2047, alors n-1 = 2046 = 2.1023

Pour a= 2, $2^{1023} \equiv 1 \bmod 2047$

Alors 2047 passe le test pour la base 2.

Pour a = 3, $3^{1023} \equiv 1565 \bmod 2047$

Nous avons rencontré une contradiction**.** Donc 2047 ne passe pas le test ; donc il n'est pas premier.

Le témoin de non-primalité est le nombre a = 3.

Exemple 4 :

Soit n = 536870911, alors n-1 = 536870910 = 2.268435455

Pour a = 2, $2^{268435455} \equiv 1 \bmod 536870911$

Alors 536870911 passe le test pour la base 2.

Pour a = 3, $3^{268435455} \equiv 89777599 \bmod 536870911$

Nous avons rencontré une contradiction. Donc 536870911 ne passe pas le test ; donc il n'est pas premier.

Le témoin de non primalité est le nombre a = 3.

Conclusion :

Les nombres premiers sont étudiés depuis l'Antiquité. Euclide a prouvé qu'il en existe une infinité par exemple classique de démonstration par l'absurde. Les nombres premiers ont de nombreuses utilisations pratiques, dont la cryptologie asymétrique. Pour déterminer si un nombre est premier, on utilise des tests de primalité .Certains tests de primalité sont probabilistes et choisissent un nombre aléatoire appelé "témoin " et vérifient quelque formule impliquant le témoin et le nombre potentiellement premier N. Après plusieurs itérations, ils déclarent N être sans aucun doute composé ou probablement premier. Ces examens ne sont pas parfaits. Pour un test donné, il peut y avoir plusieurs nombres composés qui seront déclarés " probablement premiers " indépendamment du témoin choisi. De tels nombres sont appelés pseudo premiers. Pour rechercher une liste de tous les nombres premiers inférieurs à une limite, le crible d'Eratosthène est une méthode simple et efficace.

Bibliographie

[1] R. CRANDALL and POMERANCE; prime numbers Springer (2002)

[2] J.P. DELAHAYE; Merveilleux nombres premiers, Belin, Paris (2000)

[3]L.E.DICKSON; Introduction to the Theory of Numbers, Dover Press, (1975)

[4] NIVEN, IVAN and HERBERT.S.ZUCKERMAN; An Introduction to the Theory of Numbers, 3 rd ed, John Wiley, (1972)

[5] J.E.SHOCKLEY, Introduction to the Number Theory, Holt.Inc.N.Y (1967)

[6] MENDES FRANC et TENEMBAUM; les nombres premiers, PUF (1997)

[7] M. YORINAGA, Carmichael Numbers with Many Prime factors, math J: of Okayama Université Japon, vol 22- n 0 2 (décembre 1980, page 160-184)