UNIVERSITE MOHAMED PREMIER
FACULTE DES SCIENCES
DEPARTEMENT DE MATHEMATIQUES ET INFORMATIQUE
OUJDA

MASTER INGÉNIERIE INFORMATIQUE

NOTES DU COURS DE CRYPTOGRAPHIE
PARTIE II

Du Professeur

ABDELMALEK AZIZI

Année Universitaire 2015-2016

Préface

Le présent document est un ensemble de notes de cours, du Module " Cryptographie" de la Filière Master "Ingénierie Informatique" qui est enseigné, à la Faculté des Sciences de l'université Mohammed premier depuis l'année universitaire 2007-2008, et qui entre dans le cadre du Projet Tempus CD-JEP-34001-2006(MA).
Le présent document est basé sur les notes de cours de mes anciens cours, certains mémoires de Licence, de Master ainsi que sur certaines études qui entrent dans le cadre du projet " Théorie des nombres et leurs applications en Cryptographie et en Fractals". En particulier, on retrouve ici les travaux des mémoires des étudiants HAMMOUDI Khalil et OUBRAHIM Rachid qui ont préparé un mémoire intitulé "Cryptographie : Méthodes de substitutions et leurs cryptanalyses" et des étudiants El Fardi Manal et Mouhamed Boutrah qui ont préparé un mémoire intitulé "Tests de primalité et Cryptographie" et aussi des étudiants du Master M2I, Koulali, Oudari et Rabhi qui ont préparé un mémoire intitulé "Logiciel du dictionaire Arabe Al-Ain".

Je souhaite que je puisse améliorer davantage ce document pour l'intérêt des étudiants et des chercheurs et aussi pour enrichir nos bibliothèques par des documents riches, simples et complets.

Abdelmalek Azizi

Table des matières

pages

Chapitre 1

Introduction

Comme disait Kronecker(1823 - 1852) ; Dieu a crée les entiers naturels et l'homme a fait le reste. Dieu a crée les entiers en même temps que l'univers. L'homme a su, avec son génie, comprendre et utiliser les entiers. Par la suite, suivant ses besoins, il s'est mis à utiliser d'autres nombres : les nombres rationnels, les nombres irrationnels, les nombres complexes...
L'homme s'est intéressé à l'étude de certains problèmes de nombres depuis des périodes très reculées. Les problèmes étudiés provenaient aussi bien de son activité économique (commerce, poids et mesure) que de ses préoccupations astronomiques (calendrier, astrologie). Pour désigner un nombre, l'homme a utilisé des lettres ou des symboles. Les Romains utilisaient "les chiffres Romains " I, II, III, IV, V, VI, VII, VIII, IX, X... Les Arabes ont pris en mains propres les chiffres Hindous et ils les ont développés et structurés. Le développement des nombres a donné dans le Maghreb Arabe les nombres

0, 1, 2, 3, 4, 5... connus sous le nom ”nombres Arabes” tandis que dans le Machrek Arabe il a donné les nombres <0>, <1>, <2>, <3>, <4>, <5>, <6>, <7>, <8>, <9>, $\cdots$.

Deux mille ans avant notre ère, pour effectuer leurs calculs les Babyloniens disposaient de diverses tables numériques (de multiplications, de carrés, de cubes...). Ainsi, ils accumulèrent de nombreuses connaissances en arithmétique.
Au début du troisième siècle avant notre ère, Euclide, dans son livre Les éléments, avait consacré les chapitres 7, 8 et 9 à la théorie des nombres. Dans le septième chapitre on trouve les définitions suivantes :

1. L’unité est ce selon quoi chacune des choses existantes est dite une.
2. Un nombre est un assemblage composé d’unités.
3. Un nombre est une partie d’un nombre, le plus petit du plus grand, lorsque le plus petit mesure le plus grand.
4. Un nombre est multiple d’un nombre, le plus grand du plus petit, quand il est mesuré par le plus petit.
5. Le nombre pair est celui qui peut se partager en deux parties égales.
6. Le nombre impair est celui qui ne peut se partager en deux parties égales, ou bien celui qui diffère

d'une unité du nombre pair.

7. Le nombre premier est celui qui est mesuré par l'unité seule.
8. Les nombres premiers entre eux sont ceux qui ont l'unité seule pour commune mesure.
9. Le nombre composé est celui qui est mesuré par quelques nombres.
10. Les nombres composés entre eux sont ceux qui ont quelques nombres pour commune mesure.

Chez les Grecs, parallèlement au grand développement de la géométrie (Euclide), le courant mathématique des nombres a trouvé son expression la plus célèbre chez Diophante d'Alexandrie (vers 250 ans après J - C.). Son ouvrage, l'Arithmétique, où les solutions proposées de certains problèmes de théorie des nombres se ramènent essentiellement à la résolution d'équations (du premier degré, du second degré et même de degré supérieur à une ou plusieurs inconnues), sera un puissant stimulant pour les mathématiques des 16-ème et 17-ème siècles.

Les Musulmans, après avoir étudié et assimilé les acquis des civilisations antérieures, ont donné naissance à une civilisation originale et brillante. A partir du 8 -ème siècle, El-Khawarizmi est devenu très célèbre. Il doit cette célébrité à l'influence que ses traités d'arithmétique et d'algèbre exercèrent sur plusieurs générations de mathématiciens. Son livre d'arithmétique, qui

avait un aspect académique, traite plusieurs problèmes d'arithmétique. En particulier, il explique comment, avec neuf caractères seulement et le zéro, on peut représenter tout nombre et effectuer toutes les opérations usuelles. Son deuxième livre d'Algèbre, où se trouvent ses résultats sur les équations du premier et du second degré, est le premier livre qui traite d'une façon détaillée et complète les équations du second degré.
Les Babyloniens, les Grecs et les Musulmans ont mis la théorie des nombres sur le bon chemin. Les Européens des six derniers siècles ont bien développés cette théorie. Ils ont résolu plusieurs problèmes , ils ont laissé d 'autres sous forme de conjectures et ils ont orienté cette théorie vers plusieurs axes de recherches ...

Chapitre 2

Les nombres premiers

Les nombres premiers jouent un rôle primordial en Arithmétique. Un exemple qui nous illustre ce rôle est le théorème fondamental d'arithmétique suivant :

Théorème 1. *Tout entier naturel est produit de nombres premiers, et ceci d'une façon unique.*

Parmi les plus anciens Théorèmes sur les nombres premiers, on trouve celui-ci (démontré par Euclide plus de deux siècles avant notre ère) :

Théorème 2. *L'ensemble des nombres premiers est un ensemble infini.*

Pour démontrer ce résultat, Euclide avait supposé que l'ensemble des nombres premiers est égal à $\{p_1, p_2, ..., p_n\}$ et il avait considéré l'entier $m = p_1 p_2 ... p_n + 1$. Alors cet entier est premier ou bien il possède un diviseur premier. Or aucun des premiers $p_1, p_2, ..., p_n$ ne peut diviser m ; donc il y a une contradiction. Il en déduit que l'ensemble des nombres premiers est infini. Il existe

plusieurs preuves pour ce théorème. On va donner une autre preuve, fort intéressante, et qui découle de la théorie analytique des nombres.

A partir du 14-ème siècle, la convergence des séries faisait l'objet d'études de plusieurs mathématiciens. En 1360, Nicole Oresme avait donné des critères pour la convergence ou la divergence de certaines séries. En particulier, il avait démontré la divergence de la série :

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots=\sum_{n=1}^{\infty}\frac{1}{n}.$$

Vers le 17-ème siècle plusieurs valeurs approximatives ont été données pour la valeur de

$$\sum_{n=1}^{\infty}\frac{1}{n^2}$$

et c'est en 1735 que Euler (1707 - 1783) avait donné la valeur exacte de cette somme (à savoir $\frac{\pi^2}{6}$).

En 1737, Euler avait introduit la fonction zêta :

Définition 1.

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\quad s\in\mathbf{R}$$

Par la suite il avait démontré le théorème suivant :

Théorème 3.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - \frac{1}{p^s}} \quad s > 1$$

Le produit est pris sur tout les nombres premiers.

Preuve : Voir [1] ou [13].

Remarque 4. Au début, la fonction zêta était définie uniquement pour les nombres réels. C'est Riemann (1826 - 1866) qui avait montré que cette fonction peut être prolongée analytiquement par continuité en tout nombre complexe autre que le point $s = 1$. Ce dernier point est un pôle simple pour la fonction zêta. En plus, Riemann nous a laissé un ensemble de conjectures concernant la fonction zêta. Parmi ces conjectures on trouve la conjecture connue par l'hypotèse de Riemann.

Une conséquence immédiate du théorème 4 est que l'ensemble des nombres premiers est infini. En effet, sinon et lorsque s tend vers 1, on trouve que la série

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

est convergente. Mais, on sait que ceci est faux.
Les idées de Euler ont été élaborées et développées par Dirichlet (1805 - 1859). Ce dernier avait défini la fonction L (qui est une généralisation de la fonction zêta) et il a généralisé le théorème 4 :

Définition 2. Soient m un entier supérieur ou égal à 1 et χ un caractère modulo m (un homomorphisme du groupe multiplicatif de $\mathbf{Z}/m\mathbf{Z}$ dans $\mathbf{C}^*$ qu'on prolonge par 0 sur les entiers non premiers avec m). La fonction L est définie par :

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Théorème 5.

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \frac{1}{1-\frac{\chi(p)}{p^s}} \quad s > 1$$

Le produit est pris sur tous les nombres premiers.

Preuve : Voir [1] ou [13].
En particulier, Dirichlet a prouvé le théorème de la progression arithmétique :

Théorème 6. *Soient a et m deux entiers supérieurs ou égaux à 1 et premiers entre eux. Il existe une infinité de nombres premiers p tels que $p \equiv a \bmod m$.*

Le théorème de la progression arithmétique avait été conjecturé et utilisé par Legendre. Pour le démontrer, Dirichlet avait défini et utilisé la notion de densité :

Définition 3. Soient P l'ensemble des nombres premiers et A une partie de P. Soit k un réel compris entre 0 et 1 ; on dit que A est de densité k si et seulement si le rapport

$$(\sum_{p\in A} \frac{1}{p^s}) / \log \frac{1}{s-1}$$

tend vers k lorsque s tend vers 1.

On remarque que si A est un ensemble fini, alors la densité de A est nulle. Par conséquent, pour montrer qu'un ensemble A est infini il suffit de vérifier qu'il est de densité non nulle. C'est ce que Dirichlet avait montré :

Théorème 7. *Soient m un entier supérieur ou égal à 1 et a un entier premier avec m. On note par P_a l'ensemble des nombres premiers p tels que $p \equiv a \bmod m$. Alors l'ensemble P_a est de densité $\frac{1}{\phi(m)}$* [1].

Preuve : Voir [13].
On trouve d'autres applications de la notion de densité sur l'ensemble des nombres premiers comme le montre l'exemple suivant :

Théorème 8. *Soit x un entier qui n'est pas un carré. Alors l'ensemble des nombres premiers p tels que $(\frac{x}{p}) = 1$ a pour densité $\frac{1}{2}$.*

Preuve : Voir [13].

Les mathématiciens se sont penchés sur plusieurs problèmes de nombres premiers. A quinze ans, Gauss (1777 - 1855) avait remarqué que $\pi(N)$ (la quantité de nombres premiers inférieurs ou égals à N) et $\frac{N}{\log(N)}$ deviennent

1. La fonction ϕ d'Euler est définie par : si $m = p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r}$, alors $\phi(m) = (p_1 - 1)p_1^{i_1 - 1}(p_2 - 1)p_2^{i_2 - 1} \cdots (p_r - 1)p_r^{i_r - 1}$.

de plus en plus proches lorsque N tend vers l'infini. Cette remarque avait été démontrée en 1896 par les mathématiciens Hadamard (1865 - 1963) et de la Vallée Poussin (1866 - 1962) (Théorème de la distribution des nombres premiers).
Une fois les questions de distribution et de densité des nombres premiers résolues, on se demande si on peut déterminer le n-ième nombre premier. Pour cela on donne un exemple de formules (souvent compliquées) qui donne le (n + 1)-ième nombre premier p_{n+1} (voir [5]) :

$$p_{n+1} = E(1 - \frac{1}{\log 2}\log(-\frac{1}{2} + \sum_{d|P_n} \frac{\mu(d)}{2^d - 1}))$$

Où

$$P_n = \prod_{j=1}^{n} p_j, \quad E(x) \text{ désigne la partie entière de } x,$$

et μ est la fonction de M$\ddot{o}$bius :

$$\mu(d) = \begin{cases} 1 & \text{si } d = 1, \\ o & \text{si } d \text{ est divisible par un carré}, \\ (-1)^r & \text{si } d = p_1 p_2 \cdots p_r. \end{cases}$$

Cette formule trouvée par J.M.Ghandi reste inutile pour déterminer les grands nombres premiers (comme toutes les formules trouvées jusqu'à présent) : car avec un superordinateur, le calcul du 10^{10}-ième nombre premier (par exemple) nécessite un temps énorme.

Remarques 9. 1. Fermat croyait que tous les nombres de la forme $2^{2^n}+1$ (appelés nombres de Fermat) sont des nombres premiers. Ceci est vrai pour $n = 0,\ 1,\ 2,\ 3,\ 4$ mais pour $n > 4$ nous savons maintenant que l'affirmation de Fermat est fausse.
2. Parmi les plus grands nombres premiers on trouve dans l'ensemble des nombres de Mersenne [2], le nombre premier $2^{216091}-1$ (ce nombre premier possède plus de 65000 chiffres).
3. Parmi les résultats les plus remarquables sur les nombres premiers, on trouve le Théorème de Wilson (1741 - 1793) : un entier n est premier si et seulement si $(n-1)! \equiv -1 \bmod n$. Malheureusement, ce résultat est un algorithme qui, avec un superordinateur, nous demande un temps énorme pour savoir si un nombre est premier ou non.

2. Les nombres de Mersenne sont les nombres de la forme $2^q - 1$ où q est un nombre premier.

Chapitre 3

Nombres remarquables

Nous avons déjà rencontré plusieurs nombres particuliers ; comme les nombres pairs, les nombres impairs, les nombres premiers et d'autres. Dans cette section, on va définir d'autres nombres remarquables ou historiques, dans le corps des nombres complexes, ainsi que d'autres notions importantes liées à ces nombres.

0.1 Les nombres de Carmichael

D'après Fermat, on sait que si p est un nombre premier, alors pour tout entier a premier avec p on a : $a^{p-1} \equiv 1 \bmod p$. Ce dernier résultat est utilisé dans certains algorithmes de primalité. En effet, si pour un entier naturel n on n'a pas $a^{n-1} \equiv 1 \bmod n$, alors n n'est pas premier.

Définition 4. Soit n un entier naturel composé ; on dit que n est un nombre de Carmichael si et seulement si

pour tout entier a premier avec n on a :
$a^{n-1} \equiv 1 \bmod n$.

EXEMPLE.
Le plus petit nombre de Carmichael est le nombre $561 = 3 \times 11 \times 17$.

Remarque 10. Soient t un entier naturel et $N = (6t + 1)(12t + 1)(18t + 1)$. Si les trois facteurs $6t + 1$, $12t + 1$ et $18t + 1$ sont des nombres premiers ; alors N est un nombre de Carmichael. Un exemple de nombres de Carmichael possédant cette forme est le suivant : $7 \times 13 \times 19 = (6 + 1)(12 + 1)(18 + 1)$.

Théorème 11. *Soit N un entier naturel. Le nombre N est un nombre de Carmichael si et seulement si N n'est pas premier, N est sans facteur carré et pour tout p, diviseur premier de N, on a $p - 1$ divise $N - 1$.*

Preuve : Voir [11].

1 Les nombres pseudopremiers d'Euler

Symbole de Legendre (1752 - 1833).
Soit p un nombre premier et a un entier naturel premier avec p. Le symbole $(\frac{}{p})$ est défini par : $(\frac{a}{p}) = 1$ si l'équation $x^2 \equiv a \bmod p$ possède une solution dans $\mathbb{N}$. Dans le cas contraire on a $(\frac{a}{p}) = -1$. On prolonge le symbole $(\frac{}{p})$ par zéro sur $\mathbb{N}$. Ce symbole a été défini par Legendre pour les nombres premiers impairs

et par Kronecker (1823 - 1893) pour le nombre 2.
Critère d'Euler.
Soit p un nombre premier impair ; alors pour tout entier a premier avec p on a : $a^{(p-1)/2} \equiv \pm 1 \bmod p$.
Ce critère est aussi utilisé dans les tests de primalité.

Remarques 12. 1. Le symbole de Legendre $(\frac{a}{p})$ vérifie de plus :
i) $(\frac{a}{p}) \equiv a^{(p-1)/2} \bmod p$.
ii) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ pour a et b quelconques dans $\mathbb{N}$.
2. Le symbole de Legendre a été généralisé, par Jacobi (1804 - 1851), comme suit :
Le symbole de Jacobi $(\frac{a}{n})$ est défini par :
C'est le symbole de Legendre si $n = p$, un nombre premier impair ;
c'est le symbole de Kronecker pour $n = 2$:

$$(\tfrac{a}{2}) = \begin{cases} 1 \text{ si } a \equiv 1 \bmod 8, \\ -1 \text{ si } a \equiv 5 \bmod 8, \\ 0 \text{ si } a \text{ est divisible par } 4, \\ \text{et il n'est pas défini pour les autres valeurs de } a. \end{cases}$$

Et si $n = \prod_{i=1}^{i=r} p_i^{m_i}$, alors $(\frac{a}{n}) = \prod_{i=1}^{i=r} (\frac{a}{p_i})^{m_i}$.

Définition 5. Soit N un nombre composé. On dit que N est un nombre pseudopremier d'Euler pour la base a si et seulement si $a^{(N-1)/2} \equiv (\frac{a}{N}) \bmod N$ où $(a, N) = 1$ et $(\frac{a}{N})$ désigne le symbole de Jacobi.

EXEMPLE.
Le nombre 341 est un nombre pseudopremier d'Euler pour la base 2. En effet, On a : $2^{170} \equiv 1 \bmod 341$.

2 Les nombres parfaits

Soient n un entier naturel et $\sigma(n)$ la somme de tous les diviseurs de n ; alors on a :
i) Si $n = p_1^{a_1} \cdots p_r^{a_r}$, alors $\sigma(n) = \frac{p_1^{a_1} - 1}{p_1 - 1} \cdots \frac{p_r^{a_r} - 1}{p_r - 1}$.
ii) Si $(m, n) = 1$, alors $\sigma(mn) = \sigma(m)\sigma(n)$.

Définition 6. un entier naturel n est un nombre parfait si et seulement si $\sigma(n) = 2n$.

EXEMPLES.
a) $n = 6 = 2 \times 3$. On a : $\sigma(6) = 1 + 2 + 3 + 6 = 2 \times 6$.
b) $n = 28 = 2 \times 2 \times 7$. On a : $\sigma(28) = 1+2+4+7+14+28 = 2 \times 28$.

Remarques 13. 1. Toute fonction f définie sur $\mathbb{N}$ est dite arithmétique. Une fonction arithmétique f vérifiant : Si $(m, n) = 1$, alors $f(mn) = f(m)f(n)$; est dite fonction multiplicative. La fonction σ et l'indicateur d'Euler ϕ sont des fonctions multiplicatives.
2. Soient $n = p_1^{a_1} \cdots p_r^{a_r}$ et $\tau(n)$ le nombre de diviseurs de n. Alors la fonction τ est multiplicative et on a de plus : $\tau(n) = (a_1 + 1) \cdots (a_r + 1)$.

3. En 1747, Euler avait démontré que tous les nombres parfaits pairs sont de la forme (donnée par Euclide) $2^{n-1}(2^n - 1)$ où $2^n - 1$ est un nombre premier. Parmi les nombres impairs, on ne sait pas encore s'il y a des nombres parfaits ou non.

3 Les nombres amiables

Définition 7. Soient m et n deux entiers naturels. On dit que m et n sont deux nombres amiables ou amicaux si et seulement si m est la somme des diviseurs propres de n (i.e. $\neq n$) et n est la somme des diviseurs propres de m.

EXEMPLES.
1. Les plus petits nombres amiables sont 220 et 284.
2. Fermat avait trouvé les nombres amiables suivants : 17296 et 18416.
Les nombres amiables étaient l'objet d'étude de plusieurs mathématicients ; en particulier on trouve le théorème de Thabit Ibno Qurra suivant :

Théorème 14. *Soient a, b et c trois nombres premiers et n un entier naturel. Si $a = 3.2^n - 1$, $b = 3.2^{n-1} - 1$ et $c = 9.2^{2n-1} - 1$, alors les nombres $2^n c$ et $2^n ab$ sont amiables.*

4 Les nombres de Fibonacci et le nombre d'Or

Définitions 1. 1. On appelle suite de Fibonacci la suite F_n telle que $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$. Chaque terme de cette suite est un entier naturel qu'on appelle nombre de Fibonacci.
2. On appelle nombre d'Or le nombre $g = \frac{1+\sqrt{5}}{2}$.

Remarques
1. Le nombre de Fibonacci F_n est l'entier le plus proche du nombre $\frac{g^n}{\sqrt{5}}$ où g est le nombre d'Or.
2. Sur un segment AB, la section d'Or est déterminée par un point M du segment tel que $\frac{AB}{AM} = \frac{AM}{BM}$. Il est facile de voir que cette fraction est égale à g.
3. Les nombres de Fibonacci et le nombre d'Or sont utilisés dans certains problèmes de banques comme celui de depôt d'argents.
4. Le nombre d'Or est aussi utilisé par les peintres pour avoir la proportion d'Or entre deux produits.

5 Les nombres algébriques et les nombres transcendants

Au 18-ième siècle, Legendre avait travaillé sur l'hypotèse que π pouvait ne pas être une racine d'un polynôme à coefficients rationnels. C'est ainsi que les mathématiciens ont commencé à distinguer deux genres

de nombres dans l'ensemble des nombres complexes :

Définition 8. 1. Toute solution d'un polynôme à coefficients rationnels est appelée nombre algébrique. Un nombre algébrique qui est solution d'un polynôme unitaire à coefficients dans $\mathbb{Z}$ est dit un entier algébrique.
2. Un nombre qui n'est pas algébrique est dit transcendant.

EXEMPLES.
1. le nombre $\frac{1}{\sqrt{2}}$ est un nombre algébrique car il est solution du polynôme $X^2 - \frac{1}{2}$.
Le nombre complexe i est un entier algébrique car il est solution du polynôme $X^2 + 1$. L'ensemble $\mathbb{Z}[\mathrm{i}]$ des éléments de la forme $a + bi$ est un anneau dont tout les éléments sont des entiers algébriques. Les éléments de $\mathbb{Z}[\mathrm{i}]$ sont appelés les entiers de Gauss (1777-1855).
3. Le nombre d'Euler $e(\exp(1))$ est un nombre transcendant (démontré en 1873 par Hermite (1822 - 1901)).
4. Le nombre π est un nombre transcendant (démontré en 1882 par Lindmann (1852 - 1939)).
5. En 1844, J. Liouville (1809 - 1882) avait montré que tout nombre de la forme

$$\sum_{n=1}^{\infty} \frac{a_i}{10^n},$$

où les a_i sont des entiers compris entre 1 et 9, est transcendant.

Remarques 15. 1. Au 18-ième siècle, Euler avait montré que le nombre e est irrationnel et Lambert avait montré que le nombre π est irrationnel.
2. L'anneau $\mathbb{Z}[i]$ possède plusieurs propriétés de $\mathbb{Z}$; ce qui explique son utilité pour la résolution de plusieurs problèmes en théorie des nombres. En particulier, les entiers de Gauss ont permis de régler certaines questions de représentabilité de nombres par des formes quadratiques : Par exemple p est représenté par la forme quadratique x^2+y^2 si et seulement si p est égal au produit de $x+yi$ par son conjugué $x-yi$.

6 Les nombres de Bernoulli

On considère la fonction zêta définie précédement. On appelle nombres de Bernoulli les nombres rationnels B_n définis comme suit :

$$B_0 = 1, \;\; B_n = (-1)^n 2n\zeta(1-2n), \;\; n > 0.$$

On peut aussi définir ces nombres comme suit :

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

Les premiers nombres de cette suite sont :
$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30},\ B_{10} = \frac{5}{66}$ et $B_{2k+1} = 0$ pour tout k supérieur ou égal à 1.

Remarques 16. 1. La fonction zêta prend des valeurs rationnelles sur les entiers négatifs : les valeurs de la foncion zêta sur les entiers négatifs impairs sont données à l'aide des nombres de Bernoulli tandis que pour les entiers négatifs pairs la fonction zêta est nulle.
2. Hypotèse de Riemann.
Riemann avait conjecturé que les autres zéro (qui sont différents des entiers négatifs paires) se trouvent sur la droite $R(s) = 1/2$ où $R(s)$ désigne la partie réelle de s.

7 Les nombres réguliers

Soit p un nombre premier ; on dit que p est régulier si et seulement si il existe un entier $k,\ k = 2,\ 4,\ 6, ...,\ p-3$ tel que p divise le numérateur du nombre B_k. Dans le cas contraire, on dit que p est irrégulier. Les premiers nombres premiers irréguliers sont : $37,\ 59,\ 67,\ 101,\ 103,\ 131,\ 149$ et 157.

Remarque 17. Soient p un nombre premier, ζ une racine primitive p-ième de l'unité ($\zeta^p = 1$ et $\zeta \neq 1$) et $\mathbb{Q}(\zeta)$ le corps cyclotomique engendré par $\mathbb{Q}$ et ζ. Un nombre premier p est régulier si et seulement si p divise le nombre de classes de $\mathbb{Q}(\zeta)$.

Théorème 18. *(Fermat (1601 - 1665))*
Soit n un entier naturel supérieur ou égal à 3. Alors l'équation suivante n'a pas de solutions entières non triviales :

$$X^n + Y^n = Z^n.$$

Preuve : Voir [16]. Ce théorème a été démontré par A. Weiles en 1994. Le cas où n est un nombre premier régulier a été démontré, un siècle avant, grâce à Kummer (1810 - 1893) :

Théorème 19. *Soit p un nombre premier régulier. Alors l'équation suivante n'a pas de solutions entières non triviales :*

$$X^p + Y^p = Z^p, \quad (XYZ, p) = 1.$$

Preuve : Voir [15].

Chapitre 4

Tests de Primalité

Il est très important de savoir si un nombre donné est premier ou pas ; et sinon de détérminer sa décomposition en produit d'éléments premiers. Si on arrive à déterminer la primalité d'un entier dans un temps donné, alors sa factorisation peut prendre énormément plus de temps. On peut toujours essayer de chercher parmi les nombres inférieurs à ce nombre ses diviseurs, essayer la méthode du crible d'*Eratosthène*, le test de Fermat, celui d'Euler ou bien d'autres. Cependant ces algorithmes restent incapables de déterminer, en un temps raisonnable, la factorisation d'un grand nombre.

Division et crible d'*Eratosthène*

Pour tester la primalité d'un entier il suffit de parcourir tous les entiers entre 2 et $n-1$, et tester si ces entiers divisent n ou non. Bien sûr, il est facile d'améliorer cet algorithme : si n n'est pas premier, l'un de ces diviseurs est plus petit que $\sqrt{n}$. Ainsi, il suffit de

tester les entiers entre 2 et $\sqrt{n}$. Dans le même ordre d'idées, citons le crible d'*Erathost*ène, qui permet de mettre la main sur tous les premiers entre 2 et n. A titre d'exemple pour déterminer tous les entiers premiers plus petits que 100, on procède comme suit : on écrit tous les entiers qui vont de 2 à 100 (rappelons que 1 n'est pas premier). Le premier entier écrit est 2. Il est premier : on l'entoure, et on barre tous ses multiples. Le premier entier non barré après 2 est 3 : il est premier, et on barre tous ses multiples. Le premier entier non barré après 3 est 5 : il est premier et on barre tous ses multiples. Et on procède comme ceci jusqu'à épuiser tous les entiers.... Ceux qui ne sont pas barrés sont exactement les premiers !
Voici un exemple pour déterminer tous les premiers de 1 à 40 :
Étape I

	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

Étape II

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	

Étape III

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			

Étape IV

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			

Les divisions et le crible d'*Erathotène* sont assez efficaces pour de petits entiers. Mais dès que ces entiers dépassent 50 chiffres, ils deviennent inutilisables ; ainsi il faut totalement changer de méthode.

Critère de *Fermat* :

Ce critère, repose sur le petit théorème de Fermat. On prend un entier a au hasard, et on calcule $a^{n-1} mod\ n$; si $a^{n-1} \not\equiv 1\ [mod\ n]$ alors n n'et pas premier.

Critère de *Euler* :

Ce critère, repose sur le Critère d'Euler. On prend un entier a au hasard, et on calcule $a^{\frac{n-1}{2}} mod\ n$; si $a^{\frac{n-1}{2}} \not\equiv (\frac{a}{n})\ [mod\ n]$ alors n n'et pas premier.

Critère de *Miller-Rabin* :

Le test de primalité de *Miller-Rabin* est un test de primalité probabiliste : c'est-à-dire un algorithme qui détermine si un nombre donné est probablement premier, de façon similaire au test de primalité de *Fermat*. Sa version originale, due à *G.L. Miller*, est déterministe, mais elle est reliée à l'hypothèse de *Riemann* généralisée non démontrée ; *M.O.Rabin* l'a modifiée pour obtenir un algorithme probabiliste inconditionnel.

Comme pour le Test de primalité de *Fermat*, celui de *Miller-Rabin* (à été donné par *Rabin* et *Miller* en 1977) consiste à tirer parti d'une équation ou d'un système d'équations qui sont vraies pour des valeurs premières, et à regarder si elles sont toujours vraies ou non pour un nombre dont nous voulons tester la primalité.

La difficulté crée par les nombres de CARMICHAEL peut être levée par la remarque suivante, due à Miller : si on trouve $a^{(n-1)/2} \equiv 1[mod\ n]$ et si $(n-1)/2$ est pair, on peut recommencer, et ainsi de suite.

Propriété : Soit $p > 2$, un nombre premier. Ecrivons $p-1 = 2^s.t$ avec t impair. Soit a un entier non divisible par p. Alors ou bien $a^t \equiv 1[mod\ p]$, ou bien il existe un entier i tel que $i < s$ et $a^{2^i.t} \equiv -1[mod\ n]$.

Corollaire 1. Soit $n < 1$ un entier impair. Ecrivons $n-1 = 2^s.t$ avec t impair. Supposons qu'il existe un entier a avec $1 < a < n$, $a^t \not\equiv 1[mod\ n]$ et $a^{2^i.t} \not\equiv -1[mod\ n]$ pour $i = 0, 1, ..., s-1$. Alors n est composé. (Appelons un tel entier a un témoin de *Miller*).

Propriété : Si le nombre impair n est composé, au moins les trois quarts des $n-2$ entiers a tels que $1 < a < n$ sont des témoins de *Miller* pour n.

Théorème(*Rabin*) Soit n un entier impair composé tel que $n > 9$. Posons $n-1 = 2^s.t$ avec t impair. Les entiers a compris entre 1 et n et qui satisfont à la condition $a^t \equiv 1[mod\ n]$ ou à l'une des conditions $a^{2^i.t} \equiv -1[mod\ n]$ pour $i = 0, 1, ..., s-1$ sont en nombre au plus $\varphi(n)/4$ (avec $\varphi(n)$ l'indicateur d'*Euler*).

Exemple :

Prenons l'exemple du nombre de CARMICHAEL 561, pour lequel on a $a^{560} \equiv 1[mod\ 561]$ pour tout a premier à 561 (on peut prendre a=2). Mais on a $560 = 2^4 \times 35$, $2^{2^3.35} \equiv 1[mod\ 561]$ et $2^{2^2.35} \equiv 67[mod\ 561]$, de sorte que 2 est un témoin de *Miller*.

TEST DE RABIN MILLER

Soit n un entier impair donné. A la question : n est-il premier, le test de *Rabin-Miller* donne l'une des réponses suivantes :
(1) Non, il est composé,
(2) La probabilité qu'il soit premier est x.
Remarque :
Le système de probabilité est ici l'équiprobabilité : les événements élémentaires ont la même probabilité.
La théorie sous-jacente est subtile et nous allons l'expliciter.
On écrit $n-1$ sous la forme $n-1 = 2^s t$, où t est impair. On choisit au hasard un entier b dans l'intervalle $[1, n-1]$ et on calcule les résidus dans $[0, n-1]$ des puissances suivantes de b modulo n :
$(S)\ \ b^t(mod\, n),\ \ b^{2t}(mod\, n),\ \ .....,\ \ b^{2^{s-1}}t(mod\, n),\ \ b^{n-1}(mod\, n).$

Définition 9. On dit que n passe le test de primalité de *Rabin-Miller* en base b si les deux résultats suivants

sont verifiés :
(i) $b^{n-1} \equiv 1[mod\ n]$,
(ii) Si le premier élément de (S) n'est pas égale a 1, et $b^{2^r}t$ est le premier élément égale a 1, alors l'élément précédent $b^{2^{r-1}}t(mod\ n)$ est $n-1$.

Définition 10. Un entier n est PSEUDOPREMIER fort en base b, si n est composé impair et s'il passe le test de *Rabin-Miller* en base b.

Définition 11. Soit n un entier composé impair et b dans l'intervalle $[1, n-1]$. Si n ne passe pas le test de *Rabin-Meller* en base b, alors on dit que b est un témoin de n.
On notera $t(n)$ le nombre de témoin de n et $b(n) = n-1-t(n)$ le nombre des bases pour lesquelles le nombre n passe le test.

Exemples numeriques :

I) Le nombre 9 a 6 témoins.
II) Considérons le nombre $n = 341$ et la base $b = 2$. On a $340 = 2^2 \times 85$.
Exécutons le test. La suite (S) est la suivante :
$2^{85} \equiv 32$, $2^{170} \equiv 1$, $2^{340} \equiv 1\ (mod\ 341)$.
On voit que le nombre 1 admet le nombre 32, qui est égal à $2^{85}(mod\ 341)$, comme racine carrée. Or $32 \neq \pm 1[mod\ 341]$ donc 341 est composé(en fait $341 = 11 \times 31$) et le nombre 2 est un témoin de 341.

Remarque :

(1) Si n est premier, alors n passe le test de *Rabin-Miller*. C'est essentiellement le théorème de *Fermat* dans le corps $(\mathbb{Z}/n\mathbb{Z})$.
(2) Si le résultat (i) n'est pas vérifié, alors le théorème de *Fermat* n'est pas vrai dans $(\mathbb{Z}/n\mathbb{Z})^*$, donc n n'est pas premier.
(3) Si le résultat (ii) n'est pas vérifié, c'est qu'il existe dans l'anneau $(\mathbb{Z}/n\mathbb{Z})$ un élément u tel que $u \neq \pm 1$ et $u^2 = 1$, ce qui n'est pas possible dans un corps, donc n n'est pas premier.
(4) Si n passe le test dans une base b, alors l'entier n est premier avec une probabilité supérieure à $\frac{3}{4}$.

Test de primalité de *lehmer* :
Grâce au test de Fermat, d'autre variété de test a été mise au point. Dans ce test on suppose donnée une décomposition en facteurs premiers de $p - 1$.

Proposition 1. **(Critère de *lehmer*)** Soit $n > 1$ un enter impair tel qu'on connaît tous les facteurs premiers de $n - 1$. Les conditions suivantes sont équivalentes :
(i) n est premier.
(ii) Il existe un entier a tel que $a^{n-1} \equiv 1[mod\, n]$ et $a^{(n-1)/q} \not\equiv 1[mod\, n]$ pour tout facteur premier q de $n - 1$.

Corollaire 2. Soit $n > 2$ un entier impair. Les conditions suivantes sont équivalentes :

(i) n est premier.
(ii) il existe un entier a tel que $a^{(n-1)/2} \equiv -1[mod\ n]$ et $a^{(n-1)/q} \not\equiv 1[mod\ n]$ pour tout facteur premier impair q de $n-1$.

Lemme 1. **(Critère de *Pocklington*)** Soit n un entier > 1. Ecrivons $n-1 = q^r m$, avec q premier et $r \geq 1$. Supposons qu'il existe un entier a avec $a^{q^r} \equiv 1[mod\ n]$ et $pgcd(a^{q^{(r-1)}} - 1; n) = 1$. Alors tout facteur premier de n est congru à 1 modulo q^r.

Proposition 2. **(Critère de *Lehmer-Pocklington*)** Soit n un entier > 1. Écrivons $n-1 = uv$, les facteurs premiers de u étant connus. Supposons qu'il existe pour chaque facteur premier q de u, en désignant par q^r la plus grande puissance de q qui divise u, un entier a_q avec ${a_q}^{q^r} \equiv 1[mod\ n]$ et $pgcd({a_q}^{q^{(r-1)}} - 1, n) = 1$. Alors tout facteur premier p de n est congru à 1 modulo u. Si on a de plus $v \leq u+1$, alors n est premier.

LES NOMBRES DE FERMAT ET LES NOMBRES DE MERSENNE

Pour les nombres de FERMAT, le critère de *Lehmer* devient :

Lemme 2. Pour que F_n soit premier, il faut et il suffit qu'il existe a avec

$$a^{(F_n-1)/2} \equiv -1[mod\ F_n].$$

Soit $M_n = 2^n - 1$ un nombres de *Mersenne* ; alors on a : si M_n est premier alors n est premier.

Critère de *Lucas*

En 1876 le mathématicien *Edouard Lucas* énonce une méthode irréfutable permettant de déterminer si un nombre n est premier. Par exemple le nombre $n = 257$, $n - 1 = 256 = 2^8$, pour montrer que n est premier, il suffit de trouver un nombre b tel que b^{256} est congru à 1 modulo 257 et tel que $b^{256/2}$ n'est pas congru à 1 modulo 257. Le nombre b est choisi au hasard. Cependant, la méthode de Lucas n'est applicable qu'à des nombres ayant une forme spéciale : elle ne s'applique que si on détermine les facteurs premier de $n - 1$.

Tests déterministes :

Le (n - 1)-test :

Le (n - 1)-test est un test de primalité des nombres n tels que l'on connaît la factorisation primaire de n - 1. C'est le cas des nombres de FERMAT $F_k = 2^{2^k} + 1$. L'énoncé suivant est essentiellement dû à *Lucas* (1876) mais *Lehmer* en a simplifié les hypothèses.

Théorème 20. *(Test de primalité de Lucas-Lehmer) : Soit*

n un entier > 1. S'il existe un entier a tel que, pour tout facteur premier p de $n-1$, $a > 1$, $a^{n-1} \equiv 1(mod\ n)$ et $a^{(n-1)/p} \neq 1(mod\ n)$, alors n est premier.

Pour les nombres de FERMAT $F_n = 2^{2^n} + 1$, on a un test dû à *Péepin* en 1877.

Théorème 21. *Pour $n \geq 1$, on a : F_n est premier $\Leftrightarrow 3^{(F_n-1)/2} \equiv -1(mod\ F_n)$.*

Le (n + 1)-test :

Théorème 22. *(Théorème de Lucas-Lehmer sur les nombres de* MERSENNE*)*
Soient s un nombre premier impair, $n = 2^s - 1$, a un entier tel que n soit premier avec $a^2 - 4$.
On définit par récurrence une suite d'entiers, (L_i) où $i \geq 1$, dite suite majeure de Lucas, comme suit : $L_1 = a$, $L_{i+1} = {L_i}^2 - 2$.
Alors on a : $L_{s-1} \equiv 0(mod\ n) \Leftrightarrow n$ est premier.

Les suites de *Lucas* :

Définition 12. Soit A un anneau et a un élément de A. La suite de *Lucas* de l'anneau A, associée à a, est la suite $(V_n)_{n\geq 0}$, définie par :

Conditions initiales : $V_0 = 2.1_A$, $V_1 = a$.
Formule de récurrence : $V_{n+1} = aV_n - V_{n-1}$, pour $n \geq 2$.

Lemme 3. *Soit A un anneau et a un élément de A. on considère la suite de Lucas (V_n) associée à a.*
I S'il existe un élément inversible x de A tel que $x+x^{-1} = a$, alors $V_n = x^n + x^{-n}$ pour tout $n \geq 0$.
II Réciproquement, si (V_n) est la suite de Lucas associée à a, il existe une extension d'anneaux A sur B telle que l'anneau B contienne un élément inversible x vérifiant $x + x^{-1} = a$.

Remarque :

On est donc habilité, pour étudier les propriétés d'une suite (V_n) de *Lucas*, à supposer l'existence d'un élément inversible x tel que la relation $V_n = x^n + x^{-n}$ soit vérifiée pour tout n. On obtient ainsi les relations suivantes :
$V_n V_m = V_{n+m} + V_{n-m}$
$V_{2n-1} = V_n V_{n-1} - a$
$V_{2n} = V_n^2 - 2$
$V_{2n+1} = aV_n^2 - V_n V_{n-1} - a$
$V_n = 2 \Leftrightarrow x^n = 1$

Théorème 23. *(Critère de primalité de Lucas-Lehmer) : Soient :*
• *n un entier impair > 1 tel qu'on connaisse la décomposition de $n+1$ en facteurs premiers,*
• *a un entier tel que $pgcd(n, a^2 - 4) = 1$,*
• *V_n la suite de Lucas définie par : $V_0 = 2$, $V_1 = a$ et la formule de récurrence : $V_{n+1} = aV_n - V_{n-1}$.*
Si $V_{n+1} \equiv 2 (mod\ n)$ et $pgcd(V_{(n+1)/q} - 2, n) = 1$ pour tout

facteur premier q de $n+1$, alors n est premier.

Théorème 24. *Soit s un entier impair > 1, $n = M_s = 2^s - 1$, le nombre de Mersenne et (L_n) la suite majeure de Lucas. Alors on a :*
n est premier $\Leftrightarrow L_{s-1} \equiv 0(mod\ n)$.

Chapitre 5

Application en cryptographie

1 Introduction

Depuis des temps très reculés dans l'histoire, les messages secrets étaient utilisés pour plusieurs raisons et surtout pour des raisons diplomatiques ou militaires. Ces messages secrets sont des messages qu'on écrit tout d'abord d'une façon naturelle, puis suivant certaines méthodes, on transforme les lettres originales du message en d'autres lettres ou nombres, de telle façon que le contenu du message obtenu soit illisible ou caché. Par suite, on dira que le message est codé ou bien chiffré. Les méthodes de codage et de décodage ont évolué avec le temps, et ils ont trouvé d'autres applications en Informatique, en télécommunication, en sécurité des transactions banquaires et d'autres. Ainsi, l'art des messages secrets est devenu une science.

Définition 13. La cryptologie c'est la science des messages secrets. Elle se partage en deux parties : la cryp-

tographie et la cryptanalyse :
- La cryptographie c'est la science des écritures cachées et des mécanismes qui assurent leurs secrets.
- La cryptanalyse est la science qui analyse ces écritures et déjoue les mécanismes de protection afin de découvrir leurs contenus.

Parmi les premières méthodes de cryptographie, on trouve celle de la scytale qui n'est qu'un bâton sur lequel on enroule une lanière, en spire jointive, et sur laquelle on écrit le message. Une fois la lanière déroulée, l'ordre des lettres inscrites initialement ne reste plus le même. En envoyant la lanière, son contenu ne sera dévoilé que si elle est enroulé sur un bâton de même diamètre que celui utilisé initialement. Cette méthode a été utilisée par les militaires et surtout les officiers qui ont des bâtons de même diamètre.
Une autre méthode, dite de substitution, consiste à changer chaque lettre du message par la n-ième lettre qui la suit. Le nombre n est alors la clef du secret. La méthode de César est un cas particulier de cette dernière, puis que c'est le cas où $n = 3$.
Au 9-ième siècle, le cryptanalyste Arabe Al-Kindi, a donné une méthode pour décoder tout message codé par substitution dans n'importe quelle langue. Ainsi, Al-Kindi est le premier casseur de la méthode de substitution.
Au début du 20-ième siècle, on a remarqué un passage des méthodes de substitution, de transposition de

lettres et d'autres, à des méthodes mécaniques, notamment celle qui utilisait la machine mécanique Enigma, pour transformer ou coder les messages. Dans la deuxième moitié du 20-ième siècle, on a vécu le passage des méthodes mécaniques aux méthodes Algorithmiques qui utilisent comme moyen materiel l'ordinateur. Les méthodes Algorithmiques se basent essentiellement sur certaines questions difficiles à résoudre en pratique même à l'aide d'un supperordinateur. Ces questions sont, dans la plus grande partie, issues des Mathématiques (factorisation des grands nombres, courbes elliptiques sur des corps finis, $\cdots$); mais qu'on peut trouver dans d'autres disciplines comme la physique quantique (pour plus de détail voir [8], [9], [10]).
Les méthodes de cryptographie se partagent en deux types importants : celles à clef publique et celles à clef secrète. La méthode de substitution est à clef secrète et qui n'est rien autre que le nombre n, tandis que la méthode RSA, suivante, est à clef publique. Pour plus de détail voir [8], [9], [10]).

2 Méthode RSA

Inventée en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman ; la méthode RSA est utilisée par plus de 400 million de Logiciels aujourd'hui. Cette méthode se base sur la factorisation des nombres en produit de nombres premiers. Vu cette relation avec les nombres,

on va expliquer en détail sur quoi elle se base et comment l'utiliser.

Préliminaires

Soit n un entier naturel supérieur à 2. On désigne par $\mathbf{Z}_n^*$ le groupe des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$. Fermat avait démontré le théorème suivant :

Théorème 25. *Soient p un nombre premier et a un entier positif inférieur strictement à p, alors on a :*

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

Ce dernier théorème (connu sous le nom du petit théorème de Fermat) a été généralisé, pour un entier n quelconque, en 1760 par Euler :

Théorème 26. *Soient n un entier positif supérieur à 2, a un entier premier avec n et $\phi(n)$ l'ordre du groupe $\mathbf{Z}_n^*$, alors on a :*

$\phi(n) = (p_1-1)p_1^{r_1-1} \cdots (p_s-1)p_s^{r_s-1}$ *si* $n = p_1^{r_1} \cdots p_s^{r_s}$ *et* $a^{\phi(n)} \equiv 1 \bmod n$.

En général, si a et n ne sont pas premiers entre eux on n'a pas toujours $a^{\phi(n)} \equiv 1 \bmod n$. Mais dans certain cas on a des résultats qui ressemblent à ce dernier ; comme le montre le résultat suivant :

Théorème 27. *Soient n un entier sans facteurs carrés et a un entier positif inférieur strictement à n ; alors on a :*

$$\forall k \in \mathbf{Z},\ a^{k\phi(n)+1} \equiv a \bmod n$$

Preuve : Voir [11].

Codage et décodage d'un message

On se donne le message suivant :

Attaquez

Je doit envoyer secrètement ce message à une personne X. Cette personne doit avoir une clef publique qui n'est rien autre que deux entiers n_X et s_X vérifiant les conditions suivantes :
i. $n_X = pq$ où p et q sont des nombres premiers,
ii. p et q sont gardés secrets par chacun,
iii. l'entier s_X est premier avec l'entier $(p-1)(q-1)$.

Remarque 28. La clef du destinataire doit se trouver dans un annuaire, exactement comme un numéro de téléphone. Seul le propriétaire de la clef doit connaître la décomposition de l'entier n_X en produit de nombres premiers : car, cette décomposition permet de décoder tout message codé avec cette clef.

On se demande sous quelle forme on va écrire notre message et comment le coder.

1. **Transformation du message.**

On considère les transformations suivantes :

A = 01	K = 11	U = 21	1 = 31
B = 02	L = 12	V = 22	2 = 32
C = 03	M = 13	W = 23	3 = 33
D = 04	N = 14	X = 24	4 = 34
E = 05	O = 15	Y = 25	5 = 35
F = 06	P = 16	Z = 26	6 = 36
G = 07	Q = 17	, = 27	7 = 37
H = 08	R = 18	. = 28	8 = 38
I = 09	S = 19	? = 29	9 = 39
J = 10	T = 20	0 = 30	! = 40

Pour désigner un vide entre deux mots on écrit le nombre 00. Ainsi notre message devient un nombre M :

$$M = 0120200117210526$$

2. **CODAGE DU MESSAGE.**

On coupe M en morceaux plus petits que n_X.

EXEMPLE : $n_X = 37 \times 41 = 1517$.

$$M = 0120200117210526 = \underbrace{0120}_{M_1}\,\underbrace{200}_{M_2}\,\underbrace{117}_{M_3}\,\underbrace{210}_{M_4}\,\underbrace{526}_{M_5}.$$

On travaille, dans la suite, successivement avec chaque morceau $M_1...M_5$.
Le message codé devient $\overline{M}$:

$$\underbrace{...}_{\overline{M}_1}\underbrace{...}_{\overline{M}_2}\underbrace{...}_{\overline{M}_3}\underbrace{...}_{\overline{M}_4}\underbrace{...}_{\overline{M}_5}.$$

Où $\overline{M}_i$ est le reste de la division de $(M_i)^{s_X}$ par n_X pour $i = 1, ..., 5$.

3. **DECODAGE DU MESSAGE.**

Le destinataire reçoit le message codé $\overline{M}$. Comme il connaît la décomposition $n_X = pq$ et on sait que s_X est premier avec $(p-1)(q-1)$; alors il existe un entier t_X tel que

$$1 \leq t_X < (p-1)(q-1) \ \ et \ \ s_X t_X \equiv 1 \bmod (p-1)(q-1).$$

Le destinataire peut donc facilement calculer l'entier t_X. Personne d'autre ne peut le calculer tant que la décomposition de n_X reste secrète. Pour décoder le message on calcule le reste de la division de $(\overline{M}_i)^{t_X}$ par n_X pour $i = 1, ..., 5$. Ce reste n'est rien d'autre que l'entier M_i pour $i = 1, ..., 5$.
Ainsi le message décodé est bien

$$M = 0120200117210526 = \underbrace{0120}_{M_1}\underbrace{200}_{M_2}\underbrace{117}_{M_3}\underbrace{210}_{M_4}\underbrace{526}_{M_5}.$$

Remarques 29. 1. Comme $s_X t_X \equiv 1 \bmod (p-1)(q-1)$; alors il existe un entier k tel que $s_X t_X = 1 + k(p-1)(q-1) = 1 + k\phi(n_X)$. D'après le théorème 13, on a :

$$(\overline{M_i})^{t_X} \equiv ((M_i)^{s_X})^{t_X} \equiv (M_i)^{s_X t_X} \equiv M_i \bmod n_X.$$

2. Les nombres $M,\ M_1, ..., M_5$ ne sont pas nécessairement premiers avec n_X.
3. L'entier t_X est une clef secrète.

4. **SIGNATURE DU MESSAGE.**

Une personne est identifiée par sa clef publique, et elle est parfaitement identifiée par sa clef publique et sa signature que seul lui peut la signer. Donc un message, pour plus de securité, doit être signé. On va décrire, comment on signe un message crypté en RSA.
J'ai envoyé un message M à une personne X, que j'ai transformé à l'aide des entiers n_X et s_X. La personne X va décoder le message avec sa clef secrète t_X. Mais qui prouve que c'est bien moi qui a envoyé ce message ; ma clef publique est publique et n'importe qui peut l'utiliser ! Donc je doit ajouter ma signature à ce message.
Moi aussi, Azizi Abdelmalek, j'ai une clef publique (n_A, s_A) et une clef secrète t_A. J'ajoute au message M ma signature M^{t_A}. Pour que X s'assure que c'est bien moi qui a envoyé le message M, il calcule

$$(M^{t_A})^{s_A} \bmod n_A.$$

S'il trouve M, alors c'est bien moi. Sinon, c'est que le message ne vient pas de moi.

Chapitre 6

Le logarithme discret et la cryptographie

1 Logarithme discret

Soient G un groupe cyclique fini dont la loi de composition est notée multiplicativement et a un générateur de G. Si l'ordre de G est égal à n (c'est à dire le nombre des éléments de G) et e est l'élément neutre de G ; alors $a^n = e$ et

$$G = \{e, a, a^2, a^3, ..., a^{n-1}\}.$$

Ainsi pour tout élément h de G, il éxiste un entier naturel $m < n$ tel que $h = a^m$. L'entier m est appelé le logarithme discret de h relativement à la base a et on note alors

$$dlog_a(h) = m.$$

Comme tout entier m s'ecrit sous la forme

$$m = \sum_{i=0}^{i=r} \epsilon_i 2^i$$

où $\epsilon_i \in \{0, 1\}$ et r est un entier naturel, alors pour tout $h \in G$ on a

$$h = a^m = a^{\Sigma_{i=0}^{i=r} \epsilon_i 2^i} = \Pi_{i=0}^{i=r} a^{\epsilon_i 2^i}.$$

Par suite, le calcul de h dans G revient au calcul des éléments a^{2^i} et de leurs produits.

Il n'est pas facile en général de trouver le logarithme d'un élément quelconque de G. Cette dificulté de résoudre ce problème dans certains groupes G est utilisé en cryptolographie pour coder des messages, comme le montre le paragraphe suivant.

2 Application du logarithme discret à la cryptographie

2.1 Clés d'échange de messages

Diffie et Helman ont construit une méthode d'échange de clés entre deux personnes, (Ahmed(A) et Bachir(B)), qui veulent communiquer entre elles ; la méthode est la suivante :
1. les deux personnes doivent se mettre d'accord sur le générateur a du groupe G et de son ordre n.
2. Ahmed choisie un entier non nul x tel que $x < n$ et qu'il garde secret, calcule $X = a^x$ et l'envoie à Bachir.
3. Bachir choisie un entier non nul y tel que $y < n$ et qu'il garde secret, calcule $Y = a^y$ et l'envoie à Ahmed.
4. Ahmed calcule $Y^x = (a^y)^x = a^{yx}$ et Bachir calcule

$X^y = (a^x)^y = a^{xy}$.
Ainsi Ahmed et Bachir ont le même élément a^{yx}. En plus, Ahmed garde son x secret et Bachir garde son y secret. L'élément a^{yx} est alors la clé que Ahmed et Bachir se sont échangés.

2.2 Criptage d'un message : Criptage d'ElGamal

Le système de cryptage d'ElGamal est un exemple de cryptage en liaison avec l'échange de clè de Diffie-Hellman défini sur le groupe $(Z/pZ)^*$. La securité de ce système de cryptage est basé sur la dificulté de résoudre le problème du logarithme discret dit aussi problème de Diffie-Hellman dans le groupe $(Z/pZ)^*$.
Alors si Ahmed veut envoyer un message m à Bachir, il calcule $c = g^{xy}m$ et envoie (X, c) à Bachir. Pour décrypter ce message, Bachir doit tout simplement multipler par l'inverse de la clè dans le groupe G :

$$m = a^{p-1-xy}c = a^{p-1-xy}a^{xy}m.$$

Ceci reste vrais pour un groupe G quelconque où le problème de Diffie-Hellman est dificile à résoudre .

2.3 Exemples de groupes utilisés

En plus du groupe multiplicatif $(Z/pZ)^*$, plusieurs autres groupes sont utilisés en vue d'appliquer le système

de cryptage d'ElGamal . Dans ce paragraphe, on va voir deux autres groupes qui sont utilisés en cryptographie.

1. Groupe élliptique.

Soient $p > 3$ un nombre premier et a et b deux éléments de $(Z/pZ)^*$. On concidère l'équation suivante

$$y^2z = x^3 + axz^2 + bz^3$$

et son discriminant

$$\triangle = 16(4a^3 + 27b^2).$$

On suppose que $\triangle$ est non nul. On définit une relation d'équivalence R sur l'ensemble des solutions de l'équation précédente dans $(Z/pZ)^*$ par $(x, y, z)\ R\ (x', y', z')$ si et seulement si il exite un $c \in (Z/pZ)^*$ tel que $(x, y, z) = c(x', y', z')$. La classe de (x, y, z) est noté par $(x : y : z)$ et l'ensemble des classes d'équivalence modulo R est noté par $E(p; a, b)$. Si $z \neq 0$ alors la classe de (x, y, z) contient un seul élément $(x, y, 1)$ où $y^2 = x^3 + ax + b$. Ansi

$$E(p; a, b) = \{(x : y : 1) : y^2 = x^3 + ax + b\} \cup \{(0 : 1 : 0)\}.$$

Pour simplifier on va noter $(x : y : 1)$ par (x, y) et $(0 : 1 : 0)$ par O.

Parsuite on appele courbe élliptique modulo p l'ensemble

$$E(p; a, b) = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{O\}.$$

On définit sur $E(p; a, b)$ une addition par :

$$P + O = O + P = P$$

pour tout point P de la courbe et si $P = (x, y)$ on pose $-P = (x, -y)$. Si P_1 et P_2 sont deux points tels que $P_i = (x_i, y_i)$ et $P_1 \neq -P_2$, alors

$$P_1 + P_2 = (x_3, y_3)$$

où

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

et

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ si } P_1 \neq P_2$$

et dans le cas contraire

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

Alors muni de cette loi $E(p; a, b)$ est un groupe abélien. Le grand Mathématicien Hasse, nous a donné une estimation de $n = |E(p; a, b)|$:

$$n = |E(p; a, b)| = p + 1 - t;$$

où l'entier relatif t est tel que $t \leq 2\sqrt{p}$.

2. Groupe de classes d'un corps de nombre

Soient $\mathbb{k}$ un corps de nombres et A l'anneau des entiers algébriques de $\mathbb{k}$.

1) Soit M un ensemble non vide muni d'une loi $+$ et tel que :

i) $(M, +)$ est un groupe abélien.

ii) Il existe une application f définie de $A \times M$ dans M par $x \overset{f}{\longmapsto} a.x$ tel que :
$\forall (a,b) \in A^2 \; \forall (x,y) \in M^2$ on a :
$(a+b).x = a.x + b.x$
$a.(x+y) = a.x + a.y$
$(ab).x = a.(b.x)$
$1.x = x.$

Alors M est appelé un A- module. Un sous-A-module de M est un sous-groupe de $(M,+)$ qui vérifie en plus la condition $ii)$.
2. Soit H un sous A- module de $K \neq \{0\}$.
On dit que H est un idéal fractionnaire de A (ou de K) si et seulement si, il existe $d \in A^*$ tel que $dH \subset A$.
3. On appele groupe de classes de $\mathbb{k}$, le quotient de l'ensemble des idéaux fractionaires par l'ensemble des idéaux fractionaires principaux. Muni de l'addition, ce dernier quotient est un groupe abélien.

Le groupe de classes d'un corps de nombres est un groupe fini. Parmi les corps de nombres utilisé à cette fin on trouve les corps quadratiques imaginaires $\mathbb{Q}(\sqrt{-\mathsf{d}})$ où d est entier positif. En particulier, le groupe de classes d'un corps $\mathbb{Q}(\sqrt{-\mathsf{d}})$ où $d > 0$, est produit de n groupes cycliques où n est le nombre de premiers différents divisant d. Par suite on a une relation entre la décomposition d'un entier n en produit de nombres premiers et la décomposition du groupe de classes de $\mathbb{Q}(\sqrt{-\mathsf{n}})$ en

produit de groupes cycliques.

Chapitre 7

Les Mots de passe

1 Les fonctions à sens unique

On dit qu'une fonction f est facile à évaluer si et seulement si l'image $f(x)$ de x par f est calculable dans un temps polynomial de la taille de la donnée x. Une fonction à sens unique, ou ce qu'on dit en Anglais fonction " One-Way", est une fonction bijective facile à évaluer et telle que sa réciproque est inconnue.

Exemples

1. Soient G un groupe cyclique d'ordre un nombre premier p, g un générateur de G et $\mathbb{Z}_{p-1}$ le groupe multiplicatif des classes d'équivalences modulo p dans $\mathbb{Z}$. On défint une fonction f par :

$$f : \mathbb{Z}_{p-1} \longrightarrow G$$

qui à n fait correspondre $f(n) = g^n$. Comme le calcul d'une exponentielle se fait en un temps polynomial et f est une bijection, dont la reciproque n'est pas connue si le nombre premier est bien choisie, alors la fonction

f est à sens unique.
2. Soient $n = pq$, produit de deux nombres premiers différents, et E_n le groupe multiplicatif des classes d'équivalences modulo n inversibles pour la multiplication. On suppose que la factorisation de n est connue, on définit une fonction f par : $f(m) = m^e$ où e est l'entier défini dans la méthode RSA. Alors cette fonction est à sens unique.

2 Mots de passe

L'accès à un ordinateur, avec un système d'éxploitation comme Unix ou Windows NT, est controlé par un système de mots de passe. Chaque utilisateur choisie son mot de passe X ; l'ordinateur, à l'aide d'une fonction à sens unique f, garde dans sa mémoire une image de $f(X)$. Quand un utilisateur vient pour accéder à son compte, il compose son mot de passe X et l'ordinateur calcule $f(X)$ et compare le résultat obtenu à l'image ou le nombre $f(X)$ qui éxiste déja dans la mémoire de l'ordinateur. S'il y a identification alors l'accès est permis, sinon il est refusé.

Ce même procédé est utilisé pour plusieurs genres de mots de passe, en particulier on le retrouve dans le cas de mots de passe gravé sur les cartes bancaires. L'orsqu'on fait entrer notre carte dans la machine de dis-

tribution pour la première fois , on nous demande de choisir un mot de passe X et la machine à l'aide d'une fonction à sens unique f calcule $f(X)$ et garde sa valeur ou son image $f(X)$ dans sa mémoire. L'orsqu'on fait entrer notre carte dans la machine de distribution une deuxième fois on nous demande de donner notre mot de passe X et la machine calcule $f(X)$ et le compare à la valeur ou l'image $f(X)$ qui est gravé sur la carte. S'il y a identification alors l'accès est permis, sinon il est refusé.

Chapitre 8

Les nombres une distraction et aussi un défi

1 Jouer Pile ou Face par e-mail

Soient p et q deux nombres premiers impairs, $n = pq$ et m un entier strictement inferieur à n. A l'aide du symbole de Legendre on peut savoir si l'équation

$$(*) \quad X^2 \equiv m \bmod n$$

est résoluble ou non. Si oui, alors on sait, que dans notre cas on a quatre solutions x, $n - x$, y et $n - y$. De plus on sait que, à une permutation près, le PGCD de $x + y$ et n est égal à p et le PGCD de $x + (n - y)$ et n est égal à q. Ceci vient du fait que si x et y sont deux solutions de l'équation $(*)$, alors

$$x^2 \equiv y^2 \bmod pq$$

et donc pq divise $(x + y)(x - y)$. Par suite, si les deux termes du produit sont non nuls, alors on a (à une permutation près) que p divise $x + y$ et q divise $x - y$ (si y

= x ou y = n-x, alors l'un des deux termes précédents est nul et donc le raisonnement précédent n'est plus valable).
Alors, on peut utiliser cette théorie pour jouer "Pile ou Face" via le théléphone ou par e-mail de la façon suivante :
C'est un jeu entre deux personne A et B.
1. Le joueur A choisit deux nombre premiers impairs, les plus grands possibles, pour que la factorisation de $n = pq$ soit difficile pour B, et il envoie n à B.
Le joueur B doit trouver la factorisation de n, en procédant comme suit :
2. Le joueur B choisit un nombre x strictement plus petit que n et envoie $m \equiv x^2 \bmod n$ à A.
3. Maintenant, Le joueur A qui sait que $n = pq$, calcule les quatre solutions de l'équation

$$X^2 \equiv m \bmod n$$

et il doit envoyer l'une de ces solutions à B au hasard. Si A a envoyé la solution y (ou bien n-y) à B, alors B en calculant $x+y$ et $x-y$ il peut trouver la factorisation de n ; et dans ce cas B est le gagnant. Si A a envoyé x ou $n - x$, alors B est perdant : car il ne pourra pas utiliser la solution reçue pour factoriser n.

2 Les carrés magiques

Les carrés magiques sont une occupation sans interêt mathématique pour le moment. Plusieurs Mathématiciens, des Grecs en passant par les Arabes et en arrivant au Mathématiciens de L'Europe comme Euler, ont été attirés par la construction des carrés magiques. Ils nous ont laissé beaucoup d'exemples.

Définition 14. Un carré magique est un tableau à n lignes et n colonnes, plein de nombres, tel que les sommes des nombres appartenant à une ligne, les sommes des nombres appartenant à une colonne, ou les sommes des nombres appartenant à une diagonale coincident toutes avec un même nombre s.

Propriétés. 1. Si on ajoute un même nombre à tous les nombres du carré magique, on obtient un carré magique.
2. Si on multiplie tous les nombres du carré magique par un même nombre, on obtient un carré magique.
Exemples. 1. Un carré magique d'ordre 3.

2	9	4
7	5	3
6	1	8

2. Un carré magique d'ordre 4

7	12	1	14
2	13	8	11
16	3	10	5
9	6	15	4

3. Un carré magique d'ordre 5.

23	8	5	4	25
20	14	15	10	6
19	9	13	17	7
2	16	11	12	24
1	18	21	22	3

Ceci est un carré magique dont le carré central d'ordre 3 est aussi un carré magique.

3 Les nombres et les Fractals

Pour le moment, les spécialistes refusent de donner une définition pour les Fractals. Pour le dictionnaire Larousse les Fractals " *se sont des objets mathématiques dont la création ou la forme ne trouve ses règles que dans l'irregularité ou la fragmentation, et des branches mathématiques qui étudient de tels objets* ".
Certaines Fractals sont obtenues à partir d'ensembles de points qui sont en relation avec des nombres ou avec certaines représentations de nombres comme le

montre l'exemple suivant :
On sait que tout nombre réel s'écrit sous la forme

$$\sum_k \epsilon_k 2^k \text{ où } k \in \mathbb{Z}, \ \ \epsilon_k \in \{0, 1\}.$$

De plus, tout nombre complexe peut s'écrire sous la forme

$$\sum_k \epsilon_k (1-i)^k \text{ où } i = \sqrt{-1}, \ k \in \mathbb{Z}, \ \text{ et } \epsilon_k \in \{0, 1\}.$$

Si on s'amuse à regarder quelle partie du plan va être occupé par les complexes qui sont tels que $\epsilon_k = 0$ pour tout k positif ou nul ; alors on trouve une figure qui ressemble à un double dragon. Ceci est connue dans le monde des Fractals par " Twin-Dragon".

Pour plus de détail et plus d'exemples en relations avec les nombres, on peut voir [12].

4 Les nombres, la musique et la poésie

Beaucoup de mathématiciens, n'ont pas seulement pratiqué la musique ou la poésie, mais ils ont contribué au dévelopement et à la structuration de la musique ou de la poésie.
La musique était adorée par de grands mathématiciens ; elle était pour certains une occupation et pour d'autres une discipline d'applications de l'arithmétique. Parmi

ces mathématiciens, qui ont laissé des traces sur la musiques, on trouve Pythagore à qui on attribue la relation

$$N \times L = c^{te}$$

où N est la fréquence du son émis, L la longueur de la corde qui vibre et c^{te} est une constante. On trouve aussi, Platon, Plotin, Saint-Augustin, Al Farabi, Avicenne, Descarte, d'Alembert, Euler et d'autres.
Le mathématicien Euler définissait la musique comme étant la science de combiner les sons de manière qu'il en résulte une harmonie agréable. Euler avait construit des échelles musicales suivant des règles d'Arithmétique. A titre d'exemple, le nombre des notes dans une octave est égal au nombre de diviseurs d'un entier donné parmi les éléments du monoide engendré par 3 et 5. On trouve d'autres relations arithmétiques cachées dans la construction musicale de Euler. Pour plus de détail voir [6].
La poésie à aussi une relation avec les nombres et surtout la poésie Arabe. La poésie Arabe traditionnelle est caractérisée par le fait que deux vers ont un même nombre de mots un même nombre de lettres et un même nombre de son phonétique.
La poésie Arabe se partage en plusieurs classes ; l'une d'elle s'appèle " Al Orjouza". Al Orjouza est une poésie reservée à des sujets éducatifs tels que la grammaire et l'Arithmétique. C'est ainsi qu'on trouve plusieurs poésies en Arithmétique. A titre d'exemples on cite :

1. Ibn Yassmin (12 ième ciècle)
Il a écrit un livre sous forme d'une poésie intitulé " Orjouzat Ibn Yassmin". C'est un livre qui traite des questions d'Arithmétique et des questions sur la résolution des équations du second degré.
2. Ibn Razi (15 ième ciècle)
Il a écrit un livre sous forme d'une poésie intitulé " Kitab Mouniat Al Houssab fi Ilm Al Hissab". C'est un livre d'Arithmétique.

Parmi les poètes mathématiciens on trouve Omar Al Khayam qui a travaillé sur les équations du second degré et du troisième degré. Il a une poésie celèbre qui s'appèle " Robaiat Al Khayam". C'est une poésie combinaison de plusieurs poésies à quatre vers. Donc elle a une relation avec le nombre quatre. Je pense que à travers cette poésie Al Khayam caressait les équations de degré quatre et il avait lancé un appel à la résolution de ces équations.
Jusqu'à present, beaucoup de mathématiciens sont attirés par la musique ou la poésie et le phénomène " Nombres, musique et poésie" persiste encore !

5 Nombres records.

1. Le nombre des atomes est estimé à 10^{80}.
2. La durée de vie de notre univers est d'environ 10^{20}

s.
3. L'un des plus grands nombres premiers $2^{1257787}-1$ s'écrit avec 378632 chiffres.
4. En 1995 le professeur Yasumasa Kanada a donné le π le plus précis du monde : 6442450938 chiffres après la virgule (116h de calcul 131h de vérifications). Les calculs ont été effectués sur un Hitachi S-3800/480.
5. Euler (1707-1783) avait conjecturé qu'il n'y a pas de solutions entières pour l'équation

$$x^4+y^4+z^4=u^4.$$

En 1988 Noam Elkies a trouvé un contre exemple :

$$95800^4+217519^4+414560^4=422481^4.$$

6. En 1996 Thomas Nicely a découvert que son pentium donnait des resultats incorrects pour la division de 1 par le nombre 824633702441 ; ce qui montre l'utilité des grands nombres pour tester la fiabilité et la résistance des super-calculateurs.

6 Problèmes ouverts.

1. Finitude des nombres amiables, des nombres premiers jumeaux et des nombres premiers de la forme n^2+1.
2. Conjecture de Goldbach : tout nombre pair est somme de deux nombres premiers.
3. Fermat croyait que tout nombre de la forme 2^n+1

est premier ; ceci est vrais pour $n = 0,\ 1,\ 2,\ 3,$ et 4 mais pour $n = 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12, 2^n + 1$ n'est pas premier. On se demande s'il existe d'autres nombres premiers de cette forme (ces nombres sont appelés nombres de Fermat).

4. Constante d'Euler :

$$\gamma = \lim_{n\to\infty}(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \frac{1}{n} - \log n) = 0,5772156649.$$

On ne sait pas encore si γ est irrationel ou encore moin s'il est transcendant.

Bibliographie.

[1] H. Cohn, *Advanced Number Theory*, Dover Publications, Inc New York.

[2] G. Frei, *Henrich Weber and the Emergence of Class Field Theory.*

[3] G. Frei, *the Reciprocity Law From Euler to Artin.*

[4] J.M. Gandhi, *Formula for the n-th prime.* Proc. Washington State Univ. Conf. Number Theory, Pullman, 1971, 96 - 106.

[5] Richard K. Guy, *Unsolved Problems in Number Theory, Second Edition.* Springer-Verlag.

[6] Y. Hellegouarch, *A la recherche de l'Arithmétique qui se cache dans la musique*. Gazette des Mathématiciens, N.33, 1987.

[7] H. Loo-Keng, *Introduction to Number Theory*, Springer-Verlag Berlin Heidelberg New York.

[8] Pour La Science, *Dossier hors série sur la Cryptographie*. Juiller-octobre 2002.

[9] P. Ribenboim, *Les nombres : des amis qui nous donnent des problèmes.* Conférence de théorie des nombres. Université Laval Québec 1987.

[10] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser progression, math. vol 57,1985.

[11] G. Robin, *Cryptographie et algorithmique*, Ellipses, 1991.

[12] M.R. Schroeder, *Number theory in Science and communication*. Springer-Verlag, second Enlarged Edition, 1985.

[13] J.P. Serre, *Cours d'arithmétique.* Presses universitaires de France.

[14] B. L. Vander Waerden, *A History of Algebra.* Springer-Verlag, New York Heidelberg Berlin, 1985.

[15] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York Heidelberg Berlin.

[16] A. Wiles *Modular elliptic curves and Fermat's last Theorem*, Annales of Mathematics, 142 (1995), 443-551.