ÉCOLE DE RECHERCHE CIMPA-MAURITANIE
THÉORIE ALGORITHMIQUE DES NOMBRES ET CRYPTOGRAPHIE
NOUAKCHOTT

TESTS DE PRIMALITÉ, RSA, LOGARITHME DISCRET, DIFFIE-HELLMAN ET EL GAMAL CLASSIQUE

NOTES DU COURS DU PR. ABDELMALEK AZIZI

15-26 Février 2016

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 ٠, ١, ٢, ٣, ٤, ٥, ٦, ٧, ٨, ٩, ٠٠٠.

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 ; où on trouve plusieurs définitions et théorèmes d'arithmétique. 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 Romains, 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 théoriques et appliqués. Parmis les axes appliqués on trouve la Cryptographie, science des messages secrets.

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, qui fait partie des méthodes 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 décrypter tout message crypté par substitution dans n'importe quelle langue. Ainsi, Al-Kindi est le premier casseur de la méthode de substitution.

Une méthode arithmétique de cryptographie a été inventés et utilisé dans le Maghreb à la fin du 16 ième siècle : cette méthode, a été inventé par le Sultan Al Mansour au Maroc, et consiste à utiliser des transformations aritmétiques sur le texte clair(multiplication, addition et factorisation), et n'avait pas à ma connaissance d'équivalent, ni dans le Moyen-Orient, ni en Europe, avant 1690 où on trouve, après cette date, plusieurs travaux sur la substitution polyalphabétique et en particulier le chiffre de Vigenère décrit par le scientifique franais Claude Comiers en utilisant l'addition d'une clé avec le texte clair, modulo 26 ([17]).

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]).

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 x est un carré modulo p($(\frac{x}{p}) = 1$) 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 $2^{74207281}-1$ (ce nombre premier possède 22 millions de chiffres). Le Figuaro, le 25/01/2016.
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

Quelques notions d'Arithmétique

Dans cette section, on va définir d'autres nombres remarquables, ainsi que d'autres notions importantes liées à ces nombres.

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

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 $561 = 31117$.

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 : $71319 = (6 + 1)(12 + 1)(18 + 1)$.

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 $(\frac{\cdot}{p})$ 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 $(\frac{\cdot}{p})$ 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 : $a^{(p-1)/2} \equiv \pm 1 \bmod p$.

Remarques 12. 1. Le symbole de Legendre $(\frac{\cdot}{p})$ 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) $n = 6 = 23$. On a : $\sigma(6) = 1 + 2 + 3 + 6 = 26$.
b) $n = 28 = 227$. On a : $\sigma(28) = 1+2+4+7+14+28 = 228$.

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 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 14. 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.

4 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 15. 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 16. *(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 17. *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].

5 Résultats d'arithmétique utiles pour la Cryptographie

Soit n un entier naturel supérieur à 2. On désigne par $\mathbf{Z}_n^*$ le groupe des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$. Un entier a est inversible modulo n si et seulement si a est premier avec n ; ce qui est équivalent d'après l'identité de Bezout à l'existence de u et v dans $\mathbf{Z}$ tels que

$$a.u + n.v = 1.$$

Alors, on déduit de ce qui précède que u est l'inverse de a modulo n. Le calcul des entiers u et v se fait, en utilisant les différentes équations de l'algorithme d'Euclide, en un temps polynomial.
Parmi les plus anciens théorèmes d'arithmétique on trouve le théorème des restes chinois :

Théorème 18. *Théorème Chinois : Soient n_1, n_2,..., n_r des entiers naturels premiers entre eux deux à deux, a_1, a_2,..., a_r des entiers relatifs ; alors il existe un entier x unique modulo $N = n_1 n_2 ... n_r$ tel que $x \equiv a_i \bmod n_i$ pour tout $i = 1, ..., r$. Soient $N_i = N/n_i$ et u_i l'inverse de N_i modulo n_i, alors*

$$x = \sum_{1}^{r} a_i u_i N_i.$$

On peut voir ce dernier théorème, comme conséquence du théorème suivant :

Théorème 19. *Soient deux entiers n et m premiers entre*

eux. Alors les anneaux $Z/ZnZ/mZ$ et Z/nmZ sont isomorphes.

D'autre part, en utilisant le fait que l'ordre d'une classe d'équivalence modulo n dans $\mathbf{Z}_n^*$ divise l'ordre du groupe $\mathbf{Z}_n^*$, on obtient les théorèmes suivants :

Théorème 20. *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 21. *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 :*

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

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 22. *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].

Chapitre 4

Tests de Primalité

Il est très important de savoir si un nombre donné est premier ou pas ; et sinon de déterminer 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 sr, 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' 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--dire un algorithme qui détermine si un nombre donné est probablement premier, de faon similaire au test de primalité de *Fermat*.

Comme pour le Test de primalité de *Fermat*, celui de *Miller-Rabin* (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. Écrivons $p-1 = 2^s.t$ 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 $560 = 2^4 35$, $2^{2^3.35} \equiv 1[mod\ 561]$ 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.
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 7. On dit que n passe le test de primalité de *Rabin-Miller* en base b si les deux résultats suivants sont vérifiés :
(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 8. 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 9. Soit n un entier composé impair et b dans l'intervalle $[1, n-1]$. Si n ne passe pas le test de *Rabin-Miller* 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 numériques :

I) Le nombre 9 a 6 témoins.
II) Considérons le nombre $n = 341$ et la base $b = 2$. On a $340 = 2^2 85$.
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 $341 = 1131$) 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 $(\mathbb{Z}/\mathsf{n}\mathbb{Z})$.
(2) Si le résultat (i) n'est pas vérifié, alors le théorème de *Fermat* n'est pas vrai dans $(\mathbb{Z}/\mathsf{n}\mathbb{Z})^*$, donc n n'est pas premier.
(3) Si le résultat (ii) n'est pas vérifié, c'est qu'il existe dans l'anneau $(\mathbb{Z}/\mathsf{n}\mathbb{Z})$ 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* :
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 connat 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

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

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

Théorème 23. *Pour $n \geq 1$, on a : F_n est premier $\Leftrightarrow 3^{(F_n-1)/2} \equiv -1(mod\ F_n)$.*

Théorème 24. *(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.

L'algorithme AKS

En 2002, Manindra Agrawal de l'Indian Institute of Technology à Kanpur et deux de ses étudiants Neeraj Kayal et Nitin Saxena ont trouvé un algorithme simple, possédant toutes les bonnes propriétés, qui teste la primalité de n. Ce dernier algorithme se base sur le petit théeorème de Fermat et repose sur le résultat suivant, qui est une généralisation du petit théorème de Fermat.

Théorème 25. *Soient n un entier naturel strictement supérieur à 2 et a un entier relatif premier avec n. Alors n est premier si, et seulement si,*

$$(X + a)^n \equiv X^n + a \bmod n.$$

Preuve.
On suppose que n est premier, alors $a^n \equiv a \bmod n$. De plus n divise C_n^i pour tout $i \in \{2, ..., n-1\}$, par suite le coéficient de X^i dans $(X+a)^n$, $C_n^i a^{n-i}$, est congru à 0 modulo n ; d'où $(X+a)^n \equiv X^n + a \bmod n$.
Inversement, Soit d un diviseur strict de n. On a : $C_n^d = \frac{n}{d} C_{n-1}^{d-1} \equiv 0 \bmod n$ daprès lidentité des coéficients des deux membres de l'égalité et puisque a est premier avec n. De plus, pour $i = 1$, $C_{n-1}^1 = n - 1 \equiv -1 \bmod n$. Comme on a, $C_{n-1}^i + C_{n-1}^{i+1} = C_n^{i+1}$, donc $C_{n-1}^{i+1} \equiv -C_{n-1}^i \bmod n$. Il sensuit par une rcurrence que $C_{n-1}^i \equiv (-1)^i \bmod n$ pour tout $1 \leq i \leq n-1$, et $\frac{n}{d} C_{n-1}^{d-1} \equiv \frac{n}{d}(-1)^{d-1} \equiv 0 \bmod n$, ce qui nest possible que si $d = 1$. Par suite n est premier.

Ce Théorème est donc un moyen très simple pour tester la primarité : pour l'appliquer sur un entier n, il suffit de choisir un entier a premier avec n et ensuite voir si la congruence est satisfaite. Mais, cela prend un temps en $O(n)$ puisqu'il s'agit d'évaluer n coefficients. Ainsi, il fallait trouver un moyen pour réduire le nombre de coefficients ; une idée est d'évaluer les deux membres de la congruence modulo un polynme de la forme $X^r - 1$ pour un certain entier r plus petit que n. Mais il existe des entiers r pour lesquels cette approche ne permet pas de progresser. Par suite, il faut bien choisir l'entier r.
Ainsi l'algorithme de primalité AKS, qui est déterministe,

polynômial et inconditionnel ; est le suivant.
Soit n un entier supérieur ou égal à 2.
1. Si $n = a^b$ pour a et b deux entiers tels que $b > 1$, alors n est composé.
2. Déterminer le plus petit entier r tel que l'ordre de n dans Z/rZ soit supérieur à $4log(n)^2$.
3. Si $1 < pdcd(a, n) < n$ pour un entier $a \leq r$, alors n est composé.
4. Si $n \leq r$, alors n est premier.
5. Pour $a = 1$ à $\lfloor 2\sqrt{\phi(r)}log(n) \rfloor$: si $(X + a)^n \not\equiv X^n + a$ dans $Z/nZ[X]/(X^r - 1)Z/nZ[X]$, alors n est composé.
6. Autrement n est Premier.

Enfin, l'algorithme AKS répond par "oui" ou "non" à la question : "n, est-il premier ?". Si la réponse est "non", l'algorithme ne donne pas de diviseur non trivial de n. Par suite, le problème de la factorisation, sur laquelle repose le système RSA reste un problème difficile.

Chapitre 5

La méthode RSA

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 crypté ou bien chiffré. Les méthodes de cryptage et de décryptage 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 10. 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.

Les méthodes de cryptographie se partagent en deux types importants : celles à clef publique et celles à clef secrète. Les méthodes de substitution sont à clef secrète, 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 des million de Logiciels aujourd'hui. Cette méthode se base sur la factorisation des nombres en produit de nombres premiers.

5.2.1 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 26. La clef du destinataire doit être publier ou 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. **Chiffrement du Message.**

On coupe M en morceaux plus petits que n_X.

EXEMPLE : $n_X = 3741 = 1517$.

$$M = 0120200117210526 = \underbrace{0120}_{M_1}\underbrace{20}_{M_2}\underbrace{01}_{M_3}\underbrace{1721}_{M_4}\underbrace{0526}_{M_5}.$$

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

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

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

3. **Déchiffrement du Message.**

Le destinataire reçoit le message chiffré $\overline{M}$. 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 déchiffrer 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 déchiffré est bien

$$M = 0120200117210526 = \underbrace{0120}_{M_1}\underbrace{20}_{M_2}\underbrace{01}_{M_3}\underbrace{1721}_{M_4}\underbrace{0526}_{M_5}.$$

Remarques 27. 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. Les nombres premiers p et q doivent être bien choisies : ils doivent être très grands, et leurs différence doit être grande car sinon ils seront proches de $\sqrt{n_X}$ et donc faciles trouver.

5. **Exercice.** Soient A et B deux personnes qui veulent communiquer entre eux à l'aide de la méthode RSA et E un espion. On désigne par (s_x, n_x) la clè publique d'une personne X et t_x sa clé privée :

i. On suppose que E a pu trouver $\phi(n_a)$, vérifiez qu'il peut déterminer la décomposition de n_a.
ii. On suppose que E a pu remarquer qu'un message m a été envoyé à A et à B et que $n_a = n_b$ et e_a et e_b sont premiers entre eux ; vérifiez que E peut trouver le message m.
iii. On suppose cette fois ci qu'une société a envoyé un message m aux trois personnes A, B et C et que l'espion E s'aperoit que $e_a = e_b = e_c = 3$ et que n_a, n_b, et n_c sont premiers entre eux deux à deux. On suppose que $m < n_x$ pour $x = a$, b et c ; montrer comment E peut déterminer le message m.

5.2.2 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 par la méthode 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 déchiffrer 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, 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} modulo n_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 cryptographie pour coder des messages, comme le montre le paragraphe suivant.

Remarque 28. Soit p un nombre premier. Le groupe $G = (\mathbb{Z}/p\mathbb{Z})$ muni de la somme est un groupe où le problème du logarithme discret est facile à résoudre, tandis que le groupe $G = (\mathbb{Z}/p\mathbb{Z})^*$ muni de la multiplication est un groupe où le problème du logarithme discret est difficile à résoudre si le nombre premier p est très grand et est bien choisi.

2 Application du logarithme discret à la cryptographie

6.2.1 Clés d'échange de messages

Diffie et Helman ont construit une méthode d'échange de clés entre deux personnes, (Alice(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. Alice 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 Alice.
4. Alice calcule $Y^x = (a^y)^x = a^{yx}$ et Bachir calcule $X^y = (a^x)^y = a^{xy}$.
Ainsi Alice et Bachir ont le même élément a^{yx}. En plus, Alice garde son x secret et Bachir garde son y secret. L'élément a^{yx} est alors la clé que Alice et Bachir se sont échangés.

6.2.2 Cryptage d'un message : Criyptage 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 Alice 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 difficile à résoudre .

Remarques 29. (1) Tout ce qui précède reste vrai pour un groupe cyclique fini G quelconque. La sécurité de ce système de cryptage est basée sur la difficulté de résoudre le problème de Diffie-Hellman sur le groupe choisi.

(2) Il est clair que casser le protocole d'échange de clés de Diffie-Hellman c'est casser le cryptosystème d'El-Gamal. Inversement, si on sait casser le cryptosystème d'ElGamal, c'est qu'on sait déchiffrer tout message chiffré par la méthode d'ElGamal. En particulier, si le message chiffré est $c = 1$, alors de l'égalité $1 = g^{xy}m$, on déduit que la clé est $g^{xy} = m^{-1}$.

(3) Pour le cryptosystème d'ElGamal dans le cas d'un groupe cyclique quelconque on représente un message m par un élément g_m du groupe et le message chiffré est $c = Kg_m$. Une question qui se pose c'est comment représenter le message m par l'élément g_m.

6.2.3 Signatures

La signature électronique est un moyen permettant de remplir la même fonction que la signature ordinaire. Soient I_m un ensemble de messages, I_s un ensemble de signatures et I_k un ensemble de clés.

Définition 11. Un procédé de signature est la donnée pour chaque clé $K \in I_k$ de deux fonctions calculables en temps polynomial :
$S_K : I_m \longrightarrow I_s$ une fonction de signature (secrète)
$V_K : I_m I_s \longrightarrow \{$ vrai , faux $\}$ est la fonction de vérification(publique) telles que $V_K(M; S) =$ vrai si $S = S_K(M)$ et faux dans le cas contraire.

La signature RSA
Soient $n = pq$, s l'exposant de chiffrement et t celui de déchiffrement qui est la clé privé. Pour signer un message $m \in Z/nZ$ Alice calcule la fonction $S(m) = m^t \bmod n$ et la fonction de vérification associée est $V(m; S) =$ vrai si $m = S^s \bmod n$ et faux dans le cas contraire.

La signature El Gamal
Soient p un grand nombre premier, g un générateur de $(Z/pZ)^*$, a un entier compris entre 0 et $p-2$ et $A = g^a$. Alice publie p ; g et A. Pour un $k \in (Z/(p-1)Z)^*$ on définit la fonction de signature par $sig(m) = (K; S)$ où $K = g^k \bmod p$ et $S = (m - aK)k^{-1} \bmod p - 1$, et la fonction de vérification par $V(m; K; S) = vrai$ si et seulement si $A^K K^S = g^m \bmod p$. Cette fonction de vérification permet bien d'authentifier toute signature : Dans Z/pZ on a $K^S = g^{kS} = g^{m-aK}$ puisque $g^{p-1} = 1$ et $A^K = g^{aK}$ donc $A^K K^S = g^m \bmod p$.

La signature DSS
L'algorithme DSS est une amélioration de la signature de El Gamal : dans un premier temps, il s'est appelé

DSA (Digital Signature Algorithm) ; en suite son nom est devenu DSS (Digital Signature Standard). Avec la DSS on obtient une signature plus courte qu'avec El Gamal pour une sécurité identique. Soient p de taille de 512 ou 1024 bits, q de taille 160 bits et g un élément d'ordre q dans $(Z/pZ)^*$. On travaille dans le sous-groupe engendré par g. On a que $p \equiv 1 \bmod q$(ce qui est assuré par l'existence de l'élément g d'ordre q dans $(Z/pZ)^*$). Soient $a \in N$; $1 \leq a \leq q-1$ et $A = g^a \bmod p$. Les entiers p, q, g et A sont publiques tandis que a est secret.

La fonction de signature est : $sig(m) = (K; S)$ où $K = (g^k \bmod p) \bmod q$ avec k un entier quelconque $1 \leq k \leq q-1$ et $S = (m + aK)k^{-1} \bmod q$.
La fonction de vérification est : $V(m; K; S) =$ vrai si et seulement si $A^{KS^{-1}} g^{mS^{-1}} \bmod p \bmod q = K$ où S^{-1} est l'inverse de S modulo q.

3 Attaques du logarithme discret

On suppose que G est un groupe cyclique d'ordre n engendré par g ; on cherche à calculer le logarithme d'un élément $h \in G$. L'attaque la plus simple est la recherche par force brute ou par énumération : on teste tous les entiers $x \in \{0; 1; ...; n-1\}$ jusqu' ce que l'égalité $g^x = h$ soit satisfaite. La complexité de cette méthode est en O(n) opérations, ce qui n'a d'intérêt que pour les groupes G de très petites tailles. On va décrire ici

des attaques qui se basent surtout sur le théorème des restes chinois ou sur le paradoxe des anniversaires.

4 Réduction de Pohlig-Hellman

Soit $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ la décomposition en facteurs premiers de l'ordre de G. Si le logarithme discret de h modulo chacun des $p_i^{\alpha_i}$ est connu, on peut retrouver son logarithme relativement à la base g, en utilisant le théorème des restes chinois. Pour tout premier p divisant n on pose $n_p = n/p^{\alpha}$, $g_p = g^{n_p}$ et $h_p = h^{n_p}$; alors g_p est d'ordre p^{α} et $g_p^x = h_p$. Par suite $x_p = x$ modulo p^{α} est le logarithme discret de h_p dans la base g_p. Réciproquement si x_p est le logarithme discret de h_p dans la base g_p pour tout p divisant n ; alors, d'après le théorème des restes chinois, il existe x unique modulo n tel que $x \equiv x_p \bmod p^{\alpha}$. Puisque $(g^{-x}h)^{n_p} = g_p^{-x_p} h_p = 1$ pour tout premier p divisant n ; alors l'ordre de $g^{-x}h$ est un diviseur de n_p pour chaque p, ainsi c'est un diviseur de leurs pgcd qui est égal à 1 et ainsi $g^x = h$.
De même on réduit le calcul du logarithme discret dans le cas d'un groupe cyclique d'ordre une puissance d'un nombre premier au calcul du logarithme discret dans le cas d'un groupe cyclique d'ordre un nombre premier de la faon suivante :
Soit $g^x = h$ où g est d'ordre p^{α} ; alors on peut écrire $x = x_0 + x_1 p + ... + x_{\alpha-1} p^{\alpha-1}$ avec $0 \leq x_i < p$ et on a : $(g^x)^{p^{\alpha-1}} = h^{p^{\alpha-1}} = g^{x p^{\alpha-1}} = (g^{p^{\alpha-1}})^{x_0}$. L'élément $g^{p^{\alpha-1}}$ est

d'ordre p, donc le calcul de x_0 c'est le calcul du logarithme discret de $h^{p^{\alpha-1}}$ dans un groupe d'ordre p. On fait la même chose pour déterminer les autres x_j : en supposant que x_0,...,x_{j-1} sont déterminés on a :
$g^{x_j p^j + ... + x_{\alpha-1} p^{\alpha-1}} = h g^{-x_0 + ... + -x_{j-1} p^{j-1}} = h_1$.
En élevant la dernière équation à la puissance $p^{\alpha-j-1}$; on trouve que x_j est le logarithme discret de l'élément $(h_1)^{p^{\alpha-j-1}}$ dans un groupe d'ordre p.

5 Pas-de-bébé pas-de-géant

La méthode "pas-de-bébé pas-de-géant" vise d'accélérer la recherche par énumération en essayant de trouver un certain équilibre entre le temps et la mémoire. Soient G un groupe cyclique d'ordre n et $d < n$ un entier ; si $x \in \{0; ...; n-1\}$ est le logarithme de h dans la base g, alors il s'écrit de faon unique $x = ad + r$ avec $0 \leq r < d$ et $0 \leq a \leq \lfloor n/d \rfloor$. En particulier, a est l'unique entier entre 0 et $\lfloor n/d \rfloor$ tel que

$$h(g^{-d})^a$$

appartienne à l'ensemble $\{g^i : 0 \leq i < d\}$. L'algorithme "pas-de-bébé pas-de-géant" consiste à construire l'ensemble L_d des couples $(i; g^i)$ pour $0 \leq i < d$ dans un premier temps et ensuite calculer

$$h(g^{-d})^k$$

pour $k = 0$ jusqu' ce qu'on obtient un élément de la forme g^s où $0 \leq s < d$, qui correspond à un unique

couple $(s; g^s)$ de L_d. On a alors

$$h(g^{-d})^k = g^s,$$

et on obtient $x = kd + s$.
Cet algorithme demande O($\sqrt{n}$) operations et comparaisons dans G, et aussi une mémoire pour stocker O($\sqrt{n}$) éléments de G.

6 La méthode rho de Pollard

Cette méthode vise à améliorer la complexité en mémoire. C'est Pollard qui avait introduit en 1978 un algorithme probabiliste de calcul du logarithme discret dont la complexité temporelle reste en O($\sqrt{n}$). Son idée est d'itérer une fonction $F : G \longrightarrow G$ vérifiant les propriétés suivantes :
1. F doit être simple à calculer,
2. étant donnés α ; $\beta \in Z/nZ$, on trouve facilement α' ; $\beta' \in Z/nZ$ tels que

$$F(g^\alpha h^\beta) = g^\alpha h^\beta.$$

3. le comportement de F doit être suffisamment proche de celui d'une fonction aléatoire.
Les fonctions simples vérifiant les points 1 : et 2 : sont du type $x \mapsto x^k$ avec k un entier petit, $x \mapsto gx$, $x \mapsto hx$, ou des composées de ces trois primitives. L'approche de Pollard consiste à alterner entre plusieurs fonctions de ce type de la faon suivante : on partitionne G en

trois sous-ensembles $G_1;\ G_2$ et G_3 de tailles comparables, et on définit

$$F(x) = \begin{cases} x^2 & \text{si} \quad x \in G_1\,; \\ gx & \text{si} \quad x \in G_2\,; \\ hx & \text{si} \quad x \in G_3. \end{cases}$$

En partant d'un élément $u_0 = g^{\alpha_0}h^{\beta_0}$, on calcule la suite (u_i) ainsi que les suites (α_i) ; (β_i) de telle sorte que $u_i = F(u_{i-1}) = F^i(u_0) = g^{\alpha_i}h^{\beta_i}$. Comme le groupe est d'ordre fini, la suite (u_i) est périodique : il existe deux entiers i_0 et $l > 0$ tels que $u_{i_0} = u_{i_0+l}$ (et donc $u_i = u_{i+l}$ pour tout $i \geq i_0$).
La collision entre u_{i_0} et $u_{j_0} = u_{i_0+l}(u_{i_0} = u_{i_0+l})$ entrane que $g^{\alpha_{i_0}}h^{\beta_{i_0}} = g^{\alpha_{j_0}}h^{\beta_{j_0}}$; si $\beta_{i_0} - \beta_{j_0}$ est premier avec n, l'ordre de G ; on en déduit que le logarithme discret de h relativement à la base g est $-(\alpha_{i_0} - \alpha_{j_0})(\beta_{i_0} - \beta_{j_0})^{-1} \bmod n$. Si $\beta_{i_0} - \beta_{j_0} \bmod n$ n'est pas inversible, alors il faut recommencer avec un autre élément u_0. On peut montrer que si on itère une fonction aléatoire de G dans G, le temps moyen avant de trouver une collision (i.e. de parcourir un cycle) est en O($\sqrt{n}$) ; en effet, si F est une fonction uniformément aléatoire, les éléments u_0 ; $u_1 = F(u_0)$, ... forment une suite aléatoire uniformément distribuée dans G jusqu' la première collision, et une analyse type paradoxe des anniversaires montre alors que cela arrive au bout de O($\sqrt{n}$) itérations. En pratique F n'est pas aléatoire, mais son comportement est presque similaire pour que cette analyse reste

valide.
L'autre difficulté à traiter est comment détecter les cycles : si on doit stocker toutes les valeurs des u_i jusqu' obtenir une collision, la complexité en mémoire reste encore en O($\sqrt{n}$). Il existe plusieurs méthodes pour détecter les cycles dont le cot mémoire est en O(1), on présente la plus simple et la plus ancienne due à Floyd : On considère en plus de la suite (u_i), la suite (v_i) telle que $v_i = u_{2i}$ et on itère jusqu' trouver une collision $u_i = v_i$. Une telle collision se produit dès que i est un multiple de l (la longueur du cycle) et est supérieur à i_0 (l'entrée du cycle), donc pour une valeur de i nécessairement plus petite que $i_0 + l$.

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 facile à évaluer et telle que l'image inverse de presque tout élément est impossible à calculer. Une fonction à sens unique est dite avec trappe si elle devient facile à inverser suite à la connaissance d'une valeur secrète 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 calculable 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 inconnue, 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 Générateurs

Un générateur pseudo-aléatoire est une suite de nombres, obtenues à partir d'un nombre initial appelé germe, ayant de bonnes propriétés statistiques : des propriétés d'imprévisibilité et de répartition purement aléatoire si le générateur est à usage cryptographique. Ils sont construits, en général, à l'aide de suites récurentes dont le premier terme est le germe.
Un cas tyique est celui où on a une fonction à sens unique F qui produit un bit et une fonction f telles que si t_0 est un germe, on défini une suite cachée $t_k = f(t_{k-1})$ et la suite pseudo-aléatoire $x_k = F(t_k)$.
Comme exemple de générateurs connus, je présente le générateur de Blum-Blum-Shub :

Soit $n = pq$ où p et q sont deux nombres premiers congrus à -1 modulo 4. A partir d'un germe secret t_0 choisi au hazard où $1 \leq t_0 < n$; on calcule les états secrets $t_{k+1} = t_k^2 \bmod n$. En suite, on définit la suite pseudo-aléatoire $x_k = t_k \bmod 2$ qui est le bit de poids faible de t_k.

3 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 distribution 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.

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.

[17] Joachim von zur Gathen, *Claude Comiers : the First Arithmétical Cryptography. Cryptologia, Volume 27, Issue 4 October 2003 , pages 339 - 349.*

[18] Wenbo Mao, *Modern Cryptography : Theory and Pratice. Hewlett-Packard Company, hpbooks, 2003.*

[19] P. Barthélemy, R. Rolland et P. Véron, *Cryptographie : principes et mises en oeuvre. Hermes Sciences Lavoisier 2005.*

[20] Bruce Schneier, *Cryptographie Appliquée : Algorithmes, protocoles et codes source en C. Seconde édition, Vuibert Informatique, 2001.*