Arithmétique modulaire et cryptologie

Pierre MEUNIER

Professeur de mathématiques
en Mathématiques Spéciales MP*
au lycée JOFFRE de Montpellier.

CÉPADUÈS-ÉDITIONS
111, rue Nicolas Vauquelin
31100 Toulouse – France
Tél. : 05 61 40 57 36 – Fax : 05 61 41 79 89
www.cepadues.com
Courriel : cepadues@cepadues.com
Coordonnées GPS en WGS 84
N 43° 34'43,2''
E 001° 24'21,5''

Chez le même éditeur

Robustesse et commande optimale ..... *Alazard D. et al.*
Eléments d'analyse numérique ..... *Attéia M., Pradel M.*
Analyse variationnelle et optimisation ..... *Azé D., Hiriart-Urruty J.-B.*
Simulation et algorithmes stochastiques ..... *Bartoli N., Del Moral P.*
Mesure et intégration. Intégrale de Lebesgue ..... *Bouyssel M.*
Cours d'Analyse fonctionnelle et complexe ..... *Caumel Y.*
Topologie des espaces vectoriels normés ..... *Colin J-J., Morvan J-M. et R.*
Modélisation probabiliste et statistique ..... *Garel B.*
Mathématiques et résolution des équations aux dérivées partielles classiques ..... *Giraud G., Dufour J.P.*
Les fonctions spéciales vues par les problèmes ..... *Groux R., Soulat Ph.*
Principes généraux et méthodes fondamentales ..... *Groux R.*
Polynômes orthogonaux et transformations intégrales ..... *Groux R.*
Les structures et les morphismes vus par les problèmes ..... *Groux R., Soulat Ph.*
Analyse : la convergence vue par les problèmes ..... *Groux R., Soulat Ph.*
Algèbre linéaire ..... *Grifone J.*
Exercices d'algèbre linéaire et bilinéaire ..... *Hiriart-Urruty J.-B., Plusquellec Y.*
Analyse fonctionnelle et théorie spectrale ..... *Intissar A.*
Invitation à l'Algèbre ..... *Jeanneret A., Lines D.*
Probabilités et statistique appliquées ..... *Lacaze B., Mailhes C., Maubourguet M.M., Tourneret J.-Y.*
Résolution numérique des équations aux dérivées partielles ..... *Le Pourhiet A.*
Probabilités et statistiques pour ingénieurs et commerciaux ..... *Pellaumail J., Perret A., Basle L.*
Que savez-vous de l'outil mathématique ?
collection de six fascicules ..... *Plusquellec Y., Agullo M., Boudet R., Fabre J., Guérin R.*
La démarche statistique ..... *Prum B.*
Analyse fonctionnelle ..... *Samuelides M., Touzillier L.*
Problèmes d'analyses fonctionnelle et harmonique ..... *Samuelides M., Touzillier L.*
Analyse harmonique ..... *Samuelides M., Touzillier L.*
Introduction à la Topologie ..... *Sondaz D., Morvan R.*
Limites, applications continues ..... *Sondaz D., Morvan R.*
Calcul différentiel ..... *Todjibounde L.*

ISBN : 978.2.85428.954.1

Dépôt légal : décembre 2010 N° éditeur : 954

Les autres sciences cherchent à trouver les lois que Dieu a choisies ; les mathématiques cherchent à trouver les lois auxquelles Dieu a dû obéir.

Jean-Pierre Serre

Table des matières

Introduction

L'arithmétique modulaire est, avant tout, la discipline mathématique dont l'objet est l'étude des anneaux ou des corps - le plus souvent finis - obtenus par "réduction" à partir d'un idéal I d'un anneau commutatif A ; l'idéal I définit alors ce qu'on appelle le *modulo* (ou parfois le *modulus*) à l'aune duquel sont "regardés" les éléments de l'anneau A ; l'ensemble ainsi "réduit", toujours noté A/I, porte le nom *d'ensemble quotient* (algébrique) de l'anneau A par son idéal I.

En pratique, ou bien $A = \mathbb{Z}$ et I est du type $n\mathbb{Z}$, ou bien $A = \mathbb{K}[X]$, $\mathbb{K}$ étant un corps (le plus souvent fini) et éventuellement, mais plus rarement, $A = A'[X]$ où A' est un anneau fini, l'idéal I étant toujours du type (P), c'est-à-dire l'idéal de A engendré par le polynôme P.

A partir d'un ensemble produit de l'arithmétique modulaire usuelle, anneau $\mathbb{Z}/(n)$ ou corps fini, on peut créer des sous-ensembles algébriquement très faciles à identifier, organisés en groupes cycliques, qui, à ce titre, relèvent également du concept modulaire (courbes elliptiques, surfaces de Frobénius, groupe des inversibles de $\mathbb{Z}/(n)$ lorsque $n = p^\alpha$, p premier...).

L'intérêt de l'arithmétique modulaire, telle qu'elle vient d'être exposée dans cette introduction, réside essentiellement dans le fait qu'elle dispose et crée des ensembles finis, algébriquement très riches, pourvus de modes opératoires n'ayant aucun ordre prévisible et, de ce fait, susceptibles de favoriser la création de mécanismes mathématiques de secret si nécessaires en cryptologie.

C'est la raison pour laquelle sont réunies dans le même ouvrage l'arithmétique modulaire et la cryptologie, étant entendu que cette discipline mathématique est abordée de façon élémentaire afin qu'un *taupin* ou candidat aux concours (CAPES, Agrégation) puisse "y trouver son compte".

Chapitre 1

Notions préliminaires

Introduction : Il s'agit dans ce premier chapitre, d'établir quelques résultats dont on se servira constamment dans cet ouvrage ; ils concernent, bien évidemment, des méthodes "universelles", c'est-à-dire valables dans de nombreuses situations ; il y sera fait référence aussi souvent que nécessaire.

1.1 Relation d'équivalence - Décomposition canonique d'une application

1.1.1 Relation d'équivalence - Ensemble quotient

Définitions : Si E est un ensemble quelconque non vide, on appelle *relation binaire* sur E la donnée d'un sous-ensemble (Γ) de $E \times E$, et on dira, pour x, y dans E que x est en relation avec y, ce qu'on écrira $x\mathcal{R}y$, *si et seulement si* le couple (x, y) appartient à (Γ).

La relation binaire $\mathcal{R}$ est dite *relation d'équivalence* sur E si elle possède les trois propriétés suivantes :

R_1 : Elle est réflexive, ce qui signifie que l'on a $x\mathcal{R}x$ pour tout x de E.

R_2 : Elle est symétrique, ce qui veut dire que si $x\mathcal{R}y$ alors on a également $y\mathcal{R}x$.

R_3 : Elle est transitive, ce qui signifie que :

$$x\mathcal{R}y \text{ et } y\mathcal{R}z \text{ implique } x\mathcal{R}z$$

Notation : Très souvent, lorsqu'on dispose dans E d'une relation d'équivalence, celle-ci est usuellement notée $\sim$; ainsi on écrit $x \sim y$ pour dire que x est en relation d'équivalence avec y dans E. Si $\sim$ est une relation d'équivalence, et si x appartient à E on note $\bar{x} = \{y \in E : x \sim y\}$ et on dit que $\bar{x}$ est la *classe* de x dans E modulo $\sim$.

Bien évidemment les diverses classes selon $\sim$ constituent une partition de E si bien qu'on constate que se donner une relation d'équivalence dans un ensemble E c'est constituer une partition de E.

L'ensemble des $\bar{x}$ lorsque x décrit E est un sous-ensemble de l'ensemble des parties de E, on le note usuellement $E/\sim$ et on l'appelle *l'ensemble quotient* de E modulo la relation d'équivalence $\sim$.

1.1.2 Décomposition canonique d'une application

C'est un résultat très utile et à caractère universel, en ce sens qu'il est fréquemment rencontré et utilisé en algèbre ; il peut s'énoncer de la façon suivante :

Proposition 1 : Soit f une application d'un ensemble E dans un ensemble F ; dans E la relation binaire :

$$x \sim x' \text{ si et seulement si } f(x) = f(x')$$

est une relation d'équivalence et on peut alors écrire :

$$f = i \circ b \circ s$$

avec i injective de $f(E)$ dans F, b bijective de $E/\sim$ dans $f(E)$ et s surjective de E dans $E/\sim$; en outre :

$$s(x) = \bar{x}, b(\bar{x}) = f(x) \text{ et } i(y) = y$$

$\bar{x}$ désignant la classe résiduelle de x modulo la relation $\sim$.

Démonstration : Il est bien clair que l'application :

$$x \longrightarrow s(x) = \bar{x}$$

est une surjection de E sur $E/\sim$.

Il convient d'abord de s'assurer que b est bien une application de l'ensemble quotient $E/\sim$ sur $f(E)$ ce qui revient à montrer que si $\bar{x} = \bar{x}'$ alors $f(x) = f(x')$, ce qui est bien sûr évident par définition de la relation $\sim$; b est, à l'évidence, une surjection ; enfin si $b(\bar{x}) = b(\bar{x}')$ on doit avoir $f(x) = f(x')$ *ie* $x \sim x'$, ou encore $\bar{x} = \bar{x}'$; la proposition est entièrement démontrée. On retiendra surtout que l'image $f(E)$ est en bijection avec l'ensemble quotient $E/\sim$.

1.2 Lois de composition internes - Monoïdes - Algorithme d'exponentiation rapide dans un monoïde

1.2.1 Des définitions

Etant donné un ensemble E, on appelle *loi de composition interne* la donnée d'une application f de $E \times E$ dans E. On dit que cette loi est *associative si et seulement si* :

$$\left(\begin{array}{l} \forall x \\ \forall y \in E \quad f(x, f(y,z)) = f(f(x,y),z) \\ \forall z \end{array} \right)$$

Si on convient, ce qui est toujours le cas en pratique, de noter $f(x,y) = x \cdot y$, ou $x * y$, ou plus commodément xy, dire que la loi est associative revient à dire que l'on a :

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

pour tous x, y, z de E ; la valeur commune se note encore xyz.

Définition : On appelle *monoïde* tout couple $(E, \bullet)$ où $\bullet$ est une loi de composition interne sur E, associative, et admettant un élément neutre e pour la loi $\cdot$, c'est-à-dire tel que :

$$e \cdot x = x \cdot e = x$$

pour tout x de E.

1.2.2 Extension de la loi de composition interne dans un monoïde

Définition : Soit $(E, \bullet)$ un monoïde et n un entier naturel ; si $n = 1$ on appelle *extension de la loi* $\bullet$ à E, l'application identité de E. Si $n = 2$, on appelle extension de la loi $\bullet$ à E^2, l'application :

$$(x, y) \in E \times E \longrightarrow x \bullet y \in E$$

ie la loi $\bullet$ elle-même.

Si $n \geq 3$ on appelle extension de la loi $\bullet$ à E^n toute application de E^n dans E du type :

$$(x_1, x_2, \ldots, x_n) \longrightarrow \varphi(x_1, \ldots, x_p) \cdot \psi(x_{p+1}, \ldots, x_n)$$

où φ est une extension de la loi $\bullet$ à E^p et ψ une extension de la loi $\bullet$ à E^{n-p} $(1 \leq p \leq n-1)$.

Proposition 2 : Dire que la loi $\bullet$ est associative revient à dire que toutes les extensions de cette à loi à E^n, pour n quelconque, coïncident.

Démonstration : Si toutes les extensions coïncident, c'est en particulier vrai si $n = 3$ et bien évidemment la loi $\bullet$ est associative ; c'est la réciproque qui est importante et la preuve s'effectue par récurrence sur l'entier n et elle résulte évidemment de l'associativité, comme la suite le montre.

En effet, désignons (hypothèse de récurrence) par $\varphi_1, \varphi_2, \cdots, \varphi_{n-1}$ les uniques extensions de la loi $\bullet$ à $E, E^2, \ldots, E^{n-1}$; soient alors g et g' deux extensions de $\bullet$ à E^n. Il existe donc deux entiers p et q de $\{1, 2, \ldots, (n-1)\}$ tels que :

$$g(x_1, x_2, \ldots, x_n) = \varphi_p(x_1, \ldots, x_p) \cdot \varphi_{n-p}(x_{p+1}, \ldots, x_n)$$

et

$$g'(x_1, x_2, \ldots, x_n) = \varphi_q(x_1, x_2, \ldots, x_q) \cdot \varphi_{n-q}(x_{q+1}, x_{q+2}, \ldots, x_n)$$

et ce pour tout $(x_1, x_2, \ldots, x_n) \in E^n$.

Supposons par exemple $p > q$; on peut donc écrire, *via* l'hypothèse de récurrence :

$$\varphi_p(x_1, x_2, \ldots, x_p) = \varphi_q(x_1, x_2, \ldots, x_q) \cdot \varphi_{p-q}(x_{q+1}, x_{q+2}, \ldots, x_p)$$

et ainsi :

$$\begin{aligned} g(x_1, x_2, \ldots, x_n) =& (\varphi_q(x_1, x_2, \ldots, x_q) \cdot \varphi_{p-q}(x_{q+1}, x_{q+2}, \ldots, x_p)) \cdot \\ & \varphi_{n-p}(x_{p+1}, x_{p+2}, \ldots, x_n) \end{aligned}$$

et en utilisant l'associativité de la loi $\bullet$ il vient :

$$\begin{aligned} g(x_1, x_2, \ldots, x_n) =& \varphi_q(x_1, x_2, \ldots, x_q) \cdot (\varphi_{p-q}(x_{q+1}, x_{q+2}, \ldots, x_n) \cdot \\ & \varphi_{n-p}(x_{p+1}, x_{p+2}, \ldots, x_n)) \end{aligned}$$

et *via* l'hypothèse de récurrence on a :

$$\varphi_{p-q}(x_{q+1}, x_{q+2}, \ldots, x_n) \cdot \varphi_{n-p}(x_{p+1}, x_{p+2}, \ldots, x_n) = \varphi_{n-q}(x_{q+1}, x_{q+2}, \ldots, x_n)$$

puisqu'il n'existe qu'une extension de la loi $\bullet$ à E^{n-q}.

En définitive : $g = g'$ ce qui achève la preuve.

Notation : Pour tout n on écrira :

$$\varphi_n(x_1, x_2, \ldots, x_n) = x_1 \cdot x_2 \cdots x_n$$

et si $x_1 = x_2 = \cdots = x_n$, $\varphi_n(x, x, \ldots, x)$ est noté x^n ; on a d'ailleurs prouvé que si $n = p + q$ avec $p, q \geq 1$ on a :

$$x^{p+q} = x^p x^q = x^q x^p = x^n$$

Si on convient, puisqu'on se trouve dans un monoïde, que $x^0 = e$, on a donc pour $p \geq 0$ et $q \geq 0$ et pour tout $x \in E$:

$$x^{p+q} = x^p x^q = x^q x^p$$

Remarque : Si E est un ensemble muni d'une loi de composition interne *non associative*, la suite $(u_n)_{n\geq 1}$ définie par : $u_1 = 1$, $u_n = \sum_{k=1}^{n-1} u_k u_{n-k}$ permet de dénombrer les diverses extensions de la loi à E^n, $n \geq 1$. En utilisant judicieusement la SE : $\sum_{n\geq 1} u_n x^n$ on montre ainsi qu'il y a $\frac{(2n-2)!}{n!(n-1)!}$ extensions de la loi à E^n.

1.2.3 Exemple de monoïde utilisé en cryptologie dans cet ouvrage

Soit $\mathbb{K}$ un corps quelconque et n un entier, $n \geq 2$; on désigne par F la matrice de Frobénius de taille n sur $\mathbb{K}$; F est définie par l'égalité :

$$F = \begin{pmatrix} 0 & 1 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

Si $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{K}^n$ on désigne par $A(x)$ l'élément de $M_n(\mathbb{K})$ défini par :

$$A(x) = \sum_{i=0}^{n-1} x_i F^i = \begin{pmatrix} x_0 & x_1 & \cdots & \cdots & x_{n-1} \\ x_{n-1} & x_0 & x_1 & \cdots & x_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & x_1 \\ x_1 & \cdots & \cdots & x_{n-1} & x_0 \end{pmatrix}$$

($A(x)$ est une matrice circulante par ses lignes).

Dans ces conditions si $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{K}^n$,
$y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{K}^n$ on constate aisément qu'il existe $z \in \mathbb{K}^n$ unique tel que :

$$A(z) = A(x)A(y)$$

On note alors $x * y$ le vecteur z et on peut énoncer :

Proposition 3 : Le couple $(\mathbb{K}^n, *)$ est un monoïde commutatif

Tout se vérifie aisément et $e = (1, 0, \ldots, 0)$ est l'élément neutre, d'ailleurs :

$$z_i = \sum_{\substack{k+l=i \pmod n \\ 0 \leq k,l \leq n-1}} x_k y_l$$

$*$ est la loi de convolution dans $\mathbb{K}^n$ et le lecteur constatera (puisque $F^n = I_n$) que la loi $*$ de $\mathbb{K}^n$ correspond au produit modulo $(X^n - 1)$ dans le $\mathbb{K}$-ev des polynômes de degré au plus égal à $n - 1$.

1.2.4 Calcul dans un monoïde de x^n par l'algorithme d'exponentiation rapide

$(E, \bullet)$ est un monoïde et x appartient à E ; pour calculer x^n dans E on utilisera le protocole suivant :

(i) Ecrire : $n = \sum_{i=0}^{r-1} c_i 2^i$ avec $c_i \in \{0, 1\}$ et $c_{r-1} = 1$

(ii) Poser $x_0 = x$ et puis pour $i = 1$ jusqu'à $r - 1$ faire :

$$x_i = x_{i-1}^2$$

(iii) Poser $z = e$, et pour i allant de 0 jusqu'à $r - 1$ faire :

$$\text{si } c_i = 1, z \longleftarrow z \cdot x_i$$

Fin

On peut aussi résumer ce protocole dans le schéma suivant :

Algorithme d'exponentiation rapide dans le monoïde $(E, \bullet)$

(1) Ecrire $n = \sum_{i=0}^{r-1} c_i 2^i$ (décomposition binaire de n)

(2) $z := e$, (ou $z \longleftarrow e$) puis ;
pour $k = r-1$ jusqu'à 0 faire :

$$z := z^2, \text{si } c_k = 1 \text{ alors } z := z \cdot x$$

Fin

Remarque : On rappelle que si b est un entier, $b \geq 2$, le nombre de chiffres d'un entier n représenté en base b est l'entier :

$$1 + \left[\frac{\log n}{\log b}\right]$$

ce qui explique, même lorsque l'entier n est très grand, la rapidité d'exécution de l'algorithme d'exponentiation rapide.

Cet algorithme est d'un emploi constant en cryptologie ; le lecteur pourra le constater au cours de l'élaboration des divers protocoles cryptographiques mis en œuvre dans cet ouvrage (voir notamment le chapitre **7**).

1.3 Le coût des algorithmes

Il "estime" en quelque sorte le temps mis par l'algorithme pour parvenir au résultat souhaité ; ce temps est fonction du nombre d'opérations élémentaires effectuées par l'ordinateur chargé de l'exécution des tâches.

Pratiquement tout algorithme est indexé (ou relié) à un entier n et le nombre d'opérations élémentaires à effectuer dépend bien évidemment de cet entier.

Le coût d'un algorithme attaché à un entier n est dit *polynomial* s'il existe une constante $c > 0$ et un entier p tels que le nombre d'opérations élémentaires à effectuer n'excède pas $c(\log n)^p$; s'il n'est pas de complexité polynomiale mais si le nombre précédent est borné par une expression du type An^q, on dit alors que l'algorithme est à coût *exponentiel*.

Bien évidemment, les algorithmes intéressants sont ceux qui ont un coût polynomial puisqu'ils permettent de "traiter" avec rapidité des entiers ayant plusieurs centaines de chiffres dans leur écriture décimale ($1 + \left[\frac{\log n}{\log 10}\right]$ est le nombre de chiffres de l'écriture décimale de l'entier n...).

Exemples : On peut montrer, et nous l'admettrons, les résultats suivants :

1. Si n est un entier donné, et si b est un entier quelconque, la réduction modulo n de l'entier b a un coût majoré par :

$$c \log |b| \log |b/n|$$

2. Si a, b sont compris entre 0 et n, le calcul $a+b$ (*resp.* $a-b$) modulo n a un coût n'excédant pas $c \log n$.
3. Si a et b sont compris entre 0 et n le calcul de $a \cdot b \pmod{n}$ a un coût majoré par $c(\log n)^2$.
4. Si $a \in \{0, 1, 2, \ldots, n\}$ le calcul de $a^p \pmod{n}$ a un coût majoré par $c \log p(\log n)^2$.
5. Si a et b sont deux entiers compris entre 0 et n la détermination du pgcd de a et b par l'algorithme d'Euclide a un coût polynomial n'excédant pas $c(\log n)^2$.

Dans tout cet ouvrage le lecteur attentif trouvera des indications sur la complexité des protocoles itératifs utilisés.

1.4 Notion d'algorithme probabiliste

Soit Ω une partie de $\mathbb{N}^*$ et $n \longrightarrow T(n)$ un algorithme à coût polynomial sur $\mathbb{N}^*$ dont le but est de répondre à la question : "l'entier n appartient-il à Ω ?".

On suppose que, pour tout $n \in \Omega$, $T(n)$ fournit invariablement la même réponse : "l'entier n appartient à Ω".

Soit maintenant un entier n de $\mathbb{N}^*$ choisi "au hasard" ; à l'issue de ce choix, considérons les trois événements :

A : L'entier n n'appartient pas à Ω

B : $T(n)$ répond "$n \in \Omega$"

C : $T(n)$ répond "$n \notin \Omega$"

Si l'éventualité C se présente, on est certain que $n \notin \Omega$. Mais, que se passe-t-il si l'éventualité B se produit ? Il y a erreur si, sachant B, on a A ; pour estimer la fiabilité du test T il faut donc connaître : $pr(A|B)$, la probabilité d'avoir A sachant B. Or :

$$pr(A|B) = \frac{pr(B|A)pr(A)}{pr(B)}$$

et :

$$pr(B) = pr(B|A)pr(A) + pr(B|non\ A)pr(non\ A)$$

Comme, par hypothèse, $pr(B|non\ A) = 1$, il vient :

$$pr(A|B) = \frac{pr(A)pr(B|A)}{pr(B|A)pr(A) + pr(non\ A)}$$

Or $pr(A) = \alpha$ et $pr(non\ A) = 1 - \alpha$ sont des "constantes" dépendant de l'entier n, donc connues ou estimées, *a priori* ; ainsi le protocole algorithmique est d'autant plus fiable que le nombre : $pr(B|A)$ est le plus petit possible. On dispose alors d'un algorithme probabiliste dont on peut estimer la fiabilité.

Le lecteur est prié, afin d'avoir deux exemples célèbres, de se reporter au chapitre **3** (test de Miller-Rabin), puis au chapitre **5** (algorithme de Solovay-Strassen).

Chapitre 2

Les groupes, les anneaux et les corps

Dans ce deuxième chapitre sont établis des résultats algébriques essentiels, utiles en arithmétique modulaire et en cryptologie ; ils concernent les trois types de structure algébrique fondamentaux : groupes, anneaux et corps, que l'on rencontre usuellement en cryptologie.

2.1 Les groupes

2.1.1 Définitions

On appelle *groupe* tout couple $(G, \bullet)$ où G est un ensemble non vide et où $\bullet$ est une loi de composition interne définie sur E telle que :

G_1 : $\bullet$ est associative

G_2 : Il existe un élément neutre e dans G, ce qui revient à dire : $e \cdot x = x \cdot e$ pour tout x de G.

G_3 : Quel que soit x appartenant à G, il existe x' unique dans G avec :
$x \cdot x' = x' \cdot x = e$, x' s'appelle alors *l'inverse* de x dans $(G, \bullet)$ et se note usuellement x^{-1} si la loi $\bullet$ est notée multiplicative (ce qui sera presque toujours le cas dans cet ouvrage) ou $-x$ si elle est notée additivement.

En quelque sorte un groupe est un monoïde tel que tout élément est inversible ; on peut démontrer, ce qui est facile et laissé aux soins du lecteur, qu'un groupe est un monoïde tel que tout élément possède un inverse à gauche.

Un groupe $(G, \bullet)$ est dit *commutatif* (ou *abélien*) si sa loi est commutative *ie si et seulement si* :

$$x \cdot y = y \cdot x \text{ pour } x, y \text{ quelconques dans } G$$

2.1.2 Sous-groupes et groupe engendré par une partie

a. Définition

Etant donné un groupe $(G, \bullet)$, une partie H non vide de G, est appelée *sous-groupe* si H est stable pour la loi $\bullet$ et si, de plus, le couple $(H, \bullet)$ est lui-même un groupe.

Alors, on peut démontrer aisément le résultat suivant :

Proposition 1 : Soit $(G, \bullet)$ un groupe et H une partie non-vide de G ; les énoncés suivants sont équivalents :
(i) H est un sous-groupe de G
(ii) $\forall x \in H, \forall y \in H, x^{-1} \cdot y \in H$

b. Groupe engendré

Si $(G, \bullet)$ est un groupe et si A est une partie non-vide de G, on appelle *sous-groupe engendré par* A le plus petit (au sens de l'inclusion) des sous-groupes de G contenant A ; c'est donc, à l'évidence, l'intersection de tous les sous-groupes de G qui contiennent A ; on le note usuellement $[A]$ et on vérifie que : $[A] = \{a_1 a_2 \cdots a_i, i \in \mathbb{N}, a_i \in A \cup A^{-1}\}$ où $A^{-1} = \{a^{-1}, a \in A\}$.

En particulier si $A = \{a\}$, le sous-groupe de $(G, \bullet)$ engendré par A est $[a] = \{a^n, n \in \mathbb{Z}\}$; on dit alors que l'on a affaire à un groupe *monogène*.

2.1.3 Relations d'équivalence dans un groupe associées à un sous-groupe - Applications

a. Définitions

Soit G un groupe et H un sous-groupe de G ; on peut définir "bien naturellement" dans G, deux relations binaires R_1 et R_2 en écrivant pour x, y de G :

$$xR_1y \Longleftrightarrow x^{-1}y \in H$$
$$xR_2y \Longleftrightarrow xy^{-1} \in H$$

Il est immédiat de constater que les deux relations binaires R_1 et R_2 sont des relations d'équivalence dans G.

Si x appartient à G, la classe de x vis-à-vis de la relation R_1 est l'ensemble xH, et sa classe vis-à-vis de la relation R_2 est l'ensemble Hx ; on l'appelle *classe résiduelle* de x modulo H à gauche (*resp.* à droite).

Puisque l'application : $a \in G \longrightarrow x \cdot a \in G$ est une bijection, chaque classe à gauche (ou à droite) possède, lorsque H est fini, le même nombre d'éléments que H ; d'où la proposition suivante :

Proposition 2 : (Lagrange)
Si $(G, \bullet)$ est un groupe ayant un nombre fini n d'éléments et si $(H, \bullet)$ est un sous-groupe de G, le cardinal de H divise toujours celui de G.

b. Sous-groupe distingué - Groupe quotient

Par définition, un sous-groupe H d'un groupe G est dit *distingué si et seulement si* , pour tout x de G, $xH = Hx$, ce qui revient à dire que les deux relations d'équivalence définies à l'aide de H coïncident.

Proposition 2-bis : Soit $(G, \bullet)$ un groupe et $(H, \bullet)$ un sous-groupe distingué de G ; si on note G/H l'ensemble quotient des classes résiduelles dans G modulo H vis-à-vis de la relation d'équivalence :

$$x \sim y \Longleftrightarrow x^{-1}y \in H$$

l'application :

$$(\bar{x}, \bar{y}) \in G/H \times G/H \longrightarrow \bar{x} \cdot \bar{y} = \overline{x \cdot y} \in G/H$$

confère à G/H une structure de groupe.

Démonstration : Tout d'abord, par souci de cohérence, il faut s'assurer que si $\bar{x} = \bar{x}'$ *ie* que si $x^{-1}x' \in H$, et $\bar{y} = \bar{y}'$ *ie* $y^{-1}y' \in H$, on a bien :

$$\overline{xy} = \overline{x'y'}$$

ou, ce qui revient au même, que $y^{-1}x^{-1}x'y'$ appartient à H.

En effet, on écrit :

$$y^{-1}x^{-1}x'y' = (y^{-1}(x^{-1}x')y)(y^{-1}y')$$

Comme $x^{-1}x'$ appartient à H et que H est distingué dans G l'élément $y^{-1}(x^{-1}x)y$ appartient à H ; comme il en est de même pour $y^{-1}y'$ (puisque $y \sim y'$) et que H est stable pour la loi $\bullet$ (en tant que sous-groupe de G) la définition du symbole $\bar{x} \cdot \bar{y}$ sur $G/H \times G/H$ est cohérente.

Ceci étant acquis il est très facile de constater alors que le couple $(G/H, \bullet)$ est un groupe.

Remarque : La réduction modulaire dans G selon H permet de fabriquer un ensemble mathématique (G/H) "plus petit", donc *a priori* plus commode à manipuler, sans perdre pour autant la "richesse" algébrique de l'ensemble de départ ; tout l'intérêt du raisonnement modulaire réside dans cette constatation, comme la suite de cet ouvrage va le montrer.

c. Morphisme de groupe ; théorème d'isomorphisme

Par définition, si $(G, \bullet)$ et $(G', \bullet)$ sont deux groupes, on appelle *morphisme* de $(G, \bullet)$ dans $(G', \bullet)$ toute application f de G dans G' telle que :

$$f(x \cdot y) = f(x) \cdot f(y) \text{ pour tout } x, y \text{ de } G$$

Si e (*resp.* e') est l'élément neutre de G, on a, nécessairement : $f(e) = e'$ et on peut énoncer :

Proposition 3 : Soit f un morphisme du groupe $(G, \bullet)$ dans le groupe $(G', \bullet)$; alors :

(i) $f(G)$ est un sous-groupe de $(G', \bullet)$

(ii) $\ker f = \{x \in G : f(x) = e' = f(e)\}$ est un sous-groupe distingué de $(G, \bullet)$, réduit à $\{e\}$ *si et seulement si* f est une application injective.

(iii) Le théorème de décomposition canonique (proposition 1, chapitre 1) établi précédemment montre en outre que :

$$\bar{x} \in G/\ker f \xrightarrow{b} b(\bar{x}) = f(x) \in f(G)$$

est un morphisme de groupe bijectif (isomorphisme) et l'isomorphie de $G/\ker f$ et de $f(G)$ se note usuellement :

$$f(G) \cong G/\ker f$$

Tout est facile à vérifier et, de ce fait, laissé encore une fois aux soins du lecteur.

2.1.4 Groupes monogènes et groupes cycliques

a. Définition

Etant donné un groupe $(G, \bullet)$, il est dit *monogène* s'il existe a dans G tel que : $G = [a] = \{a^n, n \in \mathbb{Z}\}$. Alors on peut montrer :

Proposition 4 : Si $G = \{a^n, n \in \mathbb{Z}\}$ est un groupe monogène, l'application :
$m \in (\mathbb{Z}, +) \xrightarrow{f} a^m \in (G, \bullet)$ est un morphisme du groupe additif $(\mathbb{Z}, +)$ dans $(G, \bullet)$.
Son noyau $\ker f$ est un sous-groupe additif de $(\mathbb{Z}, +)$; ainsi il existe $n \in \mathbb{N}$ tel que $\ker f = n\mathbb{Z}$.
Si $n = 0$ f est une isomorphie.
Sinon $n \geq 1$ et alors G est isomorphe au groupe additif $(\mathbb{Z}/n\mathbb{Z})$ des classes résiduelles dans $\mathbb{Z}$ modulo n : on dit alors que G est un *groupe cyclique* et on peut écrire :

$$G = \{e, a, a^2, \ldots, a^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$$

Tout est évident dans l'énoncé de cette proposition et résulte de ce qui a été mis en place auparavant.

b. Quelques résultats généraux concernant les groupes cycliques - Applications

b.1. Sous-groupes d'un groupe cyclique

Leur détermination résulte de l'énoncé suivant :

Proposition 5 : Soit $(G, \bullet)$ un groupe cyclique possédant n éléments, alors :

(i) Tout sous-groupe de G est, tout comme G, cyclique.

(ii) Si d est un entier diviseur de n, il existe un et un seul sous-groupe de $(G, \bullet)$ ayant d éléments.

Démonstration : C'est un résultat particulièrement utile dans la théorie des groupes cycliques ; commençons donc par (i).

Soit $(H, \bullet)$ un sous-groupe de G, $H \neq \{e\}$ (sinon tout est trivial), soit a un générateur de G et r l'entier défini par : $r = \min i, i \geq 1, a^i \in H$; alors H coïncide avec le sous-groupe de G engendré par $a' = a^r$; en effet soit $x = a^m$ appartenant à H, avec m entier, $m \in \{1, 2, \ldots, n-1\}$; par division euclidienne dans $\mathbb{N}$, on peut écrire :

$$m = kr + r'$$

où $0 \leq r' \leq r - 1$; ainsi on a : $x = (a^r)^k \cdot a^{r'}$ et comme a^r appartient à H, il en est de même de a^{rk} puis de xa^{-rk}, d'où $a^{r'} \in H$ et compte tenu de la définition de l'entier r cela impose $r' = 0$ et : $x = a'^k$; ainsi $H = [a']$ ce qui démontre l'assertion (i).

Ensuite, s'agissant de (ii), puisque d divise l'entier n, on peut écrire dans $\mathbb{N}$: $n = dd'$; désignons alors par b l'élément de G défini par : $b = a^{d'}$. Le sous-groupe de $(G, \bullet)$ engendré par b est constitué par : $e, b, \ldots, b^{d-1}$; en effet, si k est un entier tel que $b^k = e$, cela impose $a^{kd'} = e$, et ainsi : kd' est un multiple de l'entier n ; cela revient à dire que le morphisme : $k \in (\mathbb{Z}, +) \longrightarrow b^k \in [b]$ admet $d\mathbb{Z}$ pour noyau ; de ce fait le sous-groupe engendré par b possède d éléments et c'est le seul à jouir de cette propriété.

Supposons, en effet, disposer d'un sous-groupe H de G ayant d éléments ; H est, nous l'avons vu en (i), cyclique ; désignons par b' un générateur de H ; il existe m entier, $m \in \{1, 2, \ldots, (n-1)\}$ vérifiant :

$$b' = a^m$$

et puisque $b'^d = e$, dm est un multiple de l'entier n, ce qui assure l'existence d'un entier k tel que : $m = kd'$.

Dans ces conditions, il vient :

$$b' = a^{d'k} = b^k$$

cela prouve que le sous-groupe engendré par b' est contenu dans le sous-groupe engendré par b ; comme ils ont le même nombre d'éléments, ils coïncident ; ainsi la proposition est entièrement démontrée.

b.2. Les générateurs d'un groupe cyclique

Leur détermination est entièrement résolue par l'énoncé suivant :

Proposition 6 : Soit $G = [a]$ un groupe cyclique ayant n éléments ; les deux énoncés suivants sont équivalents :

(i) $b \in G$ engendre $(G, \bullet)$

(ii) Il existe un entier p, $p \in \{1, 2, \ldots, n\}$, premier avec n ,tel que : $b = a^p$.

Démonstration : Supposons (i) et écrivons $b = a^p$; puisque b engendre G, cela équivaut à dire qu'il existe un entier p' tel que $b^{p'} = a^{pp'} = a$; de ce fait $pp' - 1$ appartient à $n\mathbb{Z}$ et tout est démontré (Bezout).

Autrement dit, dans un groupe cyclique ayant n éléments il y a autant de générateurs que d'entiers compris entre 1 et n et premiers avec n ; cette observation justifie la définition suivante :

Définition : Si $n \geq 1$ est un entier, on note symboliquement $\varphi(n)$ le nombre d'entiers compris entre 1 et n et premiers avec n ; la fonction φ s'appelle alors *la fonction indicatrice d'Euler* ; elle sera, ultérieurement, précisée davantage, mais déjà on peut énoncer :

Proposition 7 (formule de Möbius) :

$$\sum_{\substack{d|n \\ 1 \leq d \leq n}} \varphi(d) = n$$

le symbole $d|n$ indiquant que d divise n.

Démonstration : Soit $(G, \bullet)$ un groupe cyclique ayant n éléments ; pour $x \in G$, convenons d'appeler ordre de x le nombre d'éléments du sous-groupe cyclique $[x]$ engendré par x.

Soit $\mathcal{D} = \{d \in \{1, 2, \ldots, n\} : d|n\}$ et pour $d \in \mathcal{D}$, soit H_d l'unique sous-groupe cyclique de $(G, \bullet)$ ayant d éléments ; via ce qui vient d'être dit, il y a exactement $\varphi(d)$ éléments du groupe G d'ordre d exactement ; lorsque d décrit $\mathcal{D}$ l'ensemble de tous les éléments de G ainsi fabriqués coïncide avec G, d'où la formule de Möbius qui, bien que pouvant se démontrer autrement, traduit avant tout une réalité algébrique commune à tous les groupes cycliques ayant n éléments.

C'est, dans cet ouvrage, le moment de définir une notion essentielle en cryptologie : *le logarithme discret* ; d'où :

Définition : Soit $(G, \bullet)$ un groupe cyclique ayant n éléments et α un générateur de G ; pour tout β de G il existe un unique entier a défini modulo n tel que :

$$\beta = \alpha^a$$

a s'appelle le logarithme discret de β en base α.

Remarques :

1. Si la loi de G est notée additivement, ce qui est notamment le cas des courbes elliptiques, le logarithme discret de β en base α est l'unique entier a défini modulo n par :
$$\beta = a\alpha$$
2. En général, si la loi du groupe G est sans ordre prévisible, il est "calculatoirement" difficile de déterminer a connaissant β et α ; cette circonstance est spécifiée en disant que dans le groupe $(G, \bullet)$ le problème du logarithme discret est difficile. Cependant, il existe des algorithmes (voir chapitre **7**) permettant, dans certains cas, de résoudre, avec un coût raisonnable en temps, le problème du logarithme discret.

Tout au long de cet ouvrage, le lecteur attentif pourra régulièrement se familiariser avec le logarithme discret aussi bien dans les groupes multiplicatifs des corps $\mathbb{Z}/p\mathbb{Z}$ (p premier) que dans les groupes additifs des courbes elliptiques.

b.3. Produit de groupes cycliques

Leur étude est réglée par le théorème suivant :

Proposition 8 : Soient $(G_1, \bullet), (G_2, \bullet), \cdots, (G_q, \bullet)$ q groupes cycliques ($q \geq 2$) d'ordres respectifs $n_1, n_2, \ldots, n_q$; les deux énoncés suivants sont équivalents :

(i) Le groupe produit $G = G_1 \times G_2 \times \cdots \times G_q$ est cyclique.

(ii) Les entiers $n_1, n_2, \ldots, n_q$ sont deux à deux premiers entre eux.

Démonstration : Elle s'effectue par récurrence sur l'entier q.

1° pas : Supposons $q = 2$ et $n_1 \wedge n_2 = 1$ (*ie* premiers entre eux) ; désignons par a_1 (*resp.* a_2) un générateur de G_1 (*resp.* de G_2).

Soit (a_1, a_2) l'élément de $G_1 \times G_2$; si m est un entier on peut écrire dans le groupe produit $G_1 \times G_2$, d'élément neutre (e_1, e_2) :

$$(a_1, a_2)^m = (a_1^m, a_2^m) = (e_1, e_2) \textit{ si et seulement si } \; a_1^m = e_1 \text{ et } a_2^m = e_2$$

ie si et seulement si m est un multiple commun à n_1 et n_2 *ie si et seulement si* m est un multiple de $n_1 \cdot n_2$; par conséquent le morphisme :

$$m \in (\mathbb{Z}, +) \longrightarrow (a_1, a_2)^m \in G_1 \times G_2$$

admet $n_1 n_2 \mathbb{Z}$ pour noyau ; cela signifie que (a_1, a_2) est d'ordre $n_1 n_2$ dans $G_1 \times G_2$, *ie* que le groupe produit $G_1 \times G_2$ est cyclique.

Si maintenant $q \geq 3$, $G_1 \times G_2 \times \cdots \times G_q = G_1 \times G_1'$ où $G_1' = G_2 \times \cdots \times G_q$; par hypothèse de récurrence G_1' est cyclique d'ordre $n_2 n_3 \cdots n_q$ premier avec n_1 et on achève (ii)⇒(i) en utilisant ce qui a été prouvé dans le cas où $q = 2$.

2° pas : Il s'agit de prouver que l'énoncé (i) implique (ii) ; supposons encore une fois $q = 2$; puisque $G_1 \times G_2$ est cyclique d'ordre $n_1 n_2$ pour la structure de groupe produit,

on peut trouver $(a,b) \in G_1 \times G_2$ d'ordre $n_1 n_2$ dans $G_1 \times G_2$; or l'ordre de (a,b) est bien évidemment égal au ppcm des ordres de a et b ; comme l'ordre de a dans G_1 (*resp.* de b dans G_2) n'excède pas n_1 (*resp.* n_2) il est nécessaire que a soit un générateur de G_1 (*resp.* b de G_2) et que $n_1 n_2 = ppcm(n_1; n_2)$; cela impose bien évidemment n_1 et n_2 premiers entre eux.

Supposons maintenant $q \geq 3$ et $G_1 \times G_2 \times \cdots \times G_q$ cyclique ; posons $G_1' = G_2 \times \cdots \times G_q$. Le sous-ensemble des (e_1, x) avec e_1 élément neutre de G_1, et x décrivant G_1' est un sous-groupe du groupe cyclique $G_1 \times G_1'$; il est donc cyclique et comme il est isomorphe à G_1', G_1' est donc lui aussi cyclique ; par hypothèse de récurrence $n_2, n_3, \cdots n_q$ sont des entiers deux à deux premiers entre eux et, *via* ce qui a été fait dans le cas où $q = 2$, n_1 est premier avec $n_2 n_3 \cdots n_q$ donc avec $n_2, \ldots, n_q$.

Corollaire : Soient n et m deux entiers premiers entre eux, alors on a :

$$\varphi(nm) = \varphi(n)\varphi(m)$$

et si n est un entier avec $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ pour décomposition primaire on a :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

Démonstration : Soient $n_1, n_2, \cdots n_r$ r nombres entiers deux à deux premiers entre eux et, pour chaque indice i, $i = 1, 2, \ldots, r$, G_i un groupe cyclique ayant n_i éléments ; le groupe produit $\prod_{1 \leq i \leq r} G_i$ est cyclique et à ce titre possède $\varphi(n_1 n_2 \cdots n_r)$ générateurs ; soit a_i $i = 1, 2, \ldots, r$ un générateur arbitraire du groupe G_i et $b = (a_1, a_2, \ldots, a_r)$. Pour m entier, dans le groupe produit des G_i, on peut écrire :

$$b^m = (a_1^m, a_2^m, \ldots, a_r^m)$$

et b^m est l'élément neutre du groupe produit $G_1 \times G_2 \times \cdots \times G_r$, *si et seulement si* m est un multiple du ppcm de $n_1, n_2, \ldots, n_r$, *ie* un multiple de $n_1 n_2 \cdots n_r$ puisque les entiers $n_1, n_2, \ldots, n_r$ sont deux à deux premiers entre eux ; cela revient à dire que $(a_1, a_2, \ldots, a_r)$ est un générateur du groupe cyclique $G_1 \times \cdots \times G_r$; réciproquement si $(a_1, \ldots, a_r)$ est un générateur du groupe cyclique $G_1 \times \cdots \times G_r$, chaque a_i génère G_i pour $i = 1, 2, \ldots, r$; ainsi on peut écrire :

$$\varphi(n_1 n_2 \cdots n_r) = \varphi(n_1)\varphi(n_2)\cdots\varphi(n_r)$$

Si, en particulier, $n_i = p_i^{\alpha_i}$ avec p_i nombre premier, calculer $\varphi(n_i)$ revient à calculer $\varphi(p^\alpha)$ pour p premier : or, de la définition de $\varphi(p^\alpha)$ il vient aussitôt :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$

Le corollaire est entièrement démontré et sera réenvisagé d'une autre manière dans un autre chapitre.

b.4. Dénombrements dans un groupe cyclique

Ils seront utiles au chapitre **3** concernant les anneaux et plus précisément dans l'étude du test de primalité de Miller-Rabin.

Proposition 8 bis : Soit $(G, \bullet)$ un groupe cyclique ayant n éléments, d'élément neutre e.

(i) Si p est un entier non nul on a :

$$card\{x \in G : x^p = e\} = pgcd(n, p) = q$$

(ii) Si $b \in G, b \neq e$ et si $p \in \mathbb{N}^*$ sont donnés on peut trouver x dans G tel que $x^p = b$ *si et seulement si* $b^{n/q} = e$, où $q = p \wedge n$ et en outre :

$$card\{x \in G : x^p = b\} = q = n \wedge p$$

Démonstration : Pour ce qui concerne (i), écrivons : $G = \{e, a, \ldots, a^{n-1}\}$ où a est un générateur de $(G, \bullet)$; si x appartient à G, il existe j unique de $\{0, 1, \ldots, n-1\}$ tel que : $x = a^j$ et pour obtenir $x^p = e$ il faut avoir $a^{pj} = e$ *ie* pj multiple de l'entier n ; désignons par q le pgcd de n et p *ie* : $q = n \wedge p$, ainsi :

$$n = n'q, p = p'q \text{ avec } n' \wedge p' = 1$$

De ce fait n divise pj *si et seulement si* n' divise j, ce qui impose : $j = 0, j = n'$, $j = 2n', \ldots, j = (q-1)n'$ et prouve l'assertion (i) de cette proposition.

Supposons donc (assertion (ii)), puisque b appartient à G, que l'on ait : $b = a^j$ avec : $j \in \{1, 2, \ldots, n-1\}$; s'il existe x dans G tel que $x^p = b = a^j$ on a, via les notations précédentes : $x^{p'q} = a^j$ et alors : $x^{p'qn'} = x^{p'n} = e = a^{jn'} = b^{n'}$ d'après le théorème de Lagrange, ou par application immédiate de la proposition 9 de **2.1.5.**

Réciproquement si on suppose $b^{n'} = b^{n/q} = e$ montrons l'existence de x appartenant à G vérifiant $x^p = b$. En effet écrivons $x = a^k$ avec $k \in \{0, 1, \cdots n-1\}$ et cherchons k afin que : $b = x^p$.

$x^p = b$ équivaut à :

$$a^{pk} = a^j = b \ ie \ \ pk - j \text{ multiple de } n$$

Comme : $b^{n'} = a^{jn'} = e$ cela impose $jn' = 0$ modulo n ou encore : $j = j'q$ de sorte que : $pk - j$ est multiple de n *si et seulement si* : $pk - j'q = p'qk - j'q$ est un multiple de n ce qui est vérifié *si et seulement si* :

$$p'k - j' \text{ est un multiple de } n'$$

Or les entiers n' et p' sont premiers entre eux ; on peut donc trouver u et v entiers tels que : $up' + vn' = 1$; dans ces conditions on a : $j' = j'up' + j'vn'$ si bien que :

$$p'k - j' = p'k - p'j'u - j'vn' \ \ ie :$$

$$p'k - j' = p'(k - j'u) - j'vn'$$

et la condition $p'k - j'$ multiple de n' est satisfaite *si et seulement si* $k - j'u$ est un multiple de l'entier n' ; ainsi :

$$k = (j'u + k'n') \text{ modulo } n$$

et on obtient exactement pour $k' = 0, 1, 2, \ldots, q-1$, $q = p \wedge n$ solutions distinctes ce qui prouve entièrement la proposition 8 bis dont une utilisation sera faite au chapitre **3**, à propos du test de primalité de Miller-Rabin.

2.1.5 Exposant d'un groupe fini - Cas des groupes abéliens

a. Commençons d'abord par une remarque générale :

Proposition 9 : Si $(G, \bullet)$ est un groupe fini quelconque ayant n éléments, pour tout a de G, $a^n = e$ (élément neutre de $(G, \bullet)$).

Cela résulte immédiatement du théorème de Lagrange ; en effet, soit $H = [a]$ le groupe cyclique engendré par a ; si p est le nombre d'éléments de H, p divise n ; comme $a^p = e$, *a fortiori*, on a bien $a^n = e$.

Par définition on appelle *exposant* d'un groupe fini $(G, \bullet)$ le ppcm des divers ordres des éléments a de G ; c'est, *via* ce qui précède, un diviseur de l'entier n, cardinal du groupe.

b. Cas des groupes abéliens

Dans ce cas la proposition suivante apporte une information supplémentaire.

Proposition 10 : Si $(G, \bullet)$ est un groupe abélien fini et si m est l'exposant de G, on peut toujours trouver un élément a de G, d'ordre m.

Démonstration : Elle s'effectue en trois étapes :

1° étape : Soient x et y dans G d'ordres respectifs p et q premiers entre eux ; alors l'élément $z = xy$ de G est d'ordre pq ; en effet si m est un nombre entier, et puisque G est abélien on peut écrire :

$$z^m = x^m y^m$$

et si $z^m = e$, on a :

$$x^{pm} y^{pm} = e = y^{pm}$$

cela impose pm multiple de l'entier q et puisque p et q sont premiers entre eux, il est nécessaire que m soit un multiple de q ; de même m doit être un multiple de p ; en définitive m est un multiple de pq, ce qui prouve bien ce que nous annoncions.

2° étape : Soient x et y dans G d'ordre p et q quelconques c'est-à-dire non nécessairement premiers entre eux ; alors on peut trouver z dans G dont l'ordre est le ppcm des entiers p et q. En effet il suffit d'utiliser convenablement la première étape. Soit

$r = ppcm(p, q)$; on peut donc (vérification aisée) écrire : $r = r'r''$ où r' divise p, r'' divise q et où $r' \wedge r'' = 1$.

Comme r' divise l'entier p on peut donc trouver un élément a du sous-groupe engendré par x d'ordre r' (proposition 5) ; de même il existe b appartenant à $[y]$ d'ordre r'' ; *via* la première étape, on en déduit que l'élément ab de G est d'ordre r.

3° étape : Soient $n_1, n_2, \ldots, n_r$ les divers ordres possibles de tous les éléments de $(G, \bullet)$; on peut donc trouver $a_1 \in G$ dont l'ordre est le ppcm m_1 des entiers n_1 et n_2, puis ensuite trouver $a_2 \in G$ dont l'ordre est le ppcm des entiers m_1 et n_3, et ainsi de suite jusqu'à épuisement du stock...

Corollaire : Soit $(G, \bullet)$ un groupe abélien ayant pq éléments où p et q sont deux nombres premiers distincts. Alors le groupe $(G, \bullet)$ est isomorphe au groupe additif produit :

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Démonstration : Supposons d'abord qu'il existe un élément a de G d'ordre pq ; dans ces conditions le groupe $(G, \bullet)$ est cyclique ; comme $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ sont, munis de l'addition, des groupes cycliques et puisque $p \wedge q = 1$, le groupe additif produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ est lui aussi cyclique et possède pq éléments ; il est donc isomorphe à G puisque deux groupes cycliques sont isomorphes *si et seulement si* ils ont le même nombre d'éléments.

S'il n'existe pas d'élément a d'ordre pq dans G, soit a un élément de G d'ordre p (p et q jouant le même rôle, ce cas de figure est légitime) ; puisque $(G, \bullet)$ est abélien, le groupe quotient $G/[a]$ possède q éléments avec q premier ; il est donc cyclique. Soit $\bar{b}$ (classe de b) un générateur du groupe $G/[a]$; ainsi :

$$G/[a] = \{\bar{e}, \bar{b}, \bar{b}^2, \ldots, \bar{b}^{(q-1)}\}$$

l'ordre de b dans le groupe $(G, \cdot)$ ne peut être égal à p ; en effet, sinon, en écrivant par division euclidienne : $p = kq + r$ avec : $1 \leq r \leq q - 1$, il vient : $b^p = e = b^{qk}b^r$, ce qui impose : $\bar{b}^r = \bar{e}$ avec $r \leq q - 1$ et $r \geq 1$; comme c'est impossible l'ordre de b dans G vaut q ou pq ; comme on suppose qu'il n'existe pas d'élément d'ordre pq, l'ordre de b vaut q ; mais on a démontré qu'alors l'élément ab de G est d'ordre pq, ce qui est encore exclu par hypothèse.

En définitive il existe toujours dans $(G, \bullet)$ un élément d'ordre pq ce qui achève la preuve du corollaire.

Remarque : S'agissant des groupes abéliens finis, il existe un résultat plus profond que nous admettons et dont voici l'énoncé :

Proposition 11 : Si $(G, \bullet)$ est un groupe abélien fini on peut trouver des entiers : $n_1 \leq n_2 \leq \cdots \leq n_r$, avec $n_1 \geq 2$ et où, si $r \geq 2$, pour tout $i = 1, 2, \ldots, r - 1$, n_i divise n_{i+1}, et tels que $(G, \bullet)$ soit isomorphe au groupe additif produit :

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

Dans ces conditions l'entier n_r désigne le nombre d'éléments du plus "gros" sous-groupe cyclique de $(G, \bullet)$; c'est donc l'exposant de G ; bien évidemment par application immédiate de cette proposition on voit que si G est abélien et possède pq éléments avec p et q premiers distincts, G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$, donc à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ (en tant que groupes additifs).

2.2 Les anneaux

2.2.1 Définition

La notion d'anneau est une notion fondamentale en cryptologie, comme la suite de cet ouvrage le montrera.

Par définition, un anneau A est un triplet $(A, +, \bullet)$ où le couple $(A, +)$ est un groupe (additif) abélien et où $\bullet$ est une loi de composition interne (appelée multiplication) sur A, associative, admettant un élément neutre e, et doublement distributive par rapport à l'addition ; ainsi :

$$\forall x \in A,\ e \cdot x = x \cdot e = x$$

et pour tous x, y, z de A :

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(x + y) \cdot z = x \cdot z + y \cdot z$$

Si, en outre, $x \cdot y = y \cdot x$ pour tous x, y de A on dit alors que l'anneau est *commutatif*.

Idéal d'un anneau

Une partie I d'un anneau est dit *idéal à gauche* (*resp.* à droite) de A s'il possède les deux propriétés suivantes :

$$\forall x, \forall y \in I,\ \ x - y \in I$$
$$\forall x \in I, \forall a \in A,\ \ a \cdot x\ (resp.\ \ x \cdot a) \text{ appartient à } I$$

I est dit *idéal bilatère* s'il est idéal à gauche et à droite ; en particulier si A est commutatif ces deux notions coïncident.

Morphisme d'anneau

Soient A et A' deux anneaux, une application f de A dans A' est un morphisme *si et seulement si* elle possède les trois propriétés suivantes :

(i) $f(x + y) = f(x) + f(y)$ pour tous $x, y \in A$

(ii) $f(xy) = f(x)f(y)$ pour tous $x, y \in A$

(iii) $f(e) = e'$; e (*resp.* e') étant l'élément neutre de A (*resp.* A') pour la multiplication.

2.2.2 Calculs modulo un idéal bilatère dans un anneau A - Applications

a. Généralités

Soit A un anneau, non nécessairement commutatif et I un idéal bilatère de cet anneau.

Dans A, la relation binaire : $x \sim y$ *si et seulement si* $x - y \in I$ est, comme on le vérifie aisément, une relation d'équivalence et, pour $x \in A$, la classe de x notée $\bar{x}$ est l'ensemble $x + I = \{x + i, i \in I\}$ et s'appelle la *classe résiduelle* de x dans A modulo I ; par définition, l'ensemble des $\bar{x}$ lorsque x décrit A est noté A/I.

Proposition 12 : Si A est un anneau et I un idéal bilatère de A le quotient algébrique A/I dispose d'une structure d'anneau si l'on pose par définition :

$$\bar{x} + \bar{y} = \overline{x + y}$$
$$\bar{x} \cdot \bar{y} = \overline{xy}$$

Démonstration : Il faut d'abord, comme pour les groupes quotients, s'assurer de la cohérence des définitions formulées.

Soient donc x, x' et y, y' dans tels que :

$$\bar{x} = \bar{x}' \text{ et } \bar{y} = \bar{y}'$$

$x - x'$ et $y - y'$ appartiennent à l'idéal I ; leur somme : $(x + y) - (x' + y')$ est donc aussi dans I, ce qui prouve la cohérence de la définition de l'addition dans A/I.

Ensuite, s'agissant de la multiplication, on écrit : $xy - x'y' = (x - x')y + x'(y - y')$ qui appartient bien à I puisque I est un idéal bilatère de A.

Ceci étant démontré on vérifie aisément que le triplet $(A/I, +, \bullet)$ ainsi constitué est un anneau.

Proposition 13 : Soit $f : A \to A'$ un morphisme d'anneaux, son noyau $Ker\ f = \{x \in A : f(x) = 0\}$ est un idéal bilatère de A et l'anneau image $f(A')$ est isomorphe à l'anneau quotient : $A/Ker\ f$

En effet, par utilisation du schéma de décomposition canonique de l'application f (voir chapitre **1, 1.1.2**) on constate immédiatement que l'application b de $A/Ker\ f$ dans $f(A)$ définie par :

$$b(\bar{x}) = f(x)$$

est un morphisme bijectif (*ie* par définition un isomorphisme) de l'anneau quotient $A/Ker\ f$ sur l'image $f(A)$.

b. Idéaux maximaux dans un anneau commutatif

C'est une notion fondamentale en arithmétique modulaire.

Définition : Etant donné un anneau A, un idéal I de A est dit *maximal* si les inclusions : $I \subset J \subset A$, où J est un idéal de A, impliquent : soit $J = I$, soit $J = A$.

En termes plus prosaïques, dire qu'un idéal I d'un anneau A est maximal, revient à dire qu'il n'est pas possible "d'intercaler" entre I et A d'autres idéaux autres que les triviaux.

Dans le cas supplémentaire et courant en pratique où A est commutatif, on peut énoncer le résultat fondamental suivant :

Proposition 14 : Soit $(A, +, \bullet)$ un anneau commutatif et I un idéal de A distinct de A ; alors les deux énoncés suivants sont équivalents :

(i) I est maximal dans A

(ii) Le triplet $(A/I, +, \bullet)$ est un corps.

Démonstration : Supposons d'abord (i) et montrons alors que l'anneau quotient A/I est un corps *ie* que tout élément non nul de A/I est inversible dans $(A/I, +, \bullet)$.

Soit donc $\bar{x} \in A/I$, $\bar{x} \neq 0$, c'est-à-dire, x n'appartenant pas à I ; dans ces conditions l'idéal engendré par I et $\{x\}$, c'est-à-dire : $I + xA = \{j + ax, j \in I, a \in A\}$ contient strictement I ; il est donc égal à A ; ainsi on peut trouver x' dans A et j dans I tels que :

$$xx' + j = e \text{ (élément neutre multiplicatif de } A)$$

Dans ces conditions : $\bar{x}\bar{x}' = \bar{e}$ ce qui prouve (ii).

Réciproquement supposons (i) et soit J un idéal de A, contenant strictement I ; on peut donc trouver $x \in J$, $x \notin I$; $\bar{x}$ est donc dans A/I un élément non nul et de ce fait, puisqu'on dispose d'un corps, inversible ; ainsi il existe $x' \in A$ tel que :

$$\bar{x}\bar{x}' = \bar{e}$$

ou encore :

$$xx' - e \in I \subset J$$

Comme xx' appartient à J (puisque J est un idéal) l'élément neutre e est aussi dans J ; cela impose : $J = A$ et achève la preuve de la proposition 14.

Exemples : (ils sont utilisés en permanence en arithmétique modulaire)

Si $A = \mathbb{Z}$, tout idéal étant du type $I = p\mathbb{Z}$, le quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps *si et seulement si* $p\mathbb{Z}$ est maximal dans $\mathbb{Z}$ *ie si et seulement si* p est un nombre premier.

Si $A = \mathbb{K}[X]$ où $\mathbb{K}$ est un corps, tout idéal étant du type : $I = P(X)\mathbb{K}[X]$, le quotient A/I est un corps *si et seulement si* P est un polynôme irréductible de $\mathbb{K}[X]$.

Cela nous amène tout naturellement au troisième paragraphe de ce chapitre.

2.3 Les corps

2.3.1 Définitions

Un corps est, par définition, un anneau commutatif tel que tout élément non nul est inversible.

La proposition précédente élabore un protocole de construction d'un corps à partir d'une structure algébrique moins riche, à savoir celle d'un anneau commutatif et d'un idéal maximal de cet anneau.

Bien évidemment, dans un corps, la notion d'idéal est inutile, puisque les deux seuls idéaux d'un corps $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$. L'usage veut que l'on note 1 l'élément neutre de $(\mathbb{K}^*, \bullet)$.

2.3.2 Le groupe multiplicatif $(\mathbb{K}^*, \bullet)$

Il possède une propriété tout à fait remarquable résultant de l'énoncé suivant :

Proposition 15 : Si $\mathbb{K}$ est un corps, tout sous-groupe fini du groupe $(\mathbb{K}^*, \bullet)$ est cyclique.
En particulier, si $\mathbb{K}$ est un corps fini, $(\mathbb{K}^*, \bullet)$ est cyclique.

Démonstration : Soit G un sous-groupe fini de $(\mathbb{K}^*, \bullet)$; désignons par n le nombre d'éléments de G et par m son exposant. Ainsi pour tout x de G on peut écrire :

$$x^m = 1$$

Dans ces conditions, le polynôme $X^m - 1$ de $\mathbb{K}[X]$ s'annule en tout x de G ; par conséquent son degré m est au moins égal à n (puisqu'il possède au moins n racines distinctes) ; mais l'exposant du groupe G n'excède pas n, nombre d'éléments du groupe.

En définitive $m = n$ et comme on sait (proposition 10) qu'il existe dans G un élément d'ordre m, $(G, \bullet)$ est cyclique.

2.3.3 Caractéristique d'un corps - Calculs dans un corps de caractéristique p

Elle se définit par application de l'énoncé suivant :

Proposition 16 : Soit $\mathbb{K}$ un corps ; l'application f de $\mathbb{Z}$ dans $\mathbb{K}$ définie par : $f(m) = m1_{\mathbb{K}}$ (où $1_{\mathbb{K}}$ est l'élément neutre de la multiplication dans $\mathbb{K}$) est un morphisme d'anneau ; son noyau $Ker\ f$ est, s'il n'est pas réduit à $\{0\}$, du type $p\mathbb{Z}$ avec $p \geq 2$ premier ; le corps $\mathbb{K}$ est alors dit de caractéristique p.

Démonstration : f est bien évidemment un morphisme d'anneau au demeurant jamais injectif si le corps $\mathbb{K}$ est un corps ayant un nombre fini d'éléments.

Si $Ker\ f \neq \{0\}$, c'est un idéal de $\mathbb{Z}$ du type $p\mathbb{Z}$ et si $p = p'p''$ on doit avoir $(p'1_{\mathbb{K}})(p''1_{\mathbb{K}}) = 0$ ce qui entraîne, puisque $\mathbb{K}$ est un corps, ou bien $p'1_{\mathbb{K}} = 0$ ou bien $p''1_{\mathbb{K}} = 0$, et prouve, à souhait, que p est un nombre premier.

Si p est le caractéristique de $\mathbb{K}$, $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ qui est, on l'a vu, un corps ; or $f(\mathbb{Z}) = \{0, 1_{\mathbb{K}}, 2 \cdot 1_{\mathbb{K}}, \ldots, (p-1)1_{\mathbb{K}}\}$; cela prouve que dans tout corps de caractéristique p il y a un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$, mais on y reviendra.

Ceci étant acquis si a et b sont dans $\mathbb{K}$ de caractéristique p on a :

$$(a+b)^{p^m} = a^{p^m} + b^{p^m}$$

quel que soit l'entier naturel m ; en effet, quitte à effectuer une démonstration par récurrence sur m, on peut supposer $m = 1$; or, via la formule du binôme on a :

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p$$

et comme $\binom{p}{i}$ est un multiple de l'entier p (car p est premier) la preuve est assurée.

2.3.4 Les polynômes cyclotomiques sur un corps $\mathbb{K}$

1.3.4.1 Introduction

Elle commence par la proposition suivante :

Proposition 17 : Soit $\mathbb{K}$ un corps quelconque ; l'application de $\mathbb{Z}[X]$ dans $\mathbb{K}[X]$ définie par :

$$u\left(\sum_i a_i X^i\right) = \sum_i \left(a_i \cdot 1_{\mathbb{K}}\right) X^i$$

où $1_{\mathbb{K}}$ est l'élément neutre de $\mathbb{K}$, est un morphisme d'anneau.

En effet tout se vérifie aisément et est laissé aux soins du lecteur ; par commodité d'écriture le polynôme $u(\sum a_i X^i)$ est encore noté : $\sum_i a_i X^i$, où il est alors entendu que pour tout $a \in \mathbb{Z}$, aX^i est l'élément de $\mathbb{K}[X]$ égal à $(a \cdot 1_{\mathbb{K}})X^i$; en général u n'est pas injectif...

1.3.4.2 Les polynômes cyclotomiques dans $\mathbb{C}[X]$

a. Définition Par définition, si n est un entier, on désigne par $\Phi_n(X)$ l'élément de $\mathbb{C}[X]$ défini par :

$$\Phi_1(X) = X - 1 \text{ et si } n \geq 2, \Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

Puisque : $\{e^{\frac{2ik\pi}{n}}, \text{pour } k = 1, 2, \ldots, n \text{ et } k \wedge n = 1\}$ est l'ensemble des générateurs du groupe des racines n-ièmes de l'unité, le polynôme Φ_n est le polynôme unitaire de $\mathbb{C}[X]$ dont les racines sont simples et constituées de tous les générateurs du groupe des z de $\mathbb{C}^*$ tels que $z^n = 1$.

Φ_n est appelé n-ième *polynôme cyclotomique*.

b. Le caractère "universel" des Φ_n

Leur intérêt en arithmétique modulaire réside dans l'énoncé suivant :

Proposition 18 : Pour tout entier n le polynôme $\Phi_n(X)$ est à coefficients entiers ; en outre on a la formule dans $\mathbb{Z}[X]$:

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Démonstration : Commençons par démontrer l'égalité polynomiale indiquée et pour cela écrivons dans $\mathbb{C}[X]$:

$$X^n - 1 = \prod_{1 \leq k \leq n} \left(X - e^{\frac{2ik\pi}{n}} \right)$$

notons alors pour d entier par Ω_d l'ensemble des entiers k de $1, 2, \ldots, n$ vérifiant :

$$k \wedge n = d$$

ie :

$$k = k'd, n = n'd \text{ avec } k' \wedge n' = 1$$

On peut donc écrire :

$$X^n - 1 = \prod_{d|n} \left(\prod_{k \in \Omega_d} \left(X - e^{\frac{2ik\pi}{n}} \right) \right) = \prod_{d|n} \left(\prod_{\substack{1 \leq k' \leq n' \\ k' \wedge n' = 1}} \left(X - e^{\frac{2ik'\pi}{n'}} \right) \right)$$

Autrement dit, on a :

$$X^n - 1 = \prod_{d|n} \Phi_{n/d}(X) = \prod_{d|n} \Phi_d(X)$$

Ceci étant acquis supposons (hypothèse de récurrence) que les polynômes $\Phi_1, \Phi_2, \ldots, \Phi_{n-1}$ sont à coefficients entiers ; ainsi nous avons dans $\mathbb{C}[X]$:

$$X^n - 1 = \Phi_n(X)P(X)$$

où $P(X) \in \mathbb{Z}[X]$. Par division euclidienne dans $\mathbb{Z}[X]$ légitime puisque $P(X)$ appartient à $\mathbb{Z}[X]$ et est unitaire, on peut écrire :

$$X^n - 1 = P(X)Q(X) + R(X)$$

et comme il y a unité dans $\mathbb{C}[X]$ de la division euclidienne, on a : $R(X) = 0$ et $Q(X) = \Phi_n(X)$ ce qui prouve ce que nous voulions.

Remarques :

1. Par construction le degré de $\Phi_n(X)$ est égal à $\varphi(n)$, où φ est l'indicatrice d'Euler ; si on identifie les degrés dans l'égalité $X^n - 1 = \prod_{d|n} \Phi_d(X)$ on obtient :

$$n = \sum_{d|n} \varphi(d)$$

ie la formule de Möbius démontrée précédemment (proposition 7) dans ce chapitre **2**.

2. Les polynômes $\Phi_n(X)$ étant tous à coefficients entiers, on peut donc, par utilisation de la proposition 17, affirmer que dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps quelconque, on a encore la relation :

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

où il est entendu que l'on "confond" bien légitimement $u(\Phi_d)$ et Φ_d, 1 étant alors l'élément neutre multiplicatif de $\mathbb{K}$.

c. Les polynômes cyclotomiques et les racines primitives n-ièmes de l'unité dans un corps $\mathbb{K}$

On commence par la définition suivante :

Définition : Si $\mathbb{K}$ est un corps, et n un entier, un élément x de $\mathbb{K}^*$ est dit *racine primitive n-ième de l'unité* dans $\mathbb{K}$ si le sous-groupe cyclique de $(\mathbb{K}^*, \bullet)$ engendré par x est d'ordre n.

Cela revient à dire que $x^n = 1$ et $x^m \neq 1$ pour tout entier m strictement inférieur à n, $m \geq 1$.

Par exemple : dans $\mathbb{C}^*$, z est une racine primitive n-ième de 1 *si et seulement si* c'est un générateur des racines n-ièmes de 1, *ie si et seulement si* z s'écrit $e^{2i\frac{k\pi}{n}}$ avec $1 \leq k \leq n$ et $k \wedge n = 1$. On voit donc que dans $\mathbb{C}$ les racines primitives n-ièmes de 1 sont exactement les racines dans $\mathbb{C}$ du n-ième polynôme cyclotomique Φ_n.

Cette propriété peut se généraliser ce qui fait l'objet de l'énoncé suivant et confère aux polynômes Φ_n un caractère universel :

Proposition 19 : Soit $\mathbb{K}$ un corps de caractéristique p et n un entier tels que $p \wedge n = 1$; alors pour a de $\mathbb{K}^*$ les deux énoncés suivants sont équivalents :

(i) a est une racine primitive n-ième de 1 dans $\mathbb{K}$

(ii) $\Phi_n(a) = 0$

Démonstration : En effet si (i) est vérifié $a^n = 1$, et de ce fait $\prod_{d|n} \Phi_d(a) = 0$; par conséquent il existe d entier, d divisant n avec $\Phi_d(a) = 0$; si d est strictement inférieur à n, étant donné que $X^d - 1 = \prod_{\delta|d} \Phi_\delta(X)$ on obtient aussitôt $a^d = 1$, ce qui est impossible puisque a est d'ordre n dans le groupe multiplicatif de $\mathbb{K}$; cela prouve donc (ii).

Réciproquement si $\Phi_n(a) = 0$ on obtient immédiatement $a^n = 1$; désignons alors par d l'ordre de a ; si on suppose d strictement inférieur à n, d divise n et $a^d = 1$; dans ces conditions puisque a est racine d'un $\Phi_\delta(X)$ avec δ divisant d, a est au moins racine double dans $\mathbb{K}[X]$ du polynôme $X^n - 1$ et on peut écrire dans $\mathbb{K}[X]$:

$$X^n - 1 = (X - a)^2 Q(X)$$

par dérivation polynomiale il vient alors :

$$nX^{n-1} = (X - a)R(X)$$

ce qui impose : $na^{n-1} = 0$ ou encore $n \cdot 1_{\mathbb{K}} = 0$.

Mais l'entier n est premier avec la caractéristique p de $\mathbb{K}$; il est donc impossible d'avoir $n \cdot 1_{\mathbb{K}}$ et dans ces conditions a est bien racine primitive n-ième de 1 dans $\mathbb{K}$.

Nous retrouverons dans le chapitre **4** notamment les polynômes cyclotomiques car ils jouent, comme nous le verrons, un rôle essentiel dans l'arithmétique modulaire...

d. Un résultat concernant les polynômes cyclotomiques

Proposition 20 : Soit n un entier impair ; alors on a la relation :

$$\Phi_{2n}(X) = \Phi_n(-X)$$

Démonstration : En effet rappelons que si $p \wedge q = 1$ et si $pp' + qq' = 1$, on a montré que l'application : $(\bar{\bar{a}}, \bar{\bar{b}}) \in \mathbb{Z}/(p) \times \mathbb{Z}/(q) \to \overline{\overline{pp'b + qq'a}} \in \mathbb{Z}/(pq)$ est un isomorphisme d'anneau (lemme chinois).

Par suite les éléments de G_{2n} (groupe des inversibles de l'anneau $\mathbb{Z}/2n\mathbb{Z}$) sont du type : $\bar{k}'$ où $k' = n - (n-1)k$ (on applique ce qui vient d'être dit avec $p = 2$, $n = 2r + 1$, $p' = -r$, $q' = 1$) avec $\bar{k} \in G_n$ *ie* k inversible modulo n. Comme : $\Phi_{2n}(X) = \prod_{\bar{k}' \in G_{2n}} \left(X - e^{\frac{2ik'\pi}{2n}}\right)$ on a :

$$\Phi_{2n}(X) = \prod_{\bar{k} \in G_n} \left(X - e^{\frac{2i\pi(n-(n-1)k)}{2n}}\right)$$

d'où :

$$\Phi_{2n}(X) = \prod_{\bar{k} \in G_n} \left(X + e^{-\frac{2ik(n-1)\pi}{2n}}\right)$$

ce qui donne :

$$\Phi_{2n}(X) = \prod_{\bar{k} \in G_n} \left(X + e^{\frac{2ik\pi}{n}\left(\frac{1-n}{2}\right)}\right) = \Phi_{2n}(X) = \prod_{\bar{k} \in G_n} \left(X + e^{-\frac{2ik\pi r}{n}}\right)$$

Comme $\bar{r}$ appartient à G_n lorsque $\bar{k}$ décrit G_n, $\overline{rk}$ décrit aussi G_n ; ainsi on peut écrire :

$$\Phi_{2n}(X) = \prod_{\bar{k} \in G_n} \left(X + e^{\frac{2ik\pi}{n}}\right) = \Phi_n(-X)$$

puisque l'on a : $\Phi_n(-X) = (-1)^{\varphi(n)} \prod_{\bar{k} \in G_n} \left(X + e^{\frac{2ik\pi}{n}}\right) = \prod_{\bar{k} \in G_n} \left(X + e^{\frac{2ik\pi}{n}}\right)$ car $\varphi(n)$ est un entier pair dès que $n \geq 3$, d'où le résultat.

Chapitre 3

Arithmétique modulaire dans $\mathbb{Z}$

3.1 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définitions - Notations - Premiers résultats

Elles commencent par la récapitulation suivante :

Proposition 1 : Les idéaux de $\mathbb{Z}$ coïncident avec les sous-groupes additifs de $\mathbb{Z}$, et sont du type $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

La preuve, évidente, de cet énoncé, résulte de la division euclidienne dans $\mathbb{Z}$ et est laissée aux soins du lecteur ; si $I = n\mathbb{Z} = (n)$ est un idéal de $\mathbb{Z}$, on note $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}/(n)$ l'anneau des classes résiduelles dans $\mathbb{Z}$ modulo $n\mathbb{Z}$ et on notera $\bar{a}$ l'élément générique de l'anneau $\mathbb{Z}/n\mathbb{Z}$. D'ailleurs on peut énoncer :

Proposition 2 :

(i) $\bar{a}$ génère le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$

(ii) $\bar{a}$ est un élément inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$

(iii) a et n sont premiers entre eux

sont des énoncés équivalents.

Démonstration : $\bar{a}$ génère $(\mathbb{Z}/n\mathbb{Z}, +)$ *si et seulement si* on peut trouver b entier tel que $b\bar{a} = \bar{b}\bar{a} = \bar{1}$ ce qui traduit (*via* l'identité de Bezout) que a et n sont premiers entre eux (notation $a \wedge n = 1$) ; de même pour (ii).

En définitive il y a $\varphi(n)$ éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. On notera, dans tout cet ouvrage, G_n le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Ainsi on peut énoncer :

Proposition 3 : Pour tout $\bar{a} \in G_n$: $\bar{a}^{\varphi(n)} = \bar{1}$ ou : $a^{\varphi(n)} = 1 \pmod{n}$.

Démonstration : $(G_n, \bullet)$ est un groupe possédant $\varphi(n)$ éléments et $\bar{a}$ appartient à G_n ; par application immédiate de la proposition 9 du chapitre **2** on obtient directement $\bar{a}^{\varphi(n)} = 1$. Cela signifie, entr'autres choses, que l'exposant du groupe commutatif G_n divise $\varphi(n)$ et est égal à $\varphi(n)$ *si et seulement si* G_n est cyclique.

En particulier si $\varphi(n) = n - 1$ *ie* si n est premier, on sait que l'anneau $\mathbb{Z}/(n)$ est un corps, d'où :

Corollaire : Si n est un nombre premier, pour tout $a \in \mathbb{Z}$ non multiple de n, $a^{n-1} = 1 \pmod{n}$. En outre, puisque n est premier, G_n est un groupe cyclique.

Selon l'usage, si n est premier, le corps $\mathbb{Z}/n\mathbb{Z}$ est noté $\mathbb{F}_n$ et on dit qu'on a alors affaire au corps premier de Frobénius ; G_n est lui, à ce moment là, égal à $\mathbb{F}_n \backslash \{\bar{0}\} = \mathbb{F}_n^*$.

3.2 Le théorème chinois - Applications

3.2.1 D'abord un lemme

Lemme : Soient p et q deux entiers et $n = pq$ leur produit. Alors les deux énoncés suivants sont équivalents :

(i) $p \wedge q = 1$ *ie* p et q sont premiers entre eux.

(ii) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à l'anneau produit :

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Démonstration : Supposons (i) et soit f l'application de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ définie par :

$$f(\bar{x}) = (\bar{\bar{x}}, \bar{\bar{\bar{x}}})$$

où $\bar{x}$ (*resp.* $\bar{\bar{x}}$, *resp.* $\bar{\bar{\bar{x}}}$) est la classe de x modulo n (*resp.* modulo p *resp.* modulo q).

f est manifestement un morphisme d'anneau, injectif car $\bar{\bar{x}} = \bar{\bar{0}}$ et $\bar{\bar{\bar{x}}} = \bar{\bar{\bar{0}}}$ implique x multiple de pq puisque $p \wedge q = 1$; comme $\mathbb{Z}/(n)$ et $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ ont le même nombre d'éléments f est aussi surjective ; c'est donc un isomorphisme de $\mathbb{Z}/(n)$ dans $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$.

Réciproquement, puisqu'on a affaire à des anneaux isomorphes, les groupes additifs correspondants le sont aussi *a fortiori* ; s'agissant de groupes cycliques, la proposition 8 du chapitre **2** assure que les entiers p et q sont premiers entre eux.

Remarque : L'application f^{-1} est définie par :

$$f^{-1}(\bar{\bar{a}}, \bar{\bar{\bar{b}}}) = \overline{pp'b + qq'a}$$

si p' et q' sont dans $\mathbb{Z}$ des entiers tels que : $pp' + qq' = 1$ (identité de Bezout) ; la vérification, élémentaire, est laissée aux soins du lecteur.

3.2.2 Le théorème chinois

Il s'énonce de la façon suivante :

Proposition 4 : Soient $n_1, n_2, \ldots, n_r$ des nombres entiers et $n = n_1 n_2 \cdots n_r$ leur produit.

(i) $\mathbb{Z}/n\mathbb{Z}$ est un anneau isomorphe à l'anneau produit : $\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$.

(ii) Les entiers n_i $(i = 1, 2, \ldots, r)$ sont deux à deux premiers entre eux,

sont des énoncés équivalents.

Démonstration : La preuve de (ii)$\Longrightarrow$(i) s'effectue en raisonnant par récurrence sur l'entier r ; elle est vraie, d'après le lemme si $r = 2$; écrivons maintenant pour $r \geq 3$: $n = (n_1 n_2 \cdots n_{r-1})n_r$; n_r est premier avec le produit $n_1 n_2 \cdots n_{r-1}$ (puisqu'il est premier avec chaque n_j, $j = 1, 2, \ldots, r-1$). D'après le lemme il s'ensuit que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à l'anneau $\mathbb{Z}/(n_1 n_2 \cdots n_{r-1}) \times \mathbb{Z}/(n_r)$; mais comme $\mathbb{Z}/(n_1 n_2 \cdots n_{r-1})$ est isomorphe à l'anneau produit $\prod_{j=1}^{r-1} \mathbb{Z}/n_j\mathbb{Z}$, l'implication (ii)$\Longrightarrow$(i) en résulte.

Réciproquement si on dispose de (i) il suffit, en se restreignant aux seules structures additives, s'agissant de groupes cycliques, d'appliquer encore une fois la proposition 8 du chapitre **2** ; ainsi $n_i \wedge n_j = 1$ si $i \neq j$, ce qui achève la démonstration.

Plus précisément l'application :

$$\bar{x} \in \mathbb{Z}/n\mathbb{Z} \xrightarrow{f} (\bar{x} \pmod{n_1}, \ldots, \bar{x} \pmod{n_r}) \in \prod_{i=1}^{r} \mathbb{Z}/(n_i)$$

est une isomorphie de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sur l'anneau produit $\prod_{i=1}^{r} \mathbb{Z}/(n_i)$; la vérification, identique à celle effectuée dans le lemme, est facile et laissée aux soins du lecteur.

Alors on peut énoncer :

Proposition 5 : Si f est l'isomorphie précédente, l'application f^{-1} est définie par :

$$f^{-1}(\bar{a}_1 \pmod{n_1}, \ldots, \bar{a}_r \pmod{n_r}) = \overline{\sum_{i=1}^{r} m_i m'_i a_i} \pmod{n}$$

où $m_i = n/n_i$ et $\bar{m'}_i = (\bar{m}_i)^{-1} \pmod{n_i}$.

Démonstration : En effet soit b l'entier défini par :

$$b = \sum_{i=1}^{r} m_i m'_i a_i$$

On peut alors écrire $b \pmod{n_i} = m_i m'_i a_i \pmod{n_i}$ (puisque pour $j \neq i$, m_j est un multiple de n_i) ; et par construction : $m_i m'_i a_i = a_i \pmod{n_i}$; d'où le résultat.

Pratiquement on peut traduire la proposition 5 en disant :

Corollaire : Soient $n_1, n_2, \ldots, n_r$ r nombres entiers deux à deux premiers entre eux, et $a_1, a_2, \ldots, a_r$ des entiers.
Alors il existe un x unique, x compris entre 1 et n où $n = n_1 n_2 \cdots n_r$ tel que :

$$\begin{aligned} x &= a_1 \pmod{n_1} \\ x &= a_2 \pmod{n_2} \\ &\vdots \\ x &= a_r \pmod{n_r} \end{aligned}$$

et x est égal au résidu modulo n de l'entier $\sum_{i=1}^{r} m_i m_i' a_i$

Remarque : Le lemme établi en **3.2.1** prouve que pour $p \wedge q = 1$ on a bien $\varphi(p \cdot q) = \varphi(p)\varphi(q)$; en effet : $(\bar{a}, \bar{\bar{b}})$ est inversible dans l'anneau $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ *si et seulement si* a est inversible dans l'anneau $\mathbb{Z}/(p)$ et $\bar{b}$ inversible dans l'anneau $\mathbb{Z}/(q)$; ainsi il y a $\varphi(p)\varphi(q)$ éléments inversibles dans $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$; cet anneau produit étant isomorphe à l'anneau $\mathbb{Z}/(n)$ avec $n = pq$ on retrouve bien la formule :

$$\varphi(pq) = \varphi(p)\varphi(q)$$

pour $p \wedge q = 1$.

3.3 Retour à l'indicatrice d'Euler

A bien d'égards l'indicatrice d'Euler joue un rôle important en arithmétique modulaire ; ainsi nous indiquons dans cette remarque quelques résultats la concernant.

a. Quelques propriétés de l'indicatrice d'Euler

(i) Pour tout $n \geq 3$, $\varphi(n)$ est un entier pair ; en effet :
si n est impair, si $a \in \{1, 2, \ldots, n-1\}$ est premier avec n, il en est de même de l'entier $n - a$, ce qui prouve bien, dans ce cas, que $\varphi(n)$ est pair.
Si $n = 2m$, et si m est impair, $\varphi(n) = \varphi(2)\varphi(m) = \varphi(m)$ est donc pair ; enfin si m est pair, avec $m = 2^\alpha m'$, et m' impair, on a : $\varphi(2m) = 2^\alpha \varphi(m') = 2\varphi(m)$ est encore pair.

(ii) De la formule de Möbius : $n = \sum_{d|n} \varphi(d)$ on obtient, classiquement, par réciprocité (voir la remarque ci-après) :

$$\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

où μ est la fonction de Möbius *ie* celle définie sur $\mathbb{N}^*$ par :

$$\mu(m) = \begin{cases} 1 \text{ si } m = 1 \\ 0 \text{ si } m \text{ est divisible par un carré} > 1 \\ (-1)^q \text{ si } m \text{ est le produit de } q \text{ facteurs premiers distincts} \end{cases}$$

$\mu(m) = \sum_{\substack{k \wedge m = 1 \\ 1 \leq k \leq m}} e^{\frac{2ik\pi}{m}}$ par application de la formule de réciprocité (voir la remarque) à partir de la suite : $u_n = \sum_{\substack{k \wedge n = 1 \\ 1 \leq k \leq n}} e^{\frac{2ik\pi}{n}}$.

(iii) Pour les curieux on a également :

$$\forall x \in]-1;1[: \sum_{n \geq 0} \frac{\varphi(n) x^n}{1 - x^n} = \frac{x}{(1-x)^2}$$

Remarque : Si μ est la fonction (de Möbius) définie précédemment, on invite le lecteur à prouver que pour toute suite $(u_n)_{n \geq 1}$ de $\mathbb{C}$, si $(v_n)_{n \geq 1}$ est la suite de $\mathbb{C}$ définie par : $v_n = \sum_{t|n} u_t$ alors on a (réciprocité) :

$$u_n = \sum_{t|n} \mu(t) v_{n/t}$$

b. Une inégalité relative à l'indicatrice d'Euler

Notation : On utilisera la notation *log* pour désigner le logarithme népérien.
Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ la décomposition primaire de l'entier n. On a donc :

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \geq n \prod_{\substack{p \text{ premier} \\ p \leq n}} \left(1 - \frac{1}{p}\right)$$

Notons :

$$\Pi_n = \prod_{\substack{p \text{ premier} \\ p \leq n}} \left(1 - \frac{1}{p}\right)$$

comme $\log(1 - 1/p) + 1/p$ est le terme général d'une série qui converge, on peut donc écrire :

$$\log \Pi_n = - \sum_{\substack{p \text{ premier} \\ p \leq n}} 1/p + c_n$$

avec : $\exists \lim_{\infty} c_n$. Or, il est "bien connu" (voir le chapitre **6** paragraphe 12) que l'on peut écrire (c étant une constante) :

$$\sum_{\substack{p \text{ premier} \\ p \leq n}} 1/p = \log(\log x) + c + o(1)$$

et dans ces conditions, il vient, bien naturellement :

$$\log \Pi_n = -\log(\log(n)) + \lambda_n$$

avec : $\exists \lim_{n\to\infty} \lambda_n$ et alors :

$$\Pi_n = \frac{e^{\lambda n}}{\log(n)} \geq \frac{\alpha}{\log(n)} \text{ avec } \alpha > 0$$

Bilan : On peut trouver $\alpha > 0$ tel que :

$$\begin{cases} \varphi(n) \geq \frac{\alpha n}{\log(n)} \\ \forall n \in \mathbb{N}, n \geq 2 \end{cases}$$

En particulier si $\mu \in]0,1[$, on a : $\varphi(n) > n^{1-\mu}$ pour tout entier n assez grand.

Remarque : Mieux : on peut montrer qu'il existe $a > 0$ tel que : $\varphi(n) \geq \frac{an}{\log(\log(n))}$ pour tout $n \geq 3$ (voir le chapitre **6**, paragraphe 12...).

c.

Il existe une généralisation de la fonction φ d'Euler ; elle se décline de la façon suivante : soit r un nombre entier et $n \in \mathbb{N}^*$; on désigne par $\varphi_r(n)$ le nombre de $r-uples$ $(a_1, a_2, \ldots, a_r)$ avec $a_i \in \{1, 2, \ldots, n\}$ tels que : $a_1 \wedge a_2 \wedge \cdots \wedge a_r \wedge n = 1$ *ie* tels que les entiers $a_1, a_2, \ldots, a_r$ et n soient premiers entre eux dans leur ensemble. Bien entendu, pour $r = 1$, $\varphi_1 = \varphi$ est l'indicatrice d'Euler.

On peut démontrer les résultats suivants :

- $\varphi_r(p \cdot q) = \varphi_r(p)\varphi_r(q)$ si $p \wedge q = 1$
- si $n = p_1^{\alpha_1} \cdots p_q^{\alpha_q}$ est la décomposition en facteurs premiers de l'entier n alors on a :

$$\varphi_r(n) = n^r \left(1 - \frac{1}{p_1^r}\right) \cdots \left(1 - \frac{1}{p_q^r}\right)$$

et :

$$\sum_{d|n} \varphi_r(d) = n^r \text{ (formule de Möbius)}$$

Ces résultats s'obtiennent (assez) facilement en raisonnant par récurrence sur l'entier n et proviennent essentiellement du fait que chaque fonction φ_r est, comme l'indicatrice d'Euler φ, une fonction à valeurs entières multiplicative *ie* telle que :

$$p \wedge q = 1 \Rightarrow \varphi_r(pq) = \varphi_r(p)\varphi_r(q)$$

Cependant, la fonction φ, contrairement aux autres φ_r pour $r \geq 2$, possède une signification algébrique très forte, puisqu'elle permet de dénombrer les générateurs de tout groupe cyclique mais aussi de dénombrer tous les éléments inversibles des anneaux $\mathbb{Z}/n\mathbb{Z}$; c'est la raison pour laquelle elle joue un rôle essentiel en arithmétique modulaire.

3.4 Algorithmes d'Euclide - Applications à l'arithmétique modulaire

Commençons par :

Proposition 6 : Soient r_0 et r_1 deux nombres entiers avec $r_0 > r_1$. L'algorithme permettant de déterminer leur pgcd $d = r_0 \wedge r_1$ utilise les divisions euclidiennes successives :

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 \quad 0 \leq r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 \quad 0 \leq r_3 < r_2 \\
&\vdots \\
r_{m-2} &= q_{m-1} r_{m-1} + r_m \quad 0 \leq r_m < r_{m-1} \\
r_{m-1} &= q_m r_m \ (ie\ r_{m+1} = 0)
\end{aligned}$$

et on a : $d = r_m$.
On peut alors écrire pour tout entier $k = 0, 1, \ldots, m$:

$$r_k = a_k r_0 + b_k r_1 \text{ avec } \begin{cases} a_0 = 1 & b_0 = 0 \\ a_1 = 0 & b_1 = 1 \end{cases}$$

$$\begin{aligned}
a_{k+1} &= a_{k-1} - q_k a_k \\
b_{k+1} &= b_{k-1} - q_k b_k
\end{aligned} \qquad \text{et } a_k b_{k+1} - a_{k+1} b_k = (-1)^k$$

Démonstration : La formule $r_k = a_k r_0 + b_k r_1$ est vraie, pour $k = 0$ et $k = 1$. Supposons-là vraie pour $j = 0, 1, \ldots, k$; alors on a :

$$r_{k-1} = q_k r_k + r_{k+1}$$

ce qui impose :

$$r_{k+1} = a_{k-1}r_0 + b_{k-1}r_1 - q_k(a_k r_0 + b_k r_1)$$

d'où :

$$r_{k+1} = (a_{k-1} - q_k r_k)r_0 + ((b_{k-1} - q_k b_k)r_1 \ ie$$
$$r_{k+1} = a_{k+1}r_0 + b_{k+1}r_1$$

La formule est donc valable pour tout $k = 0, 1, \ldots, m$. En outre : $a_0 b_1 - a_1 b_0 = 1$; si on suppose : $a_{k-1}b_k - a_k b_{k-1} = (-1)^{k-1}$ il vient alors :

$$a_k b_{k+1} - a_{k+1}b_k = a_k(b_{k-1} - q_k b_k) - (a_{k-1} - q_k a_k)b_k$$
$$= a_k b_{k-1} - a_{k-1}b_k = (-1)^k$$

la proposition est entièrement démontrée ; sa complexité, si $a, b \in \{1, 2, \ldots, n\}$, n'excèdant pas $c(\log n)^2$.

Corollaire (Algorithme d'Euclide étendu) :
Les notations $r_0, r_1, \ldots, r_m, q_0, q_1, \ldots, q_m$ étant celles de la proposition, si on considère la suite $\bar{b}_0, \bar{b}_1, \ldots, \bar{b}_m$ de $\mathbb{Z}/r_0\mathbb{Z}$ définie par :

$$\bar{b}_0 = \bar{0}, \bar{b}_1 = 1, \text{et } \bar{b}_j = \bar{b}_{j-2} - \bar{q}_{j-1}\bar{b}_{j-1}$$

pour $j = 2, \ldots, m$, alors on peut écrire dans l'anneau $\mathbb{Z}/r_0\mathbb{Z}$:

$$\bar{r}_j = \bar{b}_j \bar{r}_1$$

En particulier si r_0 et r_1 sont premiers entre eux on a :

$$\bar{r}_1 \bar{b}_m = \bar{1}$$

ce qui permet de déterminer l'inverse de $\bar{r}_1$ dans l'anneau $\mathbb{Z}/r_0\mathbb{Z}$.

C'est une application immédiate de la proposition 5, et on utilisera systématiquement ce corollaire pour déterminer algorithmiquement les inverses dans les anneaux quotients de $\mathbb{Z}$.

Proposition 7 (théorème de Lamé) : Soient r_0 et r_1 deux entiers avec $0 < r_1 < r_0$, de pgcd d. Si l'algorithme d'Euclide s'arrête après m pas, alors on a les deux inégalités :

$$r_0 \geq d u_{m+2}, \ r_1 \geq d u_{m+1}$$

où $(u_k)_{k\geq 0}$ est la suite de Fibonacci : $u_0 = 0, u_1 = 1, u_{k+1} = u_k + u_{k-1}$

Démonstration : On va raisonner par récurrence sur l'entier m égal au nombre d'itérations conduisant au pgcd d.

Si $m = 1$: $r_0 \wedge r_1 = r_1$; on a bien $r_1 = du_2$ et :

$$r_0 \geq 2r_1 \geq 2d = du_3$$

($u_2 = 1$ et $u_3 = 2$). Ainsi les inégalités de Lamé sont vraies si $m = 1$; comme $r_0 \wedge r_1 = r_1 \wedge r_2$, le pgcd de r_1 et r_2 s'obtient après $m-1$ pas, d'où, *via* l'hypothèse de récurrence on a :

$$r_1 \geq du_{m+1} \text{ et } r_2 \geq du_m$$

Or : $r_0 \geq r_1 + r_2 \geq d(u_{m+1} + u_m) = du_{m+2}$; la preuve de la proposition 6 est terminée.

Corollaire (coût de l'algorithme) : m étant le nombre d'itérations conduisant au calcul du pgcd on a l'inégalité :

$$m \leq 1 + \frac{3\ln(r_1)}{2\ln(2)}$$

Démonstration : On a : $r_1 \geq u_{m+1}$ et comme on veut montrer que $m - 1 \leq \frac{3\ln(r_1)}{2\ln(2)}$, tout revient à prouver (cela suffira) que $u_{m+1} \geq 2^{\frac{2}{3}(m-1)}$; pour démontrer cette inégalité concernant la suite de Fibonacci, on procède par récurrence sur l'entier m.

C'est vrai pour $m = 0$, et $m = 1$ (sva) ; supposons que cela soit vrai pour u_k pour $k \leq m+1$; alors on a :

$$u_{m+2} = u_{m+1} + u_m \geq 2^{\frac{2}{3}(m-1)} + 2^{\frac{2}{3}(m-2)}$$
$$\text{ce qui entraîne : } u_{m+2} \geq 2^{\frac{2}{3}m}2^{-\frac{2}{3}} + 2^{\frac{2}{3}m}2^{-\frac{4}{3}}$$
$$\text{et fournit : } u_{m+2} \geq 2^{\frac{2}{3}m}\left(2^{-\frac{2}{3}} + 2^{-\frac{4}{3}}\right)$$

et comme $2^{\frac{2}{3}} + 1 \geq 2^{\frac{4}{3}}$ on a : $2^{-\frac{2}{3}} + 2^{-\frac{4}{3}} \geq 1$ ce qui entraîne :

$$u_{m+2} \geq 2^{\frac{2}{3}m}$$

et l'inégalité est démontrée.

Par conséquent cet algorithme a un coût polynomial et de ce fait il est très rapide (voir le chapitre **1**).

3.5 Le corps de Frobénius $\mathbb{F}_p$

C'est par définition $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/(p)$ où p est premier, ce qui revient encore à dire que l'idéal $p\mathbb{Z} = (p)$ de $\mathbb{Z}$ est maximal.

On l'a déjà démontré dans la proposition 15 du chapitre **2**, le groupe $(\mathbb{F}_p^*, \bullet)$ *ie* le groupe multiplicatif du corps $\mathbb{F}_p$ est cyclique ; de ce fait pour tout $\bar{a} \in \mathbb{F}_p^*$: $\bar{a}^{p-1} = 1$ et :

$$X^{p-1} - 1 = \prod_{\bar{a} \in \mathbb{F}_p^*} (X - \bar{a})$$

si bien que dans le corps $\mathbb{F}_p$ le polynôme $X^p - X$ est scindé et à racines simples.

Comme $\mathbb{F}_p$ est de caractéristique p, on a, nous l'avons déjà vu (proposition 16 chapitre **2**) :

$$(\bar{a}+\bar{b})^{p^k} = \bar{a}^{p^k} + \bar{b}^{p^k}$$

pour $\bar{a}, \bar{b} \in \mathbb{F}_p$ et $k \geq 1$ entier.

Bien évidemment puisque $\mathbb{F}_p^*$ est un groupe multiplicatif cyclique, si $\bar{\alpha}$ désigne un générateur de ce groupe, pour tout $\bar{\beta} \in \mathbb{F}_p^*$ il existe un entier a, unique modulo $p-1$ vérifiant :

$$\bar{\beta} = \bar{\alpha}^a$$

a est le logarithme discret de $\bar{\beta}$ en base $\bar{\alpha}$.

En général lorsque l'entier premier p est un "grand" nombre premier, il est "difficile" de déterminer a (nous renvoyons le lecteur au chapitre **7** où sont présentés deux protocoles mathématiques algorithmiques ayant pour but de déterminer a (algorithmes de Shanks et Pohlig)).

Les générateurs du groupe $\mathbb{F}_p^*$, en nombre égal à $\varphi(p-1)$, sont les racines primitives $p-1$-unièmes de l'unité modulo p, autrement dit les racines dans le corps $\mathbb{F}_p$ du polynôme cyclotomique $\Phi_{p-1}(X)$ qui est donc scindé sur ce corps.

3.6 L'anneau $\mathbb{Z}/p^m\mathbb{Z}$ pour p premier et $m \geq 2$

Il joue, comme la suite le montre, un rôle important en arithmétique modulaire ; cela tient essentiellement, en effet, dans l'énoncé suivant :

Proposition 8 : Pour $p \geq 3$ premier le groupe des inversibles de l'anneau $\mathbb{Z}/p^m\mathbb{Z}$ est cyclique.

Démonstration : Désignons par G ce groupe ; $(G, \bullet)$ est commutatif et il possède $\varphi(p^m) = p^{m-1}(p-1)$ éléments. Par application de la proposition 10 (première étape) du chapitre **2**, il suffit de trouver x et y dans G d'ordres respectifs p^{m-1} et $p-1$, car alors on sait que $z = xy$ est d'ordre $(p-1)p^{m-1}$ puisque les deux entiers p^{m-1} et $p-1$ sont premiers entre eux.

1° pas : L'élément $x = \overline{p+1}$ de G est d'ordre p^{m-1}. En effet, on peut écrire :

$$(1+p)^{p^r} = 1 + p^{r+1} \pmod{p^{r+2}}$$

(vérification aisée par récurrence) ; dans ces conditions il vient :

$$x^{p^{m-1}} = \bar{1}$$

Cela montre déjà que l'ordre de x est un diviseur de p^{m-1} ; s'il est du type p^α avec $\alpha \leq m-2$ on a donc :

$$(\overline{1+p})^{p^\alpha} = x^{p^\alpha} = \bar{1} = \overline{1 + p^{\alpha+1} + kp^{\alpha+2}} \text{ avec } k \in \mathbb{Z}$$

ce qui impose : $p^{\alpha+1}(1+kp) = 0 \pmod{p^m}$; comme $\alpha \leq m-2$, cela entraîne $1+kp$ divisible par l'entier p ; comme cela n'est pas possible, l'ordre de $x = \overline{p+1}$ est bien égal à p^{m-1}.

2° pas : Soit a un entier dont la classe modulo p est un générateur du groupe multiplicatif du corps de Frobénius $\mathbb{F}_p$ et soit k l'ordre de $\bar{a}$ dans le groupe des inversibles de l'anneau $\mathbb{Z}/p^m\mathbb{Z}$; on a donc :

$$\bar{a}^k = \bar{1}$$

ou encore :

$$a^k = 1 \pmod{p^m}$$

A fortiori, $a^k = 1 \pmod{p}$ et, de ce fait, k est un multiple de l'entier $p-1$; si k' est l'entier défini par : $k = (p-1)k'$, posons : $y = \bar{a}^{k'}$; par construction $y^{p-1} = \bar{1}$ et ainsi y est d'ordre $p-1$ dans $(G, \bullet)$; le produit $z = xy = (1+p)a^{k'} \pmod{p^m}$ est bien un générateur du groupe G.

Remarque : $k = (p-1)k'$ divise (théorème de Lagrange) l'ordre de G *ie* $p^{m-1}(p-1)$; ainsi k' est du type p^r avec $r \in \{0, 1, \ldots, m-1\}$.

Corollaire : Si p est un nombre premier, $p \geq 3$ et si m est un entier, le groupe des inversibles de l'anneau $\mathbb{Z}/2p^m\mathbb{Z}$ est lui aussi cyclique.

Démonstration : Puisque les entiers 2 et p^m sont premiers entre eux, on dispose de l'isomorphisme :

$$\mathbb{Z}/2p^m\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$$

Ainsi le groupe H des inversibles de l'anneau $\mathbb{Z}/2p^m\mathbb{Z}$ est isomorphe à $G_1 \times G_2$ où G_1 est le groupe $\{1 \pmod 2\}$ et où G_2 est le groupe des inversibles de l'anneau $\mathbb{Z}/p^m\mathbb{Z}$; H est donc bien un groupe cyclique ayant, lui aussi, $p^{m-1}(p-1)$ générateurs.

Remarque importante : L'hypothèse $p \geq 3$ est essentielle car elle sert à établir la relation :

$$(1+p)^{p^\alpha} = 1 + p^{\alpha+1} \pmod{p^{\alpha+2}}$$

qui est fausse si $p = 2$.

La proposition 7 permet de trouver explicitement $\alpha \in G$ tel que : $G = [\alpha]$; si, $m = 2$, $k = (p-1)k'$ divise $p(p-1)$ d'où $k' = 1$ ou $k' = p$.

Par exemple si $p = 11$, dans $(\mathbb{Z}/121\mathbb{Z}, +, \bullet)$ le groupe des inversibles est cyclique et possède 110 éléments ; $a = 2 \pmod{11}$ génère $\mathbb{F}_{11}^*$. Donc, si $2^{10} \neq 1 \pmod{121}$, $\bar{2}$ est d'ordre 110 dans le groupe G et c'est alors un générateur.

Or on a : $2^{10} = 2048 \neq 1 \pmod{121}$; donc le groupe des inversibles de l'anneau $\mathbb{Z}/(121)$ est cyclique et engendré par $\bar{2}$. De même le groupe des inversibles de $\mathbb{Z}/(242)$ est cyclique et : $\mathbb{Z}/(242) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(121)$; on sait que si p' et q' sont tels que : $2p' + 121q' = 1$ l'application :

$$(\bar{a}, \bar{\bar{b}}) \in \mathbb{Z}/(2) \times \mathbb{Z}/(121) \xrightarrow{f} \overline{2p'b + 121q'a} \in \mathbb{Z}/(242)$$

est une isomorphie d'anneau (lemme préliminaire du théorème chinois) ; ici on peut prendre :

$$p' = -60 \quad q' = 1$$

D'où $f(\bar{a},\bar{\bar{b}}) = \overline{121a-120b}$ et $f(\bar{1},\bar{\bar{2}}) = \overline{121-240} = \overline{123}$. Ainsi : 123 modulo 242 génère le groupe cyclique des inversibles de l'anneau $\mathbb{Z}/(242)$ qui possède 40 générateurs exactement.

Comme : $p^{m-1}(p-1)$ est un "grand" entier lorsque p (ou m) sont "grands", le problème du logarithme discret dans le groupe des inversibles de $\mathbb{Z}/(p^m)$ est certainement autant difficile que dans $\mathbb{F}_p$; cette observation peut être utile pour une utilisation cryptographique ultérieure.

Proposition 9 : Le groupe des inversibles de $\mathbb{Z}/(2^n\mathbb{Z})$ n'est pas cyclique dès que $n \geq 3$; il l'est si $n = 1$ ou 2.

En effet si H est ce groupe, $card\ H = 2^{n-1}$; or si a est impair :

$$a^{2^{m-2}} = 1 \pmod{2^m} \text{ si } m \geq 3$$

En effet écrivons : $a = 2b+1$; $a^2 = (1+2b)^2 = 1 \pmod 8$; c'est donc vrai si $m = 3$; puis avec $(1+2b)^{2^m} = 1+2^{m+2}k$ on peut écrire : $(1+2b)^{2^{m+1}} = 1+2^{m+2}k)^2 = 1+2^{m+3}k'$, $k, k' \in \mathbb{N}$; la preuve est terminée.

Remarque : Si $\bar{a} \in H$, son ordre est inférieur ou égal à 2^{n-2} ; cependant $\bar{\bar{5}}$ est d'ordre 2^{n-2} dans H ; en effet, par récurrence sur m on peut écrire :

$$5^{2^{m-3}} = 1+2^{m-1} \pmod{2^m} \qquad (**)$$

C'est vrai si $m = 3$ car $5 = 1+4$; sinon en supposant (**) on peut écrire :
$5^{2^{m-2}} = (1+2^{m-1}+k2^m)^2 = 1+2^m+k'2^{m+1}$ ce qui prouve (**) pour tout m entier, $m \geq 3$; ainsi $\bar{\bar{5}}$ n'est pas d'ordre 2^{n-3} ; il est donc d'ordre 2^{n-2} dans $(H, \bullet)$. Des résultats précédents on déduit :

3.7 Condition nécessaire et suffisante pour que $(G_n, \bullet)$ soit cyclique

Elle s'énonce à l'aide de la proposition suivante :

Proposition 10 : Si n est un entier et si G_n est le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ le groupe G_n est cyclique *si et seulement si* n appartient à l'ensemble suivant :

$$\{2, 4, p^\alpha, 2p^\alpha, p \text{ premier}, p \geq 3 \text{ et } \alpha \geq 1 \text{ entier}\}$$

Démonstration : Si $n \in \{2, 4, p^\alpha, 2p^\alpha, p \text{ premier}, p \geq 3 \text{ et } \alpha \geq 1 \text{ entier}\}$ les propositions précédentes montrent que le groupe G_n des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est cyclique.

Réciproquement écrivons par décomposition primaire dans $\mathbb{N}$:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

Le théorème chinois montre que le groupe G_n est isomorphe au groupe multiplicatif produit :

$$H_1 \times H_2 \times \cdots H_r$$

où H_i est le groupe des inversibles de l'anneau $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

Pour chaque entier i, le cardinal de H_i est égal à $p_i^{\alpha_i - 1}(p_i - 1)$; or on a vu (proposition 8) du chapitre **2**, qu'un produit de groupes est cyclique *si et seulement si* chaque groupe facteur et cyclique et si de plus les ordres de ces groupes sont des entiers deux à deux premiers entre eux.

Par conséquent si tous les p_i sont supérieurs à 3, il ne peut y en avoir qu'un, et à ce moment là, n est du type p^α avec $p \geq 3$; si $p_1 = 2$, on doit avoir $\alpha_1 \leq 2$; ou bien il n'y a plus de p_i, auquel cas $n = 2$ ou 4, sinon il ne peut y avoir dans décomposition primaire de n qu'un entier p premier, $p \geq 3$ et alors n est du type $2p^\alpha$. Cela achève la preuve.

Remarque : si $p \geq 3$ est premier, l'application :

$$(\bar{a}, \bar{\bar{b}}) \in \mathbb{Z}/(2) \times \mathbb{Z}/(p^\alpha) \longrightarrow \overline{p^\alpha a - (p^\alpha - 1)b} \in \mathbb{Z}/(2p^\alpha)$$

est, *via* le lemme chinois, une isomorphie d'anneaux ; de ce fait si $\bar{\bar{b}}$ est un générateur du groupe G_{p^α} des inversibles de l'anneau $(\mathbb{Z}/(p^\alpha), +, \bullet)$, $\overline{p^\alpha - (p^\alpha - 1)b}$ est un générateur du groupe cyclique G_{2p^α}.

Si nous prenons, autre exemple, $p = 5$ et $\alpha = 3$, nous pouvons déterminer un générateur de G_{250} en procédant comme nous l'indiquons ci-après. On va, tout simplement, appliquer la proposition 8 ; en effet on a vu que si a est un générateur du groupe $(\mathbb{F}_5^*, \bullet)$ l'ordre k de $\bar{a}$ dans G_{125} est du type :

$$k = 4k'$$

et alors : $6a^{k'}$ modulo 125 est un générateur du groupe des inversibles de l'anneau $(\mathbb{Z}/(125), +, \bullet)$. En outre l'entier $k = 4k'$ doit diviser (Lagrange...) l'ordre du groupe G_{125} qui est égal à $\varphi(125) = 100$; de ce fait k' est un diviseur de 25 et alors $k' \in \{1, 5, 25\}$.

2 modulo 5 engendre le groupe $(\mathbb{F}_5^*, \bullet)$; on peut donc essayer avec $a = 2$ et calculer $2^4, 2^{20}$ *modulo* 125 ; s'ils sont tous deux distincts de 1, on a alors $k = 100$, *ie* $k' = 25$.

Or : $2^4 = 16$ et $2^{20} = 76$ modulo 125.

Bilan : $k' = 25$ et $6 \cdot 2^{25}$ modulo 125 est un générateur du groupe cyclique G_{125}, d'où puisque : $6 \cdot 2^{25} = 92$ modulo 125, $\overline{92}$ engendre G_{125}.

Par application de ce qui a été dit précédemment, le groupe cyclique G_{250} est engendré par 227 (mod 250) et possède 100 éléments.

3.8 Application du théorème de Fermat : le quotient de Fermat et la formule d'Eisenstein

Définition : Soit p un nombre premier et a un entier, $a \notin p\mathbb{Z}$; on appelle *quotient de Fermat* de a en base p l'entier $\frac{a^{p-1}-1}{p}$ modulo p *ie* le résidu modulo p de l'entier

$\frac{a^{p-1}-1}{p}$ noté $Q_p(a)$ (par abus de notation, on confondra pour m et p entiers l'élément $\bar{m}$ de $\mathbb{Z}/p\mathbb{Z}$ avec le résidu modulo p de l'entier m c'est-à-dire le reste de la division euclidienne de m par p).

Par exemple : $Q_3(2) = 1, Q_3(5) = 2\ldots$; cet exemple montre d'ailleurs que $Q_p(a)$ n'est pas intrinsèquement lié à la classe de a modulo p.

Proposition 11 : Si a et b ne sont pas dans $p\mathbb{Z}$ on a :

$$Q_p(a \cdot b) = Q_p(a) + Q_p(b)$$

En outre $Q_p(p-1) = 1$ et $Q_p(p+1) = -1$ si $p \geq 3$.

Démonstration : Posons : $m = \frac{a^{p-1}-1}{p}$ et $m' = \frac{b^{p-1}-1}{p}$. Ainsi on a :

$$(ab)^{p-1} = (pm+1)(pm'+1) = pm + pm' + p^2mm' + 1$$

d'où :

$$\frac{(ab)^{p-1}-1}{p} = m + m' + pmm'$$

ce qui prouve bien la relation énoncée.

Soit $\varepsilon \in \{-1, 1\}$ et p premier, $p \geq 3$; on peut écrire :

$$(p+\varepsilon)^{p-1} = 1 + p\varepsilon(p-1) + Mp^2$$

avec M entier ; d'où :

$$\frac{(p+\varepsilon)^{p-1}-1}{p} = -\varepsilon + M'p$$

avec $M' \in \mathbb{Z}$ ce qui laisse donc :

$$Q_p(p+\varepsilon) = -\varepsilon$$

et achève la preuve de la proposition.

Remarques :

1. On constate que sur $\mathbb{Z}/p\mathbb{Z}$, la fonction Q_p agit comme un logarithme.
2. Si p est un nombre premier, existe-t-il des a tels que $Q_p(a)$ *ie* tels que $a^{p-1} - 1 = 0 \pmod{p^2}$? Le lecteur vérifiera que, si $p = 3511$, on a bien $Q_p(2) = 0$ c'est-à-dire :

$$2^{3510} = 1 \pmod{3511^2}$$

en utilisant l'algorithme d'exponentiation rapide.

Proposition 12 : Soit p un nombre premier, $p \geq 3$ avec $p = 2q+1$; si $\bar{r}$ est l'élément de $\mathbb{F}_p$ défini par :

$$\bar{r} = (\bar{2})^{-1}\left[\sum_{k=0}^{q-1}\left((\overline{2k+1})\right)^{-1} - \sum_{k=1}^{q}(\bar{2}\bar{k})^{-1}\right]$$

on peut alors écrire :

$$Q_p(2) = \bar{r} \qquad \text{(Théorème d'Eisenstein)}$$

ou encore schématiquement dans $\mathbb{F}_p^*$:

$$Q_p(2) = \frac{1}{\bar{2}}\left(\bar{1} - \frac{1}{\bar{2}} + \frac{1}{\bar{3}} - \frac{1}{\bar{4}} + \cdots + \frac{(-1)}{\overline{p-1}}\right)$$

Démonstration : On écrit : $2^{(p-1)} - 1 = \sum_{k=1}^{p-1} \frac{(p-1)(p-2)\cdots(p-k)}{k!} = mp + Mp^2$ avec m et M entiers, ce qui fixe : $Q_p(2) = \bar{m}$ dans le corps $\mathbb{F}_p$.

Soit $P_k(X) = \frac{(X-1)(X-2)\cdots(X-k)}{k!} = \sum_{i=0}^{k} a_{i,k}X^i$, alors on peut écrire :

$$2^{p-1} - 1 = \sum_{k=1}^{p-1} P_k(p) = \sum_{k=1}^{p-1} a_{0,k} + X\sum_{k=1}^{p-1} a_{1,k} + \left(\sum_{k=2}^{p-1} a_{2,k}\right)X^2 + \cdots + a_{p-1,p-1}X^{p-1}$$

Or on a :

$$\sum_{k=1}^{p-1} a_{0,k} = \sum_{k=1}^{p-1}(-1)^k = 0$$

ce qui fournit alors :

$$2^{p-1} - 1 = p\sum_{k=1}^{p-1} a_{1,k} + p^2\sum_{k=2}^{p-1} a_{2,k} + \cdots + a_{p-1,p-1}p^{p-1}$$

Les $a_{i,k}$ sont du type : $a_{i,k} = \frac{b_{i,k}}{k!}$ avec $b_{i,k}$ entier ; cela entraîne donc :

$$\frac{2^{p-1}-1}{p} = \sum_{k=1}^{p-1} a_{1,k} + p\sum_{k=2}^{p-1}\frac{b_{2,k}}{k!} + \cdots + \frac{p^{p-1}}{(p-1)!}$$

et peut encore s'écrire :

$$m = \frac{2^{p-1}-1}{p} = \sum_{k=1}^{p-1} a_{1,k} + p\frac{A}{(p-1)!}$$

où A est un entier.

Pour chaque entier k on a : $a_{1,k} = P_k'(0)$ et comme : $\frac{P_k'(X)}{P_k(X)} = \sum_{i=1}^{k} \frac{1}{X-i}$ on obtient : $P_k'(0) = (-1)^{k+1}(1 + \frac{1}{2} + \cdots + \frac{1}{k})$ ce qui entraîne :

$$\sum_{k=1}^{p-1} a_{1,k} = -\left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2q}\right)$$

si $p = 2q + 1$. En définitive il vient :

$$m = \frac{2^{p-1} - 1}{p} = -\frac{1}{2}\left(1 + \frac{1}{2} + \cdots + \frac{1}{q}\right) + \frac{pA}{(p-1)!} = \frac{-u}{2(q!)} + \frac{pA}{(p-1)!}$$

avec u entier ; cela peut encore s'écrire : $m = \frac{\alpha}{\beta} + \frac{\alpha'}{\beta'}$ où β, β' sont des entiers premiers avec p. Comme $m\beta\beta' = \alpha\beta' + \alpha'\beta$, dans le corps $\mathbb{F}_p$ on obtient :

$$\bar{m}\bar{\beta}\bar{\beta}' = \bar{\alpha}\bar{\beta}' + \bar{\alpha'}\bar{\beta}$$

ce qui fournit :

$$\bar{m} = \bar{\alpha}(\bar{\beta})^{-1} + \bar{\alpha'}(\bar{\beta}')^{-1}$$

ou $\bar{\alpha'} = \bar{p}\bar{A} = \bar{0}$; par conséquent il reste :

$$\bar{m} = -\bar{u}(\bar{2})^{-1}(\overline{q!})^{-1}$$

ce qui peut encore s'écrire :

$$\bar{m} = -(\bar{2})^{-1}\sum_{i=1}^{q}(\bar{i})^{-1}$$

Dans $\mathbb{F}_p[X]$ on a :

$$X^{p-1} - \bar{1} = \prod_{i=1}^{p-1}(X - \bar{i}) = \prod_{i=1}^{p-1}\left(X - (\bar{i})^{-1}\right)$$

ce qui impose avec des notations évidentes (et faciles à comprendre) :

$$\sum_{i=1}^{2q} \frac{1}{\bar{i}} = 0$$

ainsi :

$$\sum_{k=0}^{q-1} \frac{1}{\overline{2k+1}} + \sum_{k=1}^{q} \frac{1}{\overline{2k}} = 0$$

ce qui nous permet d'écrire :

$$\sum_{k=0}^{q-1} \frac{1}{\overline{2k+1}} - \sum_{k=1}^{q} \frac{1}{\overline{2k}} = -\bar{2}\sum_{k=1}^{q} \frac{1}{\overline{2k}} = -\sum_{k=1}^{q} \frac{1}{\bar{k}} = \bar{2}\bar{m}$$

Il en résulte donc bien l'identité :

$$Q_p(2) = \bar{m} = \frac{1}{2}\left(\bar{1} - \frac{1}{\bar{2}} + \frac{1}{\bar{3}} - \frac{1}{\bar{4}} + \cdots + \frac{1}{\overline{p-2}} - \frac{1}{\overline{p-1}}\right)$$

ce qui démontre entièrement la formule d'Eisenstein.

3.9 Le test de primalité de Miller-Rabin - Sa fiabilité

a.

Il est la conséquence de la proposition suivante :

Proposition 13 : Soit n premier impair $n > 9$ tel que : $n-1 = 2^k m$ avec m impair.
Pour $a \in \{1, 2, \ldots, n-1\}$ ou bien : $a^m = 1 \pmod n$, ou bien il existe
$i \in \{0, 1, \ldots, k-1\}$ tel que : $a^{2^i m} = -1 \pmod n$.

Démonstration : Remarquons que si n est premier, pour tout
$a \in \{1, 2, \ldots, n-1\}$, $a^{n-1} = 1 \pmod n$ (petit théorème de Fermat) et posons : $\bar{x}_i = \bar{a}^{2^i m}$ pour $i = 0, 1, 2, \ldots, k$; on a, par construction :

$$\bar{a}^{n-1} = \bar{x}_k = \bar{1} = (\bar{x}_{k-1})^2, \text{d'où } \bar{x}_{k-1} = 1 \text{ ou bien } \bar{x}_{k-1} = -1$$

Si $\bar{x}_{k-1} = -1$ c'est fini ; sinon on recommence jusqu'à épuisement du stock ; si on a obtenu $\bar{x}_k = \bar{x}_{k-1} = \cdots = \bar{x}_0$ on a bien alors : $\bar{a}^m = \bar{1}$, ce qui prouve entièrement la proposition 9.

D'où l'idée suivante :

Soit n impair, $n > 9$ avec $n = 1 + 2^k m$, et m impair ; on veut "estimer" la primalité de l'entier n ; on a vu que, si n est premier, la suite $\bar{x}_i$, $i = 0, 1, \ldots k$, associée à tout $a \in \{1, 2, \ldots, n-1\}$, vérifie les conclusions de la proposition 9 ci-dessus ; d'où l'idée de "tester" plusieurs fois, en faisant varier a de manière aléatoire dans $\{1, 2, \ldots, n-1\}$, les valeurs $\bar{x}_i$ prises par la suite des $\bar{a}^{2^i m}$ pour $i = 0, 1, 2, \ldots, k-1$. Si pour un certain $a \in \{1, 2, \ldots, n-1\}$, $a^{2^i m} \neq -1$ modulo n pour tout $i = 0, 1, \ldots, k-1$, et si de plus $a^m \neq 1$ modulo n, l'entier n n'est pas un nombre premier.

Ainsi on peut schématiser une itération du test de Miller-Rabin à l'aide du tableau suivant pour $n = 1 + 2^k m$ avec m impair et $n > 9$.

1. Choisir a arbitraire, $a \in \{1, 2, \ldots, n-1\}$
2. Calculer $b = a^m \pmod n$
3. Si $b = 1$ écrire "n est premier" et fin.
4. Si $b \neq 1$ alors pour i allant de 0 jusqu'à $k-1$ faire :
   - Si $b = -1$ écrire "n est premier" et fin.
   - Sinon remplacer b par b^2 modulo n.
5. Ecrire "n n'est pas premier". Fin.

b. La fiabilité de ce protocole itéré p fois

b.1.

Supposons d'abord que ce test soit effectué une seule fois ; il peut afficher "n premier" sans que l'entier n le soit ; par contre s'il affiche "n n'est pas premier" la réponse fournie

est exacte (on a donc affaire à un algorithme probabiliste, voir chapitre **1**). A l'issue d'une seule épreuve (testant la primalité de $n = 1 + 2^k m$), désignons par E_1 et E_2 les deux événements suivants :

E_1 : l'entier n choisi n'est pas premier

E_2 : le test répond "n est premier"

La fiabilité de ce test, autrement dit la probabilité d'erreur, est le réel : $pr(E_1|E_2)$ *ie* la probabilité que E_1 soit vrai alors que l'on sait E_2 ; or on peut écrire :

$$pr(E_1|E_2) = \frac{pr(E_1 \cap E_2)}{pr(E_2)} = \frac{pr(E_2|E_1)pr(E_1)}{pr(E_2)}$$

or : $pr(E_2) = pr(E_2|E_1)pr(E_1)+pr(E_2|non\ E_1)pr(non\ E_1)$. Si l'on sait que n est premier le test répond à coup sûr "n est premier" ; cela veut dire que : $pr(E_2|non\ E_1) = 1$ et de ce fait : $pr(E_2) = pr(E_2|E_1)pr(E_1) + pr(non\ E_1)$ ce qui entraîne :

$$pr(E_1|E_2) = \frac{pr(E_2|E_1)pr(E_1)}{pr(E_2|E_1)pr(E_1) + pr(non\ E_1)}$$

Comme on se préoccupe dans ce test de la primalité des "grands" nombres entiers, il faut savoir estimer la probabilité de l'événement E_1 *ie* du cas où n n'est pas premier ; entre 1 et n, d'après le théorème de raréfaction, on sait que le nombre d'entiers premiers est équivalent à $\frac{n}{\log(n)}$ et comme bien entendu on ne s'intéresse qu'aux entiers impairs, on a :

$$pr(E_1) \underset{\infty}{\sim} 1 - \frac{2}{\log(n)} \quad (\log \equiv \ln)$$

Reste, et c'est le point délicat de l'étude, pour connaître la validité de ce test, à "estimer" le réel : $pr(E_2|E_1)$ *ie* la probabilité que le test réponde "n est premier" alors que l'on sait qu'il ne l'est pas. Cela revient à comptabiliser les témoins (de Miller) a, qui, dans le cas où n n'est pas premier, satisfont à la condition : $a^m = 1 \pmod n$ ou à l'une des conditions $a^{2^i m} = -1 \pmod n$ pour $i = 0, 1, 2, \cdots, k-1$. Ce décompte fait l'objet de l'énoncé suivant :

Proposition 14 : Soit n un nombre entier non premier, impair, strictement supérieur à 9, s'écrivant : $n = 1 + 2^k m$ avec m impair. Soit Ω l'ensemble des entiers $a \in \{1, 2, \ldots, n-1\}$ tels que :
– ou bien : $a^m = 1 \pmod n$
– ou bien : il existe $i \in \{0, 1, \ldots, k-1\}$ avec $a^{2^i m} = -1 \pmod n$
Alors on a l'inégalité :

$$card(\Omega) \leq \frac{1}{4}\varphi(n)$$

ce qui implique : $pr(E_2|E_1) \leq \frac{1}{4}$

Démonstration : φ est bien évidemment l'indicatrice d'Euler.

1° pas : Supposons d'abord $n = p^\alpha$ avec $\alpha \geq 2$ et p premier. Notons alors $A = \{\bar{a} \in \mathbb{Z}/(p^\alpha) : \bar{a}^m = 1\}$, $B_j = \{\bar{a} : \bar{a}^{2^j m} = -1\}$ pour $j = 0, 1, \ldots, k-1$ et $B = \cup_{0 \leq j \leq k-1} B_j$; on veut calculer $card\ \Omega$ où $\Omega = A \cup B$. A ce propos, nous rappelons le résultat démontré au chapitre **2** dans la proposition 8-bis :

Soit $(G, \bullet)$ un groupe cyclique ayant q éléments, d'élément neutre e, alors :

(i) Si $q' \in \mathbb{N}^*$: $card(\{x \in G : x^{q'} = e\}) = q \wedge q'$ (pgcd de q et q')

(ii) Si $b \neq e$, il existe $x \in G : x^{q'} = b$ *si et seulement si* $b^{\frac{q}{q \wedge q'}} = e$ et en outre : $card(\{x \in G : x^{q'} = b\}) = q \wedge q'$.

Ceci étant acquis, désignons ici, par G, le groupe des inversibles de l'anneau quotient $\mathbb{Z}/(p^\alpha)$; on sait que ce groupe est cyclique (proposition 8 du chapitre **3**). Ici, $n = p^\alpha = 1 + 2^k m$ et $q = \varphi(n) = p^{\alpha-1}(p-1)$; posons alors : $p - 1 = 2^u v$ avec v entier impair.

a. Pour ce qui concerne le cardinal de A, on peut écrire :

$$card\ A = (p^{\alpha-1}(p-1)) \wedge m = (2^u v p^{\alpha-1}) \wedge m$$

Or l'entier p n'est pas facteur premier de l'entier m ; il en est de même pour 2 ; ainsi :

$$card\ A = v \wedge m$$

Or v divise $p - 1$, donc v divise $p^\alpha - 1$, et de ce fait v divise m puisque $v \wedge m = 1$. Finalement, on obtient :

$$card\ A = v$$

b. Notons bien que les B_j sont deux à deux disjoints, et que $B \cap A$ est vide.

Pour que l'on puisse trouver des $\bar{x}$ avec (j étant fixé) $\bar{x}^{2^j m} = -1$ il faut, d'après ce qui a été rappelé, que si d est le pgcd des entiers $2^j m$ et $2^u v p^{\alpha-1}$ on ait $(-1)^{\frac{\varphi(n)}{d}} = 1$. Or nous pouvons écrire :

$$d = (2^j m) \wedge (2^u v p^{\alpha-1}) = v 2^{\min(u,j)}$$

d'où :

$$\frac{\varphi(n)}{d} = 2^{u - \min(u,j)} p^{\alpha-1}$$

qui est pair pour tout entier j vérifiant $j < u$, sinon il est impair.

Dans ces conditions l'ensemble B_j est non-vide *si et seulement si* $j \leq \min(k-1, u-1)$; comme $k \geq u$ on peut donc écrire :

$$\forall j \leq u - 1,\ card\ B_j = 2^j v$$

et alors : $card\ B = v \sum_{0 \leq j \leq u-1} 2^j = (2^u - 1)v$, ce qui, en définitive, dans ce premier pas, fournit :

$$card\ \Omega = v + (2^u - 1)v = 2^u v = p - 1 \quad ie :$$

$$\boxed{card\ \Omega = \frac{\varphi(n)}{p^{\alpha-1}}}$$

2° pas : Supposons désormais que la décomposition primaire de l'entier n soit du type : $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ avec ici $r \geq 2$, puisque le cas où $r = 1$ vient d'être étudié.

On sait qu'alors l'application :

$$\bar{a}(n) \in \mathbb{Z}/n\mathbb{Z} \longrightarrow (\bar{a}(p_1^{\alpha_1}), \ldots, \bar{a}(p_r^{\alpha_r})) \in \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

est un isomorphisme d'anneaux ; on sait aussi que si G_i désigne le groupe des inversibles de chaque anneau $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, G_i est un groupe cyclique (proposition 8 de ce chapitre...).

Pour i fixé, $i \in \{1, 2, \ldots, r\}$ notons :

$$A_i = \{\bar{a} : \bar{a}^m = \bar{1} \pmod{p_i^{\alpha_i}}\}$$

et $A = A_1 \times A_2 \times \cdots \times A_r$. Puis $B_{i,j} = \{\bar{a} : \bar{a}^{2^j m} = -1 \pmod{p_i^{\alpha_i}}\}$; $B_j = B_{1,j} \times \cdots \times B_{r,j}$ et $B = \bigcup_{1 \leq j \leq r} B_j$; enfin $\Omega = A \cup B$; A et B sont disjoints, ainsi d'ailleurs que les B_j.

Nous supposons que pour tout $i = 1, 2, \ldots, r$ on a :

$$p_i - 1 = 2^{u_i} v_i \text{ avec } v_i \text{ impair}$$

D'après ce qui a été fait dans le premier pas on a : $card\ A = \prod_{1 \leq i \leq r} m \wedge v_i$ et :

$$card\ B_{i,j} = \begin{cases} 0 \text{ si } j \geq u_i \\ 2^j m \wedge v_i \text{ si } j \leq u_i - 1 \end{cases}$$

Soit s l'entier défini par :

$$s = \min\{u_i, i = 1, 2, \ldots, r\}$$

on a donc B_j vide si $j \geq s$ et pour $j \leq s-1$ on peut écrire : $card\ B_j = 2^{rj} \prod_{1 \leq i \leq r} (m \wedge v_i)$ et ainsi :

$$card\ B = \sum_{0 \leq j \leq s-1} card\ B_j$$

Désignons par λ le produit $\lambda = \prod_{1 \leq i \leq r} (m \wedge v_i)$; alors on peut écrire :

$$card\ \Omega = \lambda[1 + (1 + 2^r + \cdots + 2^{r(s-1)})] = \lambda\left(1 + \frac{2^{rs} - 1}{2^r - 1}\right)$$

Or on a :

$$1 + (1 + 2^r + \cdots + 2^{r(s-1)}) \leq 2^{r(s-1)+1}$$

et il s'ensuit qu'alors on dispose de l'inégalité :

$$card\ \Omega \leq (2^{r(s-1)+1})\lambda$$

Pour ce qui est de l'entier $\varphi(n)$, on peut aussi écrire :

$$\varphi(n) = p_1^{\alpha_1-1} \cdots p_r^{\alpha_r-1} 2^{u_1+\cdots+u_r} v_1 \cdot v_2 \cdots v_r$$

Pour alléger les notations, posons alors : $U = u_1 + \cdots + u_r$ et $V = v_1 \cdots v_r$. Ecrivons pour chaque entier $i = 1, 2, \ldots r$: $d_i = m \wedge v_i$, si bien que l'on a :

$$\begin{cases} m = d_i m_i \\ v_i = d_i v_i' \end{cases} \quad \text{avec } m_i \wedge v_i' = 1$$

dans ces conditions :

$$\lambda = \frac{V}{V'} = d_1 d_2 \cdots d_r$$

où $V' = v_1' v_2' \cdots v_r'$ et avec $\varphi(n) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_r^{\alpha_r} 2^U V$ on a :

$$\frac{\varphi(n)}{card\ \Omega} \geq \left(\prod_{i=1}^{r} p_i^{\alpha_i-1} \right) \left(V' 2^{U-r(s-1)-1} \right)$$

Par construction, chaque entier u_i et supérieur ou égal à s ; cela entraîne :
$u_1 + u_2 + \cdots + u_r \geq rs$ et alors on dispose de l'inégalité :

$$\frac{\varphi(n)}{card\ \Omega} \geq 2^{r-1} V' \prod_{i=1}^{r} p_i^{\alpha_i-1}$$

(puisque : $U - r(s-1) - 1 \geq rs - rs + r - 1$)

Si donc r est un entier au moins égal à 3 on obtient :

$$\frac{\varphi(n)}{card\ \Omega} \geq 4 \ ie \ : \ card\ \Omega \leq \frac{1}{4}\varphi(n)$$

comme annoncé dans la proposition 10.

3° (et dernier) pas : Si $r = 1$ on a, on l'a vu dans la première étape : $card\ \Omega = \frac{\varphi(n)}{p^{\alpha-1}}$ et si $p \geq 5$, comme $\alpha \geq 2$ on retrouve bien l'inégalité $card\ \Omega \leq \frac{1}{4}\varphi(n)$.

Toujours dans le cas où $r = 1$ et $p = 3$, comme $n > 9$ (c'est ici que cela sert) on a $\alpha \geq 3$ et $3^{\alpha-1} > 4$ et l'inégalité souhaitée est toujours valable. Enfin, reste le cas où $r = 2$, *ie* le cas où : $n = p_1^{\alpha_1} p_2^{\alpha_2}$. Comme : $\frac{\varphi(n)}{card\ \Omega} \geq 2V' p_1^{\alpha_1-1} p_2^{\alpha_2-1}$ si l'un des deux entiers α_1 ou α_2 est supérieur ou égal à 2, et puisque $p_1 \geq 3$ et $p_2 \geq 3$, l'inégalité : $card\ \Omega \leq \frac{1}{4}\varphi(n)$ est encore vraie et elle le reste si $V' \geq 2$ quels que soient $\alpha_1 \geq 1$ et $\alpha_2 \geq 1$.

Pour finir si $\alpha_1 = \alpha_2 = 1$ et $V' = 1$ il reste :

$$n = p_1 p_2 = 2^k m + 1$$
$$\varphi(n) = (p_1 - 1)(p_2 - 1) = 2^{u_1+u_2} v_1 v_2$$

puisque $V' = 1$, v_1' et v_2' sont égaux à 1 et alors v_1 et v_2 divisent l'entier m ; or $2^k m = 2^{u_1+u_2} v_1 v_2 + 2^{u_1} v_1 + 2^{u_2} v_2$; de ce fait v_1 divise v_2 et réciproquement ; donc : $v_1 = v_2$.

Si $u_1 > u_2$, $u_1+u_2 > 2s$ et alors $U-2(s-1)-1 \geq 2$ et encore on a bien : $\frac{\varphi(n)}{card\ \Omega} \geq 4$; comme le cas $u_1 = u_2$ est impossible car alors $p_1 = p_2$, la démonstration est terminée.

Application : La proposition 14 entraîne alors les résultats suivants ; en pratique on veut tester la primalité d'un grand entier n ; à cet effet on utilisera p fois le test de Miller-Rabin si bien que si l'on désigne à l'issue de ces p tests par A,B et C les événements suivants :

A : l'entier n est décomposable

B : le test répond à chaque itération : "n est premier"

C : au cours d'une itération le test a répondu : "n est composé"

Si la réponse C est fournie, on est certain que l'entier n n'est pas un nombre premier. Sinon :

$$pr(A|B) = \frac{pr(B|A)pr(A)}{pr(B|A)pr(A) + pr(non\ A)}$$

D'après ce qui vient d'être prouvé : $pr(B|A) \leq \frac{1}{4^p} = 2^{-2p}$ et compte tenu du théorème de raréfaction des nombres premiers (voir chapitre **6**) :

$$pr(A) \underset{\infty}{\sim} 1 - \frac{2}{\log(n)}$$

En définitive il reste "approximativement" :

$$pr(A|B) \leq \frac{2^{-2p}\left(1 - \frac{2}{\log(n)}\right)}{2^{-2p}\left(1 - \frac{2}{\log(n)}\right) + \frac{2}{\log(n)}}$$

ie

$$pr(A|B) \leq \frac{\log(n) - 2}{(\log(n) - 2) + 2^{2p+1}}$$

et si on prend "n voisin de 2^{256}", ce réel est voisin de : $\frac{175}{175+2^{2p+1}}$ qui est "suffisamment petit" pour p compris entre 50 et 100 ; autrement dit, avec une très grande précision (mais ce n'est pas une preuve) on peut affirmer que le test de Miller-Rabin est fiable (on rappelle log ≡ ln). Par exemple, on montre en quelques secondes que l'entier $n = 10^{1000} + 453$ est premier avec un risque d'erreur très faible, et que tous les $10^{1000} + m$ avec $0 \leq m \leq 452$ sont composés.

c. En conclusion

Soit n un entier impair s'écrivant $n = 1 + 2^k m$ avec m impair. S'il existe un entier $a \in \{1, 2, \ldots, n-1\}$ tel que : $a^m \neq 1$ modulo n et $a^{2^i m} \neq 1$ modulo n pour $i = 0, 1, 2, \ldots, k-1$, l'entier n est non premier (proposition 13) et un tel entier a est appelé *témoin de Miller* pour l'entier n.

En particulier, si n est un entier impair composé (*ie* non premier) tous ses diviseurs sont des témoins de Miller pour cet entier ; en effet si $a \in \{2, \ldots, n-1\}$ divise n avec $ab = n$, et si on suppose qu'il existe $q \in \{2^i m, 0 \leq i \leq k-1\}$ avec $a^q = \pm 1$ modulo n, a est inversible modulo n et alors $b = 0$ modulo n ce qui est faux ; par conséquent a est bien un témoin de Miller de l'entier n.

Mais, et c'est beaucoup mieux, la proposition 14 nous affirme que si un entier impair est composé, les $3/4$ au moins des entiers compris entre 1 et $n-1$ sont des témoins de Miller relativement à n.

9 est le plus petit entier impair composé admettant 2 pour témoin de Miller et bien souvent 2 est un témoin de Miller ; dans le cas où $n = 9$, il y a exactement 6 témoins de Miller, à savoir : $2, 3, 4, 5, 6, 7$ (vérification laissée aux soins du lecteur).

Pour les nombres de Carmichael *ie* les nombres impairs non premiers n vérifiant $a^{n-1} = 1$ modulo n pour tout a premier avec n, 2 est souvent un témoin de Miller, puisque $2^k m$ est un multiple strict de l'ordre de 2 modulo n ; par exemple, si l'on prend $n = 561$ (qui est le plus petit entier de Carmichael) on vérifie sans peine que 2 est un témoin de Miller associé à l'entier n.

Chapitre 4

Arithmétique modulaire dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps fini

4.1 Introduction

Nous avons, à la proposition 14 du chapitre **2**, décrit un protocole "universel" de construction d'un corps ; il suffit de disposer d'un couple (A, I) où $(A, +, \bullet)$ est un anneau commutatif et I un idéal maximal de A ; alors $\mathbb{K} = A/I$ est naturellement muni d'une structure de corps ; avec $A = \mathbb{Z}$ et $I = p\mathbb{Z}$, où p est un nombre premier, on a déjà construit les $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (corps de Frobénius).

D'où l'idée, dans $\mathbb{F}_p[X]$ et plus généralement dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps, de déterminer des éléments irréductibles puisqu'on sait que, si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est *principal*, ce qui signifie que tout idéal de $\mathbb{K}[X]$ est du type $(P) = P(X)\mathbb{K}[X] = \{P(X)Q(X), Q \in \mathbb{K}[X]\}$.

4.2 Un théorème d'isomorphisme

Il s'énonce ainsi :

Proposition 1 : Soient $\mathbb{K}$ un corps quelconque, R et S deux polynômes unitaires de même degré n ; on suppose qu'il existe $A \in \mathbb{K}[X]$, de degré au plus égal à $n-1$, tel que :

(i) $1, A(X), A^2(X) \pmod{S(X)}, \ldots, (A(X))^{n-1} \pmod{S(X)}$ est une base du $\mathbb{K}$-espace vectoriel des polynômes de $\mathbb{K}[X]$ de degré $\leq n-1$.

(ii) $R(A(X))$ est un multiple de $S(X)$

Alors l'application

$$u : \bar{P} \in \mathbb{K}[X]/(R) \longrightarrow \overline{\overline{P(A(X))}} \in \mathbb{K}[X]/(S)$$

est une isomorphie d'anneaux et même une isomorphie de $\mathbb{K}$-ev.

Démonstration : D'abord on s'assure de la cohérence de u ; soit donc P et Q de $\mathbb{K}[X]$ avec $P = Q \pmod R$ *ie* : $P(X) = Q(X) + B(X)R(X)$; alors :

$$P(A(X)) = Q(A(X)) + B(A(X))R(A(X))$$

et de ce fait :

$$P(A(X)) = Q(A(X)) \pmod{S(X)}$$

Ensuite il est aisé de vérifier que u est un morphisme d'anneaux et même un morphisme de $\mathbb{K}$-ev *ie* une application linéaire.

Si $\bar{P} \in \text{Ker } u$, écrivons :

$$\overline{P(X)} = a_0 + a_1\bar{X} + \cdots + a_{n-1}\bar{X}^{n-1}$$

de ce fait on a :

$$u(\bar{P}) = a_0 + a_1\overline{\overline{A(X)}} + \cdots + a_{n-1}(\overline{\overline{A(X)}})^{n-1} = 0 \pmod{S(X)}$$

cela revient à dire que : $\sum_{i=0}^{n-1} a_i(A(X))^i$ est égal à 0 modulo S et *via* l'hypothèse (i) il s'ensuit que tous les a_i sont nuls *ie* $\bar{P} = 0$; u est donc injectif.

Comme de plus, u est linéaire, et que les $\mathbb{K}$-ev, $\mathbb{K}[X]/(R)$ et $\mathbb{K}[X]/(S)$ sont de même dimension n (pour cause de division euclidienne...) u est une isomorphie de $\mathbb{K}$-ev ; la preuve est complète.

Corollaire 1 : Si $\mathbb{K}$ est un corps quelconque et si R et S sont deux polynômes irréductibles vérifiant les hypothèses de la proposition 1, les corps : $\mathbb{K}[X]/(R)$ et $\mathbb{K}[X]/(S)$ sont isomorphes.

Remarque : Les hypothèses (ii) et (i) sont essentielles. En effet prenons $\mathbb{K} = \mathbb{Q}$, $R(X) = X^2 + 1$ et $S(X) = X^2 + 2$.

R et S sont premiers dans $\mathbb{Q}[X]$; (ii) n'est pas satisfaite car $\sqrt{2} \notin \mathbb{Q}$; nous allons montrer qu'alors les corps : $\mathbb{Q}[X]/(X^2+1)$ et $\mathbb{Q}[X]/(X^2+2)$ ne sont pas isomorphes ; en effet supposons qu'il existe $f : \mathbb{Q}[X]/(X^2+1) \longrightarrow \mathbb{Q}[X]/(X^2+2)$ et que f soit un isomorphisme de corps ; on a donc : $f(i) = \alpha + i\sqrt{2}\beta$ et $(f(i))^2 = f(i^2) = f(-1) = -1 = (\alpha + i\beta\sqrt{2})^2$ avec α et β rationnels ; ainsi : $\begin{cases} \alpha\beta = 0 \\ \alpha^2 - 2\beta^2 = -1 \end{cases}$ ce qui est impossible puisque $\sqrt{2} \notin \mathbb{Q}$.

Néanmoins les $\mathbb{Q}$-ev : $\mathbb{Q}[X]/(X^2+1)$ et $\mathbb{Q}[X]/(X^2+2)$ sont isomorphes à $\mathbb{Q}^2$. Cependant on a :

Corollaire 2 : Soit p un nombre premier et $\mathbb{K}$ le corps de Frobénius $\mathbb{F}_p$; si R et S sont deux polynômes irréductibles de $\mathbb{F}_p[X]$ de même degré n, les corps : $\mathbb{F}_p[X]/(R)$ et : $\mathbb{F}_p[X]/(S)$ sont isomorphes et possèdent tous deux p^n éléments.

Démonstration : Ce corollaire 2, comme la suite va le prouver, est fondamental. Notons : $\mathbb{K}' = \mathbb{F}_p[X]/(R)$ et $\mathbb{K}'' = \mathbb{F}_p[X]/(S)$; puisque R et S sont irréductibles $\mathbb{K}'$ et $\mathbb{K}''$ sont des corps.

L'élément générique de $\mathbb{K}'$ est du type :

$$\overline{\sum_{0\leq i\leq n-1} a_i X^i}$$

ie du type : $a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1}$ où $a_i \in \mathbb{F}_p$ et où $\omega = \bar{X}$; par conséquent :

$$card\ \mathbb{K}' = card\ \mathbb{K}'' = p^n$$

Dans le corps $\mathbb{K}'$, on a $R(\omega) = 0$ et puisque R est irréductible, R est, dans $\mathbb{F}_p[X]$, le polynôme minimal de ω.

Précisons un peu : Il existe donc, dans $\mathbb{F}_p[X]$ des polynômes s'annulant en ω ; ces polynômes constituent un idéal monogène auquel R appartient ; mais comme R est premier dans $\mathbb{F}_p[X]$ cet idéal est engendré par le polynôme R. Puisque $\mathbb{K}'$ est un corps disposant de p^n éléments, le polynôme $X^{p^n} - X$, de $\mathbb{F}_p[X]$, est scindé sur $\mathbb{K}'$; cela signifie que, dans $\mathbb{F}_p[X]$, R divise : $X^{p^n} - X$.

R appartient aussi à $\mathbb{K}''[X]$ tout comme $X^{p^n} - X$; soit donc β une racine de $R(X)$ dans $\mathbb{K}''[X]$ ($X^{p^n} - X$ est aussi scindé dans $\mathbb{K}''[X]$...) ; R est aussi le polynôme minimal de β sur $\mathbb{F}_p[X]$; comme $deg\ R = n$, si $a_0, a_1, \ldots, a_{n-1}$ sont dans $\mathbb{F}_p$ et si :
$a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}$ est nul dans $\mathbb{K}''$ cela impose :

$$a_0 = a_1 = \cdots = a_{n-1} = 0 \qquad (**)$$

Par construction, il existe $A(X) \in \mathbb{F}_p[X]$, de degré $\leq n-1$, tel que :

$$\beta = A(X) \pmod{S} = \overline{\overline{A(X)}} \text{ et ainsi : } R(A(X)) = 0 \pmod{S(X)}$$

ie (ii) ; enfin l'hypothèse (i) est spécifiée par (**). De ce fait $\mathbb{K}'$ et $\mathbb{K}''$ sont des corps isomorphes.

4.3 Un théorème fondamental

Commençons d'abord par un lemme.

Lemme : Si $\mathbb{K}$ est un corps fini, il existe p premier et $n \in \mathbb{N}^*$ tel que : $card\ \mathbb{K} = p^n$

Démonstration : Soit p la caractéristique de $\mathbb{K}$; puisque $\mathbb{K}$ est un corps fini, p est un nombre premier ; ceci étant dit les applications :

$$(x, y) \in \mathbb{K} \times \mathbb{K} \longrightarrow x + y \in \mathbb{K}$$
$$(\bar{a}, x) \in \mathbb{F}_p \times \mathbb{K} \longrightarrow ax \in \mathbb{K}$$

confèrent à $\mathbb{K}$, comme on le vérifie aisément, une structure de $\mathbb{F}_p$ espace vectoriel ; si $n = dim_{\mathbb{F}_p}(\mathbb{K})$, $\mathbb{K}$ est isomorphe en tant que $\mathbb{F}_p$-ev à $\mathbb{F}_p^n$ et de ce fait il possède p^n éléments, d'où le lemme.

Nous avons ensuite besoin du résultat suivant :

Proposition 2 : Soit $\mathbb{K}$ un corps fini de caractéristique p ; si on note encore $\mathbb{F}_p$ le sous-corps de $\mathbb{K}$ défini par : $\{0, 1, 2, \ldots, p-1\}$ où 1 est l'élément neutre de la multiplication dans $\mathbb{K}$, une condition nécessaire et suffisante pour que $A(X) \in \mathbb{K}[X]$ appartienne à $\mathbb{F}_p[X]$ est que :

$$A(X^p) = (A(X))^p$$

dans $\mathbb{K}[X]$.

Démonstration : Soit $A(X) = a_0 + a_1X + \cdots + a_kX^k$ un élément de $\mathbb{K}[X]$; puisque $\mathbb{K}$ est de caractéristique p, on a, dans $\mathbb{K}[X]$: $(A(X))^p = a_0^p + a_1^pX^p + \cdots + a_k^pX^{kp}$ et $(A(X))^p = A(X^p)$ équivaut à : $a_i^p = a_i$ pour tout $i = 0, 1, \ldots, k$.

Si $a \in \mathbb{F}_p, a^p = a$ et ainsi pour $A(X) \in \mathbb{F}_p[X]$ on a bien : $A(X^p) = (A(X))^p$.

Réciproquement si $(A(X))^p = A(X^p)$ pour chaque i, a_i est racine du polynôme $X^p - X$ qui est, on le sait, scindé sur $\mathbb{F}_p$; d'où $a_i \in \mathbb{F}_p$ et la preuve est complète ; ceci étant acquis alors on peut énoncer :

Proposition 3 : Si $\mathbb{K}$ et $\mathbb{K}'$ sont deux corps finis ayant le même nombre d'éléments, ils sont isomorphes en tant que corps.

Démonstration : Soit p^n (p premier, $n \in \mathbb{N}^*$) le nombre d'éléments communs à $\mathbb{K}$ et $\mathbb{K}'$.

1° pas : Désignons par α un générateur du groupe cyclique $(\mathbb{K}^*, \bullet)$ et soit $R(X)$ le polynôme de $\mathbb{K}[X]$ tel que :

$$R(X) = (X-\alpha)(X-\alpha^p)\cdots\left(X-\alpha^{p^{n-1}}\right) = \prod_{i=0}^{n-1}\left(X-\alpha^{p^i}\right)$$

on a :

$$(R(X))^p = (X-\alpha)^p(X-\alpha^p)^p\cdots\left(X-\alpha^{p^{n-1}}\right)^p = \prod_{i=0}^{n-1}\left(X-\alpha^{p^i}\right)^p$$

Comme : $\left(X-\alpha^{p^i}\right)^p = X^p - \alpha^{p^{i+1}}$ il vient aussitôt (puisque $\alpha^{p^n} = \alpha$) $(R(X))^p = R(X^p)$ ce qui prouve que $R(X)$ appartient à $\mathbb{F}_p[X]$.

En outre le polynôme minimal sur $\mathbb{F}_p[X]$ de α est R ; en effet si $Q \in \mathbb{F}_p[X]$ annule α, comme : $Q(X^p) = (Q(X))^p$, on a : $Q(\alpha^{p^i}) = 0$ pour $i = 0, 1, 2, \ldots, n-1$, d'où l'assertion et R est irréductible sur $\mathbb{F}_p[X]$. (Remarquons au passage que α est une racine primitive (p^n-1)-ième de 1 dans $\mathbb{K}$; à ce titre α est racine du polynôme cyclotomique $\Phi_{p^n-1}(X)$).

Ceci étant dit, tout élément de $\mathbb{K}$ peut donc s'écrire de manière unique sous la forme : $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ avec $a_i \in \mathbb{F}_p$; considérons alors l'application f de $\mathbb{K}$ dans $\mathbb{F}_p[X]/(R)$ définie par :

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \xrightarrow{f} \overline{a_0 + a_1X + \cdots + a_{n-1}X^{n-1}}$$

f est une isomorphie du corps $\mathbb{K}$ dans le corps modulaire $\mathbb{F}_p[X]/(R)$; la vérification, très facile, étant laissée aux soins du lecteur.

2° pas : De la même façon on démontre que le corps $\mathbb{K}'$ est isomorphe à un corps modulaire du type $\mathbb{F}_p[X]/(S)$ où S est un polynôme de $\mathbb{F}_p[X]$, irréductible et de degré n. Le corollaire 2 de la proposition 1 montre alors que les deux corps $\mathbb{K}$ et $\mathbb{K}'$ sont isomorphes.

4.4 Le corps à p^r éléments (p premier, et $r \geq 1$)

Nous allons établir que si p est premier et si $r \in \mathbb{N}^*$ il existe toujours un corps ayant p^r éléments ; pour cela nous avons besoin des polynômes cyclotomiques comme l'énoncé suivant le stipule.

Proposition 4 : Soit $\mathbb{K}$ un corps fini ayant q éléments et n un entier naturel premier avec q *ie* : $q \wedge n = 1$.
$\bar{q}$ est donc un élément du groupe G_n des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ et si r est l'ordre de $\bar{q}$ dans G_n le polynôme $\Phi_n(X)$ de $\mathbb{K}[X]$ se décompose en produit de polynômes unitaires, irréductibles, tous différents et de degré égal à r.

Démonstration : C'est un résultat essentiel de ce chapitre.

1° pas : Le polynôme $\Phi_n(X)$ de $\mathbb{K}[X]$ n'admet aucun facteur carré. En effet, si on suppose que $\Phi_n(X)$ est divisible par P^2 où $P \in \mathbb{K}[X]$, *a fortiori*, on a :

$$X^n - 1 = P^2 Q \text{ dans } \mathbb{K}[X]$$

Par dérivation polynomiale (dans $\mathbb{K}[X]$) il vient :

$$nX^{n-1} = 2PP'Q + P^2Q'$$

d'où :

$$n \cdot 1 = X(nX^{n-1}) - n(X^n - 1) = PR$$

avec $R \in \mathbb{K}[X]$. Comme $q \wedge n = 1$, n n'est pas un multiple de la caractéristique du corps $\mathbb{K}$; ainsi $n \cdot 1 = PR$ est distinct de 0, mais ceci est impossible puisque le degré de P est au moins égal à 1 ; en définitive tous les facteurs premiers de $\Phi_n(X)$, dans $\mathbb{K}[X]$, sont simples.

2° pas : Soit donc P un facteur premier unitaire de $\Phi_n(X)$ dans $\mathbb{K}[X]$, et m le degré de P ; le quotient modulaire $\mathbb{K}' = \mathbb{K}[X]/(P)$ est un sur-corps de $\mathbb{K}$ et il possède, puisque P est supposé de degré m, q^m éléments.

Par suite, quel que soit $x \neq 0$, x de $\mathbb{K}'$, on a : $x^{q^m-1} = 1$; cela vaut, en particulier, si $\alpha = \bar{X} \pmod P$; comme $P(\alpha) = 0$, *a fortiori* on a : $\Phi_n(\alpha) = 0$; α est donc dans $\mathbb{K}'$ une racine primitive n-ième de 1 (proposition 19 du chapitre **2**) ; il s'ensuit que l'entier $q^m - 1$ est un multiple de l'entier n, ce qui entraîne :

$$\bar{q}^m = \bar{1} \pmod n$$

d'où l'inégalité $m \geq r$.

3° pas : Puisque $q^r - 1$ est un multiple de l'entier n on peut écrire : $\alpha^{q^r-1} = 1$ ce qui entraîne $(\alpha^i)^{q^r} = \alpha^i$ pour tout entier naturel i ; mais alors le polynôme $X^{q^r} - X$ de $\mathbb{K}[X]$ admet tous les éléments de $\mathbb{K}'$ pour racine ; on a donc $q^m \leq q^r$ ce qui impose l'inégalité : $m \leq r$.

Bilan : Si les hypothèses de la proposition 4 sont supposées réalisées alors le polynôme cyclotomique $\Phi_n(X)$ de $\mathbb{K}[X]$ est décomposable en produit de facteurs premiers unitaires simples et tous de degré r où r est l'ordre de $\bar{q}$ dans le groupe G_n des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. D'où un corollaire fort important :

Proposition 5 : Soient p un nombre premier et $r \geq 1$ un entier. Alors il existe toujours un corps $\mathbb{K}$ ayant p^r éléments et tous les autres corps ayant p^r éléments sont isomorphes au précédent. C'est en ce sens qu'on parle du corps à p^r éléments ; en outre dans $\mathbb{K}[X]$ on a : $X^{p^r} - X = \prod_{\lambda \in \mathbb{K}} (X - \lambda)$.

Démonstration : Posons $n = p^r - 1$; dans $\mathbb{Z}/n\mathbb{Z}$ l'entier p est inversible et même $(\bar{p})^r = \bar{1}$; $\bar{p}$ est d'ordre r dans G_n ; en effet si r' est l'ordre de $\bar{p}$ on a : $r \geq r'$ et comme $p^{r'} - 1$ est multiple de n, $p^{r'} \geq p^r$, ce qui impose $r' \geq r$; en définitive $r = r'$.

Dans $\mathbb{F}_p[X]$ le polynôme $\Phi_n(X)$ est décomposable en un produit de facteurs premiers simples tous de degré r ; si P est l'un d'entre eux, $\mathbb{K} = \mathbb{F}_p[X]/(P)$ est un corps et il possède p^r éléments et il est bien clair, puisque pour tout x de $\mathbb{K}$, $x^{p^r} = x$, que dans $\mathbb{K}[X]$ on peut écrire : $X^{p^r} - X = \prod_{\lambda \in \mathbb{K}} (X - \lambda)$.

Remarque : Si $\alpha = \bar{X} \pmod{P}$ $P(\alpha) = 0$, donc $\Phi_n(\alpha) = 0$ et alors dans $\mathbb{K}$, α est une racine primitive n-ième de 1 (proposition 19 du chapitre **2**) c'est-à-dire, ici, un générateur du groupe multiplicatif du corps $\mathbb{K}$.

Etude d'un exemple : Sur $\mathbb{F}_2[X]$, le polynôme : $X^8 + X^7 + X^3 + X^2 + 1$ est un polynôme irréductible et c'est un facteur premier du polynôme $\Phi_{255}(X)$ (la vérification est laissée aux soins du lecteur) ; dans ces conditions le quotient modulaire : $\mathbb{K} = \mathbb{F}_2[X]/(P)$ où : $P = X^8 + X^7 + X^3 + X^2 + 1$, et où : (P) est l'idéal (maximal) de $\mathbb{F}_2[X]$ engendré par P, est un corps ayant $2^8 = 256$ éléments ; si on pose $\bar{X} = \alpha$, α est racine primitive 255 de l'unité dans ce corps dont l'élément générique est :

$$b_0 + b_1\alpha + \cdots + b_7\alpha^7 \text{ avec } b_i \in \{0, 1\}$$

Convenons de noter $(b_0, b_1, \ldots, b_7)$ cet élément. Si $b' = (b'_0, b'_1, \ldots, b'_7) \in \mathbb{K}$, $b + b' = (b_0 + b'_0, \ldots, b_7 + b'_7)$, l'addition s'effectuant "bit à bit" ; par contre la multiplication bb' s'effectue en tenant compte du modulus *ie* de P.

Un calcul facile, laissé aux soins du lecteur, montre qu'alors on a :

$$bb' = (b''_0, b''_1, \ldots, b''_7)$$

où :

$$\left(\sum_{i=0}^{7} b_i X^i\right)\left(\sum_{i=0}^{7} b'_i X^i\right) = \sum_{i=0}^{7} b''_i X^i \pmod{(X^8 + X^7 + X^3 + X^2 + 1)}$$

Comme on peut le constater, sur cet exemple, ce n'est pas l'addition dans $\mathbb{K}$ qui crée du désordre mais c'est, bien entendu, la multiplication qui crée "doublement" du désordre... ; nous y reviendrons en conclusion de ce chapitre.

Des résultats précédents, on déduit :

Proposition 6 : Soit $\mathbb{K}$ un corps ayant q éléments et n un nombre entier premier avec q ; le polynôme cyclotomique $\Phi_n(X)$ de $\mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$ *si et seulement si* l'ordre de $\bar{q}$ dans le groupe G_n des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est maximal *ie* égal à $\varphi(n)$; dans ce cas G_n est cyclique.
Il ne peut en être ainsi que si n appartient à l'ensemble $\{2, 4, p^\alpha, 2p^\alpha, p \text{ premier}, p \geq 3 \text{ et } \alpha \geq 1 \text{ entier}\}$.

Cela résulte de l'ensemble des résultats établis à la proposition 8 du chapitre **2**, ainsi qu'à la proposition 10 du chapitre **3** auxquels le lecteur est prié de se reporter. Par exemple si $n = 9$ et $q = 5$, $\bar{5}$ appartient ici à G_9 et on a modulo 9 : $5^2 = 7$; $5^3 = -1; 5^4 = -5; 5^5 = 2$ et $5^6 = 1$. Ainsi l'ordre de $\bar{5}$ dans G_9 est égal à 6 ; le polynôme cyclotomique $\Phi_9(X) = X^6 + X^3 + 1$ irréductible dans l'anneau $\mathbb{F}_5[X]$, $\mathbb{F}_5$ étant le corps de Frobénius $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ des classes résiduelles dans $\mathbb{Z}$ modulo 5.

De la même manière le groupe G_{18} des inversibles de l'anneau $\mathbb{Z}/18\mathbb{Z}$ est cyclique ; avec $q = 11$ on constate aisément (laissé aux soins du lecteur) que $\bar{q}$ est d'ordre 6 dans G_{18}, *ie* est un générateur du groupe cyclique G_{18} ; il s'ensuit que le polynôme cyclotomique :

$$\Phi_{18}(X) = X^6 - X^3 + 1$$

est irréductible dans $\mathbb{F}_{11}[X]$.

Enfin et pour terminer avec cette liste d'exemples prenons l'exemple suivant :
$n = 54 = 2 \cdot 3^3$ et $q = 5$; on trouve que $\bar{5}$ est d'ordre $18 = \varphi(54)$ dans G_{54} ; alors le polynôme :

$$\Phi_{54}(X) = X^{18} - X^9 + 1$$

est irréductible dans $\mathbb{F}_5[X]$.

Remarques :

1. A la lumière de ces exemples, nous invitons le lecteur à montrer que si p est un nombre premier et si k est un entier quelconque on a :

$$\Phi_{p^k}(X) = \Phi_p\left(X^{p^{k-1}}\right) = 1 + X^{p^{k-1}} + X^{2p^{k-1}} + \cdots + X^{(p-1)p^{k-1}}$$

2. On rappelle que si n est impair on a aussi $\Phi_{2n}(X) = \Phi_n(-X)$ (proposition 20 du chapitre **2**).

4.5 Sous-corps d'un corps à p^n éléments

Leur étude est résumée par :

Proposition 7 : Soit $\mathbb{K}$ un corps ayant p^n éléments alors :

(i) si $\mathbb{K}'$ est un sous-corps de $\mathbb{K}$, $card\ \mathbb{K}' = p^r$ avec r divisant n.

(ii) si r divise n il existe un sous-corps de $\mathbb{K}$ et un seul ayant p^r éléments.

Démonstration : Pour (i) on observe que $\mathbb{K}$ est un $\mathbb{K}'$ espace vectoriel ; comme la caractéristique de $\mathbb{K}'$ est égale à p, $card\ \mathbb{K}' = p^r$ et si $s = \dim_{\mathbb{K}'} \mathbb{K}$, $\mathbb{K}$ est isomorphe (en tant que $\mathbb{K}'$ espace vectoriel) à $\mathbb{K}'^s$, d'où :

$$p^n = p^{rs} \text{ et } r \text{ divise } n$$

Réciproquement, soit, r entier, r divisant n, avec : $n = rs$. On peut alors écrire :

$$p^n - 1 = p^{rs} - 1 = (p^r)^s - 1 = (p^r - 1)m$$

avec $m \in \mathbb{N}$; ainsi :

$$X^{p^n} - X = X\left(X^{(p^r-1)m} - 1\right) = X\left(X^{p^r-1} - 1\right)Q(X) = (X^{p^r} - X)Q(X)$$

où $Q(X) \in \mathbb{K}[X]$; comme $X^{p^n} - X$ est scindé sur $\mathbb{K}$ et à racines simples, il en est de même du polynôme $X^{p^r} - X$; soit $\mathbb{K}' = \{x \in \mathbb{K} : x^{p^r} = x\}$. $\mathbb{K}'$ est un corps et il possède p^r éléments, et c'est l'unique sous-corps de $\mathbb{K}$ ayant p^r éléments.

En effet : soient x, y dans $\mathbb{K}'$; puisque $(x+y)^{p^r} = x^{p^r} + y^{p^r}$ on a bien : $(x+y)^{p^r} = x+y$ et $x + y \in \mathbb{K}'$; de même : $(xy)^{p^r} = x^{p^r} y^{p^r} = xy$ montre que $xy \in \mathbb{K}'$.

Enfin : si $x \neq 0$ est dans $\mathbb{K}'$, on a : $x^{p^r-1} = 1$ ce qui prouve $(x^{-1})^{p^r-1} = \left(\frac{1}{x}\right)^{p^r-1} = 1$ *ie* $\frac{1}{x} \in \mathbb{K}'$; $\mathbb{K}'$ est donc bien un corps et il est unique puisqu'il est constitué par l'ensemble des racines dans $\mathbb{K}$ du polynôme $X^{p^r} - X$.

4.6 Conclusion

Un corps fini à p^n éléments, avec $n \geq 2$, est un ensemble algébriquement "très riche" obtenu, qu'on le veuille ou non, comme quotient modulaire d'un anneau $\mathbb{F}_p[X]$ (p premier) par un idéal du type (P) où $P(X)$ est un polynôme irréductible de $\mathbb{F}_p[X]$; c'est l'ensemble des racines d'un polynôme du type : $X^q - X$ où q est le cardinal du corps. L'addition dans $\mathbb{K} = \mathbb{F}_p[X]/(P)$ se ramène à n additions dans le corps de Frobénius $\mathbb{F}_p$ si n est le degré de $P(X)$; par contre, la multiplication dans le corps $\mathbb{K}$ "ajoute" au "désordre" de la réduction modulo $P(X)$ dans $\mathbb{F}_p[X]$, le "désordre" de la réduction modulo p dans $\mathbb{Z}$.

Ainsi, les calculs arithmétiques élémentaires dans $\mathbb{K}$ n'ayant aucun ordre prévisible, ils sont, de ce fait, susceptibles de favoriser la création de mécanismes mathématiques

de secret si utiles en cryptologie comme le lecteur pourra le constater dans la suite de cet ouvrage.

Pour ce qui concerne la division dans $\mathbb{K} = \mathbb{F}_p[X]/(P)$ on pourra utiliser la proposition suivante et plus précisément son corollaire :

Proposition 8 : Soient P_0 et P_1 deux polynômes sur un corps $\mathbb{K}$ quelconque et :

$$\begin{aligned} P_0 &= P_1Q_1 + P_2 \\ P_1 &= P_2Q_2 + P_3 \quad \text{avec : } P_{i+1} = 0 \text{ ou } deg\ P_{i+1} < deg\ P_i \\ &\vdots \\ P_{k-1} &= P_kQ_k + P_{k+1} \end{aligned}$$

le schéma des divisions euclidiennes successives effectuées jusqu'à l'obtention d'un reste nul. Alors on peut écrire :

$$P_k = A_kP_0 + B_kP_1 \text{ avec : } \begin{cases} A_0 = 1, B_0 = 0 \\ \\ A_1 = 0, B_1 = 1 \end{cases} \text{ et :}$$

$$A_{k+1} = A_{k-1} - Q_kA_k, B_{k+1} = B_{k-1} - Q_kB_k$$

En outre : $A_kB_{k+1} - A_{k+1}B_k = (-1)^k$ pour $k = 0, 1, 2, \ldots, m$ $(P_{m+1} = 0)$.

La démonstration est en tous points identique à celle de la proposition 6 du chapitre **3** ; il s'ensuit que l'on peut alors énoncer :

Corollaire : Les notations étant celles de la proposition 8, considérons la suite de $\mathbb{K}[X]/(P_0)$ définie par :

$$\bar{B}_0 = \bar{0}, \bar{B}_1 = \bar{1}, \text{et } \bar{B}_j = \bar{B}_{j-2} - \bar{Q}_{j-1}\bar{B}_{j-1} \text{ pour } j = 2, 3, ..., m$$

Alors dans l'anneau $\mathbb{K}[X]/(P_0)$ on a :

$$\bar{P}_j = \bar{B}_j\bar{P}_1$$

et si, en particulier, P_0 et P_1 sont premiers entre eux :

$$\bar{P}_1 \times \bar{B}_m = \bar{a} \text{ où } a \text{ est dans } \mathbb{K}^*$$

où B_m est le "dernier" polynôme obtenu *ie* celui correspondant au dernier reste non nul. Si P_0 est un polynôme irréductible cet algorithme permet de déterminer $(\bar{A})^{-1})$ pour tout $\bar{A}$ non nul du corps $\mathbb{K}[X]/(P_0)$.

Remarque importante : Cependant comme $\mathbb{K}$ est toujours un corps fini et, disons-le, toujours un $\mathbb{F}_p$, le corps $\mathbb{K}' = \mathbb{K}[X]/(P_0)$ (lorsque P_0 est irréductible) est tel que $\mathbb{K}'\backslash\{0\}$ est cyclique ; si α est un générateur du groupe multiplicatif $(\mathbb{K}'^*, \bullet)$ et si m est le nombre d'éléments de $\mathbb{K}'$, α est une racine primitive $m-1$-ième de 1 et à ce moment

là l'inverse dans $\mathbb{K}'$ de α^i est α^{m-1-i} ; il n'est donc nullement besoin d'avoir recours à la version polynomiale de l'algorithme d'Euclide pour diviser dans un corps fini du type $\mathbb{K}[X]/(P_0)$, encore faut-il avoir établi un correspondance entre les α^i et les $\bar{A}$ modulo (P_0) *ie* avoir résolu le problème du logarithme discret ce qui n'est pas évident.

En pratique, nous l'avons dit, $\mathbb{K} = \mathbb{F}_p$; si n est l'entier défini par :

$$n = p^r - 1$$

dans $\mathbb{Z}/(n)$ on a : $\bar{p}^r = \bar{1}$ et $\bar{p}$ est d'ordre r ; dans ces conditions on sait (proposition 4) que tous les facteurs premiers de $\Phi_n(X)$ dans $\mathbb{F}_p[X]$ sont de degré r ; ainsi le corps $\mathbb{K}' = \mathbb{F}_p[X]/(P_0)$, si P_0 est l'un de ces facteurs premiers, est "le corps" standard ayant $m = p^r$ éléments et en outre : $\alpha = \bar{X}$ est une racine primitive $(p^r - 1)$-ième de l'unité dans $\mathbb{K}'$ *ie* un générateur du groupe $(\mathbb{K}'^*, \bullet)$ ce qui permet, comme nous venons de le souligner, d'effectuer (simplement ?) des multiplications ou des divisions dans $\mathbb{K}'$; pour les additions, ou bien on effectuera les calculs modulo P_0 par divisions euclidiennes, ou bien on déterminera la fonction h, définie modulo $p^r - 1$ par : $1 + \alpha^i = \alpha^{h(i)}$ ce qui permettra de calculer simplement une somme du type : $\alpha^i + \alpha^j$... (voir aussi la remarque à la fin du paragraphe **7.7**, du chapitre **7**...).

Chapitre 5

Résidus quadratiques - Loi de réciprocité

5.1 Les carrés dans un corps fini

$\mathbb{K}$ désigne un corps fini (ce pourra être un $\mathbb{F}_p$, avec p premier) de caractéristique $p \geq 3$; on sait qu'alors le nombre d'éléments de $\mathbb{K}$ est un entier q du type $q = p^m$ (m est la dimension de $\mathbb{K}$ regardé comme $\mathbb{F}_p$ espace vectoriel).

Un élément x non nul de $\mathbb{K}$ est dit *carré* dans $\mathbb{K}$, s'il existe y non nul tel que $x = y^2$; alors on peut énoncer :

Proposition 1 : Soit $\mathbb{K}$ un corps fini de caractéristique impaire ayant q éléments ; parmi les $q-1$ éléments de $\mathbb{K}^*$, $\frac{q-1}{2}$ exactement sont des carrés et $a \in \mathbb{K}^*$ est un carré *si et seulement si* :

$$a^{\frac{q-1}{2}} = 1$$

En particulier -1 est un carré *si et seulement si* $q = 1 \pmod 4$.

Démonstration : Soit $f : x \in (\mathbb{K}^*; \times) \longrightarrow x^2 \in (\mathbb{K}^*, \times)$; f est manifestement un morphisme de groupe dont le noyau est l'ensemble des x tels que :

$$x^2 = 1 \quad ie \quad (x-1)(x+1) = 0$$

c'est-à-dire *si et seulement si* $x \in \{-1, 1\}$; comme $-1 \neq 1$, l'image $f(\mathbb{K}^2)$ est un sous-groupe de $\mathbb{K}^*$ isomorphe à $\mathbb{K}^*/Ker\ f$ et de ce fait $f(\mathbb{K}^2)$ possède $\frac{q-1}{2}$ éléments.

Si $a = b^2$, $a^{\frac{q-1}{2}} = b^{q-1} = 1$ d'après le théorème de Lagrange ; en outre dans $\mathbb{K}[X]$ on peut écrire :

$$X^{\frac{q-1}{2}} - 1 = \prod_{a \in f(\mathbb{K}^2)} (X - a)$$

ce qui prouve que si x est racine de ce polynôme, *ie* si $x^{\frac{q-1}{2}} = 1$, x appartient à $f(\mathbb{K}^2)$, et par voie de conséquence, x est un carré.

Enfin -1 est un carré *si et seulement si* :

$$(-1)^{\frac{q-1}{2}} = 1$$

et en écrivant $q = 4q' + r$ avec $r \in \{1, 3\}$ on voit que la relation précédente n'a lieu que si $r = 1$ ce qui achève la démonstration.

5.2 Les résidus quadratiques ; les symboles de Legendre et Jacobi

a. Résidu quadratique modulo p

Soit p un nombre premier, $p \geq 3$; un entier a est dit *résidu quadratique* modulo p *si et seulement si* , par définition :

$$a^{\frac{p-1}{2}} = 1 \pmod{p}$$

ou encore, de manière équivalente, *si et seulement si* $\bar{a}$ est un carré de $\mathbb{F}_p^*$.

Puisque $(\mathbb{F}_p^*, \times)$ est cyclique on constate alors que l'ensemble des classes de résidus quadratiques modulo p constitue un sous-groupe cyclique, d'indice 2, de $\mathbb{F}_p^*$.

b. Symbole de Legendre ; symbole de Jacobi

Soit p un nombre premier impair (*ie* $p \geq 3$) et a un entier ; on convient alors de noter :

$\left(\frac{a}{p}\right)$ l'entier défini par : $\begin{cases} 0 \text{ si } a \text{ est un multiple de } p \\ 1 \text{ si } a \text{ est un résidu quadratique modulo } p \\ -1 \text{ sinon} \end{cases}$

Le symbole $\left(\frac{a}{p}\right)$ porte le nom de *symbole de Legendre* et on peut énoncer :

Proposition 2 : Si $p \geq 3$ est premier et si a est entier, $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \pmod{p}$.

Tout dans cette proposition se vérifie facilement et cependant constatons que $\left(\frac{a}{p}\right)$ ne dépend que de la classe de a modulo p ($\bar{a}$) ce qui revient à dire que si $a = b \pmod{p}$ alors :

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

c. Le symbole de Jacobi

Il généralise le symbole de Legendre ; en effet soit n un entier impair, dont la décomposition en facteurs premiers s'écrit :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

Si a est un entier, l'entier $\left(\frac{a}{n}\right)$ défini par :

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i}$$

porte le nom de *symbole de Jacobi*, étant entendu que, dans le produit $\prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i}$, l'entier $\left(\frac{a}{p_i}\right)$ représente le symbole de Legendre de l'entier a relativement au nombre premier impair p_i.

Etant donnée la définition, on constate aisément que $\left(\frac{a}{n}\right) = 0$ *si et seulement si* $a \wedge n \neq 1$; par conséquent $\left(\frac{a}{n}\right) \in \{-1, 0, 1\}$.

Remarque : Contrairement au cas du symbole de Legendre on peut avoir, s'agissant du symbole de Jacobi, $\left(\frac{a}{n}\right) = 1$ sans pour autant que a soit un carré modulo n. En effet, il suffit de prendre $n = 15$, et $a = 2$ pour s'en convaincre.

d. Quelques propriétés élémentaires de ces symboles

Proposition 3 : Si n est un entier impair $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ quels que soient a et b. En outre si $a = \alpha \pmod{n}$, alors :

$$\left(\frac{a}{n}\right) = \left(\frac{\alpha}{n}\right)$$

Démonstration : Si n est premier, on a *via* ce qui précède :

$$\left(\frac{ab}{n}\right) = (ab)^{\frac{n-1}{2}} = a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \pmod{n}$$

Dans le cas où n est un entier impair quelconque écrivons : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et ainsi :

$$\left(\frac{ab}{n}\right) = \prod_{i=1}^{r} \left(\frac{ab}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i} \left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

Enfin, si $a = \alpha \pmod{n}$, il est évident (laissé aux soins du lecteur) que $\left(\frac{a}{n}\right) = \left(\frac{\alpha}{n}\right)$.

Remarque : Si n est un entier premier impair et si $\bar{a}$ est un générateur du groupe multiplicatif $\mathbb{F}_n^*$, autrement dit si $\bar{a}$ est une racine primitive $(n-1)-$ième de 1 dans $\mathbb{F}_n^*$ on a : $\bar{a}^{n-1} = 1$ et $\bar{a}^{\frac{n-1}{2}} = -1$ ce qui signifie : $\left(\frac{a}{n}\right) = -1$.

5.3 La loi de réciprocité quadratique concernant le symbole de Legendre

A.

Dans tout ce paragraphe lorsqu'un écrit $\left(\frac{a}{p}\right)$ avec $a \in \mathbb{N}$, p est toujours supposé premier et impair.

Proposition 4 : On a $\left(\frac{2}{p}\right) = 1$ *si et seulement si* $p = \pm 1 \pmod 8$, ce qu'on peut écrire : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Démonstration : En effet, on écrit :

$$(1+i)^p = (\sqrt{2}e^{i\frac{\pi}{4}})^p = 2^{\frac{p-1}{2}}(\varepsilon + \varepsilon' i)$$

avec $\varepsilon, \varepsilon' \in \{-1; +1\}$; en travaillant dans l'anneau $\mathbb{Z}[i]$ modulo p il vient :

$$1 + i^p = 2^{\frac{p-1}{2}}(\varepsilon + \varepsilon' i) \pmod p$$

Comme 2 est un carré modulo p *si et seulement si* $2^{\frac{p-1}{2}} = 1 \pmod p$ il en est ainsi *si et seulement si* p est tel que dans $\mathbb{Z}[i]$ on ait : $1 + i^p = \varepsilon + \varepsilon' i$ ce qui impose donc $\varepsilon = 1$ et implique $\sqrt{2}\cos\left(\frac{p\pi}{4}\right) = 1$; en écrivant $p = 8q + r$ il faut que $\cos\left(\frac{r\pi}{4}\right) = \frac{\sqrt{2}}{2}$ ce qui impose $r = \pm 1$ puisque $r \in \{1, 3, 5, -1\}$ et prouve entièrement ce que nous voulions.

Proposition 5 (loi de réciprocité) : Soient p et q premiers impairs ; on a :

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$$

ce qui revient à dire :

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ si } p = q = 3 \pmod 4$$
$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ dans tous le autres cas}$$

Démonstration :

1° pas : Pour p premier on pose : $\varepsilon(p) = \left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ si } p = 1 \pmod 4 \\ -1 \text{ sinon} \end{cases}$. Soit A un anneau quelconque :

$$S(X) = \sum_{k=0}^{q-1}\left(\frac{k}{q}\right)X^k = \sum_{\bar{k}\in\mathbb{F}_q^*}\left(\frac{k}{q}\right)X^k$$

$S(X)$ appartient à $A[X]$ et on a :

$$S(X)^2 \pmod{(X^q - 1)} = \sum_{m=0}^{q-1}\left(\sum_{\substack{k+l=m \pmod q \\ 0\le k,l\le q-1}}\left(\frac{k}{q}\right)\left(\frac{l}{q}\right)\right)X^m$$

Si $m = 0$ le terme constant de cette égalité vaut :

$$\sum_{k=0}^{q-1}\left(\frac{k}{q}\right)\left(\frac{q-k}{q}\right)=\sum_{k=0}^{q-1}\left(\frac{-k^2}{q}\right)=\varepsilon(q)\sum_{k=1}^{q-1}\left(\frac{k^2}{q}\right)=(q-1)\varepsilon(q)$$

Si $m \neq 0$ le coefficient de X^m est égal à :

$$\sum_{k=1}^{q-1}\left(\frac{k}{q}\right)\left(\frac{m-k}{q}\right)=\sum_{k=1}^{q-1}\left(\frac{k(m-k)}{q}\right)$$

si $\bar{k} \in \mathbb{F}_q^*$ désignons par k' un entier tel que $kk' = 1 \pmod q$; alors on peut écrire :

$$\left(\frac{k(m-k)}{q}\right)=\left(\frac{k^2(mk'-1)}{q}\right)=\left(\frac{mk'-1}{q}\right)$$

et lorsque $\bar{k}$ décrit $\mathbb{F}_q^*$, $\overline{mk'-1}$ décrit $\mathbb{F}_q^*\backslash\{-1\}$; comme :

$$\left(\frac{-1}{q}\right)+\sum_{\bar{k}'\in\mathbb{F}_q^*}\left(\frac{mk'-1}{q}\right)=\sum_{k=1}^{q-1}\left(\frac{k}{q}\right)=0$$

(puisqu'il y a $\frac{q-1}{2}$ carrés et $\frac{q-1}{2}$ non carrés dans $\mathbb{F}_q^*$) il vient :

$$\sum_{k=1}^{q-1}\left(\frac{k(m-k)}{q}\right)=-\varepsilon(q)$$

d'où l'on déduit dans $A[X]$:

$$\boxed{S(X)^2 \pmod{(X^q-1)} = q\varepsilon(q) - \varepsilon(q)[1 + X + \cdots + X^{q-1}]}$$

2° pas : Supposons que l'anneau A soit un anneau de caractéristique p ; alors dans $A[X]$ on peut écrire :

$$S(X)^p=\sum_{k=0}^{q-1}\left(\frac{k}{q}\right)X^{kp}$$

et ainsi :

$$\left(\frac{p}{q}\right)S(X)^p=\sum_{k=0}^{q-1}\left(\frac{pk}{q}\right)X^{pk}$$

ce qui entraîne modulo $(X^q - 1)$ dans $A[X]$:

$$\left(\frac{p}{q}\right)S(X)^p=\sum_{k=0}^{q-1}\left(\frac{pk}{q}\right)X^{pk \pmod q} \pmod{(X^q-1)}$$

or l'application :

$$\bar{k} \in \mathbb{F}_q^* \longrightarrow \overline{pk} \in \mathbb{F}_q^*$$

est une bijection ce qui nous permet d'écrire :

$$\left(\frac{p}{q}\right) S(X)^q = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) X^i \pmod{(X^q - 1)}$$

ou encore :

$$\boxed{\left(\frac{p}{q}\right) S(X)^p = S(X) \pmod{(X^q - 1)}}$$

Via ce qui vient d'être établi, on voit tout l'intérêt de disposer d'un anneau A de caractéristique p et d'un élément α de A tel que : $1 + \alpha + \cdots + \alpha^{q-1} = 0$; dans ce cas on a : $\alpha^q = 1$ (car $\alpha^q - 1 = (\alpha - 1)(1 + \alpha + \cdots + \alpha^{q-1})$) et de plus :

$$\boxed{\begin{cases} (S(\alpha))^2 = q\varepsilon(q) \\ \left(\frac{p}{q}\right)(S(\alpha))^p = S(\alpha) \end{cases}}$$

Les conditions précédentes sont requises si on définit A par :
$A = \mathbb{F}_p[X]/(1 + X + \cdots + X^{q-1})$ où $(1 + X + \cdots + X^{q-1})$ est l'idéal de $\mathbb{F}_p[X]$ engendré par $\Phi_q(X) = 1 + X + \cdots + X^{q-1}$ (q-ième polynôme cyclotomique) et si on prend $\alpha = \bar{X}$. On a donc :

$$(S(\alpha))^{p-1} = (S(\alpha)^2)^{\frac{p-1}{2}} = (\varepsilon(q))^{\frac{p-1}{2}} q^{\frac{p-1}{2}} = (\varepsilon(q))^{\frac{p-1}{2}} \left(\frac{q}{p}\right)$$

L'élément $S(\alpha)$ de A est inversible dans l'anneau A ; en effet puisque q est premier avec l'entier p, $\bar{q}$ est inversible dans le corps $\mathbb{F}_p$; si $\bar{q}'\bar{q} = \bar{1}$ dans $\mathbb{F}_p$, il s'ensuit alors que dans l'anneau A nous avons :

$$(\bar{q}' S(\alpha)) S(\alpha) = \varepsilon(q)$$

ce qui prouve bien que $S(\alpha)$ est inversible dans l'anneau A que nous avons choisi ; mais alors il reste :

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \varepsilon(q)^{\frac{p-1}{2}}$$

ce qui fournit le théorème de Gauss sur la réciprocité quadratique, à savoir, pour p et q premiers impairs distincts : $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ si $p = q = 3 \pmod 4$ et $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ sinon.

Remarques :

a. L'anneau A étant quelconque, on a pour $\alpha \in A$ tel que : $1 + \alpha + \cdots + \alpha^{q-1} = 0$:

$$\boxed{S(\alpha)=\sum_{k=0}^{q-1}\left(\frac{k}{q}\right)\alpha^k=\sum_{k=0}^{q-1}\alpha^{k^2}}$$

En effet : $S(\alpha)=\sum_{k=0}^{q-1}\left(\frac{k}{q}\right)\alpha^k=\sum_{\left(\frac{k}{q}\right)=1}\alpha^k-\sum_{\left(\frac{k}{q}\right)=-1}\alpha^k$ et comme : $1+\sum_{\left(\frac{k}{q}\right)=1}\alpha^k+\sum_{\left(\frac{k}{q}\right)=-1}\alpha^k=0$ il vient naturellement :

$$S(\alpha)=2\sum_{\left(\frac{k}{q}\right)=1}\alpha^k+1=\sum_{k=0}^{q-1}\alpha^{k^2}$$

et comme la formule $S(\alpha)^2=q\varepsilon(q)$ ne tient qu'au fait que $1+\alpha+\cdots+\alpha^{q-1}=0$, si on prend $A=\mathbb{C}$ on voit avec $\alpha=e^{\frac{2i\pi}{q}}$ que l'on a : $\left(\sum_{k=0}^{q-1}e^{\frac{2i\pi k^2}{q}}\right)^2=q\varepsilon(q)$ ce qui fournit :

$$\sum_{0\leq k\leq q-1}e^{\frac{2i\pi k^2}{q}}\in\{\pm\sqrt{q},\pm i\sqrt{q}\}$$

b. En fait le lecteur curieux pourra montrer que si $q\geq 3$ est premier on a :

$$\sum_{k=0}^{q-1}e^{\frac{2i\pi k^2}{q}}=\sqrt{q}\frac{1+i^{-q}}{1+i^{-1}}=\begin{cases}\sqrt{q}\text{ si }q=1\pmod 4\\ i\sqrt{q}\text{ si }q=3\pmod 4\end{cases}$$

(cette somme porte aussi le nom de somme de Gauss).

B. Exemples d'utilisation de la loi de réciprocité relative au symbole de Legendre

Exemple 1 : Soit p un nombre premier ; on peut écrire : $\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$; si $p=1$ modulo 4, $\left(\frac{-1}{p}\right)=1$ et alors $\left(\frac{-3}{p}\right)=\left(\frac{3}{p}\right)$; si, par contre $p=3$ modulo 4, $\left(\frac{-1}{p}\right)=-1$ et $\left(\frac{3}{p}\right)=-\left(\frac{p}{3}\right)$. Donc, dans tous les cas de figure :

$$\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$$

qui est égal à 1 *si et seulement si* $p=1$ modulo 3.

Exemple 2 : p est toujours premier, $p\geq 7$. $\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)$; on peut écrire $p=5p'+i$ avec $i\in\{1,2,3,4\}$ et $\left(\frac{p}{5}\right)=\left(\frac{i}{5}\right)=1$ *si et seulement si* $i\in\{1,4\}$ et un calcul facile montre que $\left(\frac{5}{p}\right)=p^2\pmod 5$.

5.4 La réciprocité concernant le symbole de Jacobi

Elle peut se résumer dans la proposition suivante :

Proposition 6 : Soient m et n des entiers impairs supérieurs ou égaux à 3. On a :

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

Si $a = b$ modulo n :

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} \text{ et enfin } \left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) \text{ si } m = n = 3 \pmod 4 \\ \left(\frac{n}{m}\right) \text{ dans tous les autres cas} \end{cases}$$

Démonstration : Les deux premières assertions étant évidentes (donc laissées aux soins du lecteur) montrons désormais la relation :

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

Ecrivons : $n = p_1 p_2 \cdots p_m p_{m+1} \cdots p_r$ (décomposition de l'entier n en facteurs premiers, certains pouvant se répéter) où : $p_1, p_2, \ldots, p_m = \pm 1 \pmod 8$ et $p_{m+1}, \ldots, p_r = \pm 3 \pmod 8$. Dans ces conditions on a : $\left(\frac{2}{n}\right) = (-1)^{r-m}$ et si $r - m$ est pair n est égal à ± 1 modulo 8 et on a bien :

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

si $r - m$ est impair $n = \pm 3$ modulo 8 et alors $\left(\frac{2}{n}\right) = -1 = (-1)^{\frac{n^2-1}{8}}$, ce qui prouve bien ce que nous voulions.

Reste à prouver que $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$ si $m = n = 3$ modulo 4 et $\left(\frac{n}{m}\right)$ sinon ; en effet évacuons d'abord le cas où $m \wedge n \neq 1$, auquel cas $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 0$.

Ecrivons donc : $m = u_1 u_2 \cdots u_r u_{r+1} \cdots u_s$ avec $u_1, \ldots, u_r = 1 \pmod 4$ et $u_{r+1} = \cdots = u_s = 3 \pmod 4$, et $n = v_1 v_2 \cdots v_k v_{k+1} \cdots v_l$ (décomposition de n en facteurs premiers) où : $v_1 = \cdots = v_k = 1 \pmod 4$ et $v_{k+1} = \cdots = v_l = \pmod 4$; notons qu'il peut y avoir des facteurs premiers multiples dans la décomposition primaire de m (*resp.* de n).

Puisque $m \wedge n = 1$ on a : $u_i \neq v_j$ pour tout couple (i, j) ; dans ces conditions on peut écrire :

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{l} \left(\frac{m}{v_i}\right) = \left(\frac{m}{v_1}\right) \cdots \left(\frac{m}{v_k}\right)\left(\frac{m}{v_{k+1}}\right) \cdots \left(\frac{m}{v_l}\right)$$

Si $i \in \{1, 2, \ldots, k\}$, $\left(\frac{m}{v_i}\right) = \left(\frac{u_1}{v_i}\right) \cdots \left(\frac{u_s}{v_i}\right) = \left(\frac{v_i}{u_1}\right) \cdots \left(\frac{v_i}{u_s}\right) = \left(\frac{v_i}{m}\right)$.

Si $i \in \{k+1, \ldots, l\}$:

$$\begin{aligned}\left(\frac{m}{v_i}\right) &= \left(\frac{u_1}{v_i}\right)\cdots\left(\frac{u_r}{v_i}\right)\left(\frac{u_{r+1}}{v_i}\right)\cdots\left(\frac{u_s}{v_i}\right)\\ &= \left(\frac{v_i}{u_1}\right)\cdots\left(\frac{v_i}{u_r}\right)(-1)^{s-r}\left(\frac{v_i}{u_{r+1}}\right)\cdots\left(\frac{v_i}{u_s}\right)\\ &= (-1)^{s-r}\left(\frac{v_i}{m}\right)\end{aligned}$$

En définitive on obtient :

$$\left(\frac{m}{n}\right) = \left(\frac{v_1}{m}\right)\cdots\left(\frac{v_k}{m}\right) \times (-1)^{(s-r)(l-k)}\left(\frac{v_{k+1}}{m}\right)\cdots\left(\frac{v_l}{m}\right)$$

ou encore :

$$\left(\frac{m}{n}\right) = (-1)^{(s-r)(l-k)}\left(\frac{n}{m}\right)$$

dans ces conditions si $m = n = 3 \pmod 4$, $(s-r)$ et $(l-k)$ sont impairs et on a bien : $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$; sinon, le produit $(s-r)(l-k)$ est alors un entier pair et il s'ensuit que l'on a : $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$; la proposition concernant la réciprocité faisant intervenir le symbole de Jacobi est donc entièrement démontrée.

5.5 Application : le test de primalité de Solovay-Strassen

A.

Ce paragraphe commence par la proposition suivante :

Proposition 7 : Soit n un entier impair ; si pour tout $\bar{a}$ de l'anneau $\mathbb{Z}/n\mathbb{Z}$ inversible, $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod n$, alors l'entier n est premier (le symbole $\left(\frac{a}{n}\right)$ désigne ici celui de Jacobi).

Démonstration : 1° pas : On a donc, si G_n désigne le groupe multiplicatif des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$:

$$\forall \bar{a} \in G_n, \quad \bar{a}^{n-1} = \bar{1}$$

Alors n est sans facteur premier carré ; en effet supposons qu'il existe p entier premier tel que :

$$n = p^2 n'$$

et soit a l'entier défini par :

$$a = 1 + pn'$$

puisque p est premier les coefficients binomiaux $\binom{p}{k}$ sont des multiples de p pour $k = 1, 2, \ldots, p-1$ et de ce fait il vient : $a^p = 1 \pmod n$ et comme $a \neq 1$ modulo n il s'ensuit que l'ordre de $\bar{a}$ dans G_n est égal à p ; dans ces conditions puisque $a^{n-1} = 1 \pmod n$, p divise l'entier $n-1$, autrement dit p divise $p^2 n' - 1$ ce qui est impossible et achève la preuve du premier pas.

2° pas : Supposons n non premier et écrivons : $n = p_1 p_2 \cdots p_r$ sa décomposition en facteurs premiers avec $r \geq 2$ et où $p_i \neq p_j$ si $i \neq j$.

Ainsi pour tout a premier avec n on peut écrire :

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right) = a^{\frac{n-1}{2}} \pmod{n}$$

notons $a_i = a \pmod{p_i}$. Ainsi :

$$a^{\frac{n-1}{2}} \pmod{n} = \prod_{i=1}^{r} \left(\frac{a_i}{p_i}\right)$$

et en raisonnant modulo p_1 l'égalité précédente entraîne :

$$\left(\frac{a_1}{p_1}\right) \cdots \left(\frac{a_r}{p_r}\right) = a_1^{\frac{n-1}{2}} \pmod{p_1}$$

a_1 est premier avec p_1 puisque $a \wedge n = 1$ (il en est de même d'ailleurs pour a_i avec p_i, $i = 2, \ldots, r$) ; soit a'_2 un entier tel que $\left(\frac{a'_2}{p_2}\right) = -\left(\frac{a_2}{p_2}\right)$. L'application :
$\bar{a} \in \mathbb{Z}/n\mathbb{Z} \longrightarrow (\bar{a} \pmod{p_1}, \ldots, \bar{a} \pmod{p_r})$ est, *via* le théorème chinois, une isomorphie de $\mathbb{Z}/n\mathbb{Z}$ sur l'anneau produit $\prod_{i=1}^{r} \mathbb{Z}/p_i\mathbb{Z}$; par conséquent on peut trouver b entier tel que :

$$\bar{b} \pmod{p_1} = \bar{a}_1, \bar{b} \pmod{p_2} = \bar{a'}_2, \ldots, \bar{b} \pmod{p_r} = \bar{a}_r$$

On peut alors écrire :

$$a_1^{\frac{n-1}{2}} = \left(\frac{a_1}{p_1}\right)\left(\frac{a'_2}{p_2}\right) \cdots \left(\frac{a_r}{p_r}\right) \pmod{p_1}$$

ce qui impose $a_1^{\frac{n-1}{2}} = 0 \pmod{p_1}$, ce qui est impossible puisque a_1 est premier avec p_1. Par conséquent on ne peut pas avoir $r \geq 2$, ce qui, en d'autres termes signifie que l'entier n est premier.

B. Le test de Solovay-Strassen - Sa fiabilité

Soit n un entier impair ; on appelle *test de primalité de Solovay-Strassen* associé au marqueur aléatoire a entier choisi entre 1 et $n-1$, le protocole mathématique représenté par les quatre étapes décrites ci-dessous :

Etape 1 : Calculer $d = a \wedge n$; si $d \neq 1$, écrire n est composé ; sinon :
Etape 2 : Calculer le symbole de Jacobi $\left(\frac{a}{n}\right)$ et $a^{\frac{n-1}{2}} \pmod{n}$
Etape 3 : Si $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}$ écrire n est premier.
Etape 4 : Si $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \pmod{n}$, écrire n est composé.

Pratiquement, on effectuera p fois le test précédent en changeant aléatoirement de marqueur a ; à l'issue de ces p tests, notons A, B et C les événements suivants :

A : l'entier n est décomposable

B : le test répond à chaque itération "n est premier"

C : au cours d'une itération le test a répondu : "n est composé"

Comme pour le test de Miller-Rabin on a affaire à un algorithme probabiliste. Si la réponse C est fournie, on est certain que l'entier n n'est pas premier, car on sait que si n est premier, pour tout $a \in \{1, 2, \ldots, n-1\}$ on peut écrire :

$$\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}$$

Par contre, ce qui est fâcheux, c'est l'éventualité B sous l'hypothèse A ; en quelque sorte ce qu'il faut savoir estimer c'est la probabilité : $pr(B|A)$ = probabilité d'avoir B sachant A, puisque la probabilité d'erreur du protocole est $pr(A|B)$ (*ie* la probabilité qu'on ait A sachant B) avec :

$$pr(A|B) = \frac{pr(B|A)pr(A)}{pr(B)}$$

où :

$$pr(B) = pr(B|A)pr(A) + pr(B|non\ A)pr(non\ A)$$

ie puisque $pr(B|non\ A) = 1$:

$$pr(B) = pr(B|A)pr(A) + pr(non\ A)$$

Cette question concernant la fiabilité est alors réglée par la proposition suivante :

Proposition 8 : A l'issue d'un seul test (cas où $p = 1$) on a l'inégalité :

$$pr(B|A) \leq \frac{1}{2}$$

Démonstration : Soit $a \in \{1, 2, \ldots, n-1\}$ le marqueur aléatoire associé au test ; puisque le test a répondu "n est premier" c'est que l'on peut écrire :

$$\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}$$

alors que de par ailleurs on sait que l'entier n est composé.

Désignons pour n impair composé, par $H = \{\bar{a} \in G_n : \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \text{ modulo } n\}$.

H est donc strictement contenu dans le groupe G_n des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ puisque n est composé, d'après la proposition 7 ; en outre H est un sous-groupe de G_n, ce qui se vérifie aisément et résulte des propriétés élémentaires du symbole de Jacobi ; le cardinal de H divise (théorème de Lagrange) le cardinal de G_n ; ainsi :

$$card\ H \leq \frac{1}{2}\varphi(n)$$

avec φ l'indicateur d'Euler. Or l'ensemble des marqueurs est tout l'ensemble $\{1, 2, \ldots, n-1\}$ ce qui permet d'écrire :

$$pr(B|A) \leq \frac{1}{2}\frac{\varphi(n)}{n-1} \leq \frac{1}{2}$$

Application et mise en pratique

D'après le théorème de raréfaction des nombres premiers, on sait que si $\Pi(x)$ est le nombre d'entiers premiers inférieurs ou égaux à x on a :

$$\Pi(x) \underset{+\infty}{\sim} \frac{x}{\ln(x)} \text{ (Hadamard, De la Vallée Poussin)}$$

Pratiquement on veut tester la primalité d'un "grand" entier n ; à cet effet on effectue p fois le test de Solovay-Strassen, si bien que l'on a ainsi :

$$pr(B|A) \leq \frac{1}{2^p} = 2^{-p}$$

et compte tenu de ce qui vient d'être dit, la probabilité pour que n soit non-premier est voisine de $1 - \frac{2}{\ln(n)}$; en définitive la probabilité d'erreur du test de Solovay-Strassen répété p fois est approximativement inférieure ou égale à :

$$\frac{\ln(n) - 2}{2^{p+1} + (\ln(n) - 2)}$$

pour $p = 50$ c'est un réel voisin de $0.78 \cdot 10^{-13}$ et pour $p = 100$ il est voisin de $0.7 \cdot 10^{-29}$ pour des entiers inférieurs ou égaux à 2^{256}.

Pratiquement on calculera $\left(\frac{a}{n}\right)$, par utilisation des règles établies précédemment ;quant au calcul de $a^{\frac{n-1}{2}}$ modulo n il sera effectué par utilisation de l'algorithme d'exponentiation rapide.

A titre d'exemple on prend :

$n = 108\,488\,104\,853\,637\,470\,612\,961\,399\,842\,972\,948\,409\,834\,611\,525\,790\,577\,211\,6753$.

Tester sa primalité par utilisation du protocole précédent.

5.6 Comparaison des tests de primalité de Miller-Rabin et Solovay-Strassen

Soit n un entier impair tiré (ou choisi) aléatoirement et T un test de primalité défini dans $\mathbb{N}$; à l'issue de ce tirage et de l'exécution du test désignons par A et B les événements suivants :

A : l'entier n est décomposable (*ie* non premier)

B : le test T répond "l'entier n est premier"

La fiabilité de T est mesurée par le réel :

$$pr_T(A|B)$$

lequel dépend de $pr_T(B|A)$. On a montré que si T_1 est le test de Miller-Rabin et T_2 celui de Solovay-Strassen alors :

$$pr_{T_1}(B|A) \leq \frac{1}{4} \text{ et } pr_{T_2}(B|A) \leq \frac{1}{2}$$

Le simple bon sens nous permet de choisir T_1 de préférence à T_2 ; mais en fait on a mieux et on peut énoncer :

Proposition 9 : Soit n un entier naturel, $n > 9$, impair, s'écrivant : $n = 1 + 2^k m$ où m est un entier impair. Si $a \in \{1, 2, \ldots, n-1\}$ vérifie l'une des conditions du test de primalité T_1, à savoir : $a^m = 1 \pmod n$, ou il existe $i \in \{0, 1, \ldots, k-1\}$: $a^{2^i m} = -1$ modulo n, alors il vérifie les conditions de primalité du test T_2, à savoir :

$$\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod n$$

$\left(\frac{a}{n}\right)$ désignant le symbole de Jacobi.

Démonstration : En d'autres termes, cette proposition affirme que, si n est déclaré premier au sens de Miller-Rabin, il l'est aussi selon le test de Solovay-Strassen dès lors que l'on utilise les mêmes marqueurs a ; on peut dire, en quelque sorte, que T_1 est "plus fin" que T_2 ou encore que T_2 n'apporte aucun renseignement complémentaire à T_1, ce qui justifie l'utilisation de T_1 de préférence à T_2. En effet :

1° pas : Supposons d'abord que $a^m = 1 \pmod n$; on a donc : $\left(\frac{a^m}{n}\right) = \left(\frac{1}{n}\right) = \left(\frac{a}{n}\right)^m = 1$ ce qui impose $\left(\frac{a}{n}\right) = 1$ et en outre : $a^{\frac{n-1}{2}} = a^{2^{k-1}m} = (a^m)^{2^{k-1}} = 1 \pmod n$, ce qui prouve bien l'égalité souhaitée.

2° pas : Supposons ensuite qu'il existe $i \in \{0, 1, \ldots, k-1\}$ tel que l'on ait :

$$a^{2^i m} = -1 \pmod n$$

il s'agit de prouver que l'on a encore : $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod n$.

(i) Si on suppose, dans un premier temps, que l'entier i est strictement inférieur à $k-1$, alors $a^{2^i m} = -1$ entraîne $a^{2^{i+1} m} = 1$ et ainsi : $a^{\frac{n-1}{2}} = 1 \pmod n$.

(ii) Si, au contraire, $i = k-1$, on a directement $a^{\frac{n-1}{2}} = -1 \pmod n$.

Il s'agit donc de prouver que si $i < k-1$, $\left(\frac{a}{n}\right) = 1$ et que si $i = k-1$, $\left(\frac{a}{n}\right) = -1$.

3° pas : Commençons par supposer $i < k-1$ et montrons $\left(\frac{a}{n}\right) = 1$. Si n s'écrit par décomposition primaire : $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ on a :

$$\left(\frac{a}{n}\right) = \prod_{1 \leq j \leq r} \left(\frac{a}{p_j}\right)^{\alpha_j}$$

Soit donc p un facteur premier de l'entier n ; p est impair et on peut écrire : $p - 1 = 2^s t$ avec t impair ; puisqu'on a : $a^{2^i m} = -1$ modulo n, *a fortiori* on a : $a^{2^i m} = -1$ modulo

p ; puisque t est un entier impair on également : $a^{2^i mt} = -1 \pmod p$. On sait que l'on a, dans le corps $\mathbb{F}_p$:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = a^{2^{(s-1)}t} = a^{2^{(s-1)}tm} \pmod p$$

puisque l'entier m est lui aussi un nombre impair.

Si $\left(\frac{a}{p}\right) = 1$, $s - 1 > i$ et si $\left(\frac{a}{p}\right) = -1$, $s = 1 + i$.

Dans le cas où $\left(\frac{a}{p}\right) = 1$, $p = 1 \pmod{2^{i+2}}$.

Dans le cas où $\left(\frac{a}{p}\right) = -1$, $p = 1 \pmod{2^{i+1}}$.

Désignons alors par : N le nombre de facteurs premiers p de n (chacun étant compté avec sa multiplicité) pour lesquels $s = 1 + i$ (p s'écrivant : $1 + 2^S t$, avec t impair). On a donc : $\left(\frac{a}{n}\right) = (-1)^N$ et : $n = (1 + 2^{i+1})^N \pmod{2^{i+2}}$.

Or :

$$(1 + 2^{i+1})^N = (1 + N2^{i+1}) \pmod{2^{i+2}} \text{ (formule du binôme)}$$

Si $i + 1 < k$ *ie* $i < k - 1$ comme $n = 1$ modulo 2^{i+2} cela impose que N soit un entier pair et alors :

$$\left(\frac{a}{n}\right) = 1$$

comme attendu.

Si, au contraire, $i = k - 1$, il faut que l'entier N défini précédemment soit impair pour avoir :

$$n = (1 + 2^k)^N = 1 + 2^k N \pmod{2^{k+1}}$$

et comme $n = 1 + 2^k \pmod{2^{k+1}}$, N est impair et encore :

$$\left(\frac{a}{n}\right) = -1$$

comme prévu.

5.7 Résidus quadratiques et polynômes sur le corps fini $\mathbb{F}_q$

5.7.1 Instance du problème

Soit $\mathbb{K} = \mathbb{F}_q$ le corps de Frobénius avec $q \geq 2$ premier et n un nombre premier tels que :

$$\begin{cases} q \text{ est un carré modulo } n, ie \quad \left(\frac{q}{n}\right) = q^{\frac{n-1}{2}} = 1 \pmod n \\ n = 2m + 1 \text{ avec } m \text{ premier} \end{cases}$$

Dans ces conditions l'ordre de $\bar{q}$ dans le groupe $\mathbb{F}_n^*$ est égal à m. D'après ce qui a été prouvé lors de l'étude des corps finis, on sait que le n-ième polynôme cyclotomique $\Phi_n(X)$ de $\mathbb{K}[X]$ admet deux facteurs premiers unitaires, chacun étant de degré m ; désignons les par $g(X)$ et $G(X)$.

On a donc :

$$g(X)G(X) = 1 + X + \cdots + X^{n-1}$$

puisque n est premier. Désignons par (g) l'idéal de $\mathbb{K}[X]$ engendré par le polynôme $g(X)$; le quotient algébrique : $\mathbb{K}' = \mathbb{K}[X]/(g)$ est un corps ; posons alors, $\alpha = \bar{X}$; g est dans $\mathbb{K}[X]$ le polynôme minimal de α, c'est-à-dire le polynôme unitaire de degré le plus petit s'annulant en α. En outre, $\alpha^n = 1$, et comme n est premier, cela montre que α est une racine primitive n-ième de 1 dans le corps $\mathbb{K}'$. Désignons momentanément par $A(X)$ et $B(X)$ les éléments de $\mathbb{K}'[X]$ définis par :

$$A(X) = \prod_{(\frac{i}{n})=1} (X - \alpha^i), B(X) = \prod_{(\frac{i}{n})=-1} (X - \alpha^i)$$

Alors on a :

Proposition 10 : $A(X)$ et $B(X)$ sont dans $\mathbb{K}[X]$ et :

$$g(X) = A(X), G(X) = B(X)$$

Démonstration : $A(X)$ et $B(X)$ sont de degré m dans $\mathbb{K}'[X]$ et ils sont tous deux unitaires ; comme α est racine primitive n-ième de 1, on peut donc écrire, toujours dans $\mathbb{K}'[X]$:

$$X^n - 1 = (X - 1) \prod_{i=1}^{n-1} (X - \alpha^i)$$

et il est bien clair que : $\prod_{i=1}^{n-1}(X - \alpha^i) = A(X)B(X)$. De ce fait, dans $\mathbb{K}'[X]$ on dispose de l'égalité polynomiale :

$$A(X)B(X) = g(X)G(X)$$

Dans $\mathbb{K}'[X]$ on peut écrire :

$$A(X)^q = \prod_{(\frac{i}{n})=1} (X - \alpha^i)^q = \prod_{(\frac{i}{n})=1} (X^q - \alpha^{iq})$$

et comme $q \wedge n = 1$, l'application : $\bar{i} \in \mathbb{F}_n^* \longrightarrow \bar{q}\bar{i} \in \mathbb{F}_n^*$ est une bijection et lorsque i décrit l'ensemble des carrés modulo m il en est de même de qi puisque q est lui aussi un carré modulo n ; de ce fait on a :

$$(A(X))^q = \prod_{(\frac{j}{n})} (X^q - \alpha^j) = A(X^q)$$

or si on écrit dans $\mathbb{K}'[X]$:

$$A(X) = X^m + \lambda_{m-1}X^{m-1} + \cdots + \lambda_0$$

on a donc :

$$\begin{aligned}(A(X))^q &= X^{mq} + \lambda_{m-1}^q X^{q(m-1)} + \cdots + \lambda_i^q X^{qi} + \cdots + \lambda_0^q \\ &= A(X^q) = X^{mq} + \lambda_{m-1} X^{q(m-1)} + \cdots + \lambda_i X^{qi} + \cdots + \lambda_0\end{aligned}$$

ce qui impose dans $\mathbb{K}'$:

$$\lambda_i^q = \lambda_i$$

pour $i = 0, 1, \ldots, m-1$. Or le polynôme $X^q - X$ de $\mathbb{K}'$ a toutes ses racines dans $\mathbb{K}$ puisque q étant le cardinal de $\mathbb{K}$ on sait que pour tout $x \in \mathbb{K}$, $x^q = x$.

Bilan : $\lambda_i \in \mathbb{K}$ pour tout i et $A(X)$ est dans $\mathbb{K}[X]$; comme $A(\alpha) = 0$, et que le degré de A est égal à m il en résulte :

$$g(X) = A(X) \text{ puis : } G(X) = B(X)$$

5.7.2 Comment déterminer les polynômes $g(X)$ et $G(X)$?

(i) Remarques générales
Remarquons d'abord que $X^{n-1} g(1/X) G(1/X) = g(X)G(X)$ *ie* que l'on a :

$$(X^m g(1/X))(X^m G(1/X)) = g(X)G(X)$$

dans $\mathbb{K}[X]$. Nous envisageons alors deux cas :

1° cas : -1 n'est pas un résidu quadratique modulo n, ce qui est équivalent à $n = 3 \pmod 4$; le polynôme $G(X)$ admet $1/\alpha = \alpha^{-1}$ pour racine et la relation précédente impose alors :

$$\begin{cases} X^m G(1/X) = \varepsilon g(X) \\ X^m g(1/X) = \varepsilon G(X) \end{cases}$$

$\varepsilon \in \{-1; 1\}$ selon le cas.

2° cas : -1 est un résidu quadratique modulo n ; alors $\alpha^{-1} = 1/\alpha$ est racine de $g(X)$ et dans ces conditions il vient : $X^m g(1/X) = g(X), X^m G(1/X) = G(X)$ dans $\mathbb{K}[X]$ (on rappelle que $\mathbb{K} = \mathbb{F}_q$).

(ii) Etude du premier cas, *ie* du cas où $n = 3 \pmod 4$, et $q \neq 2$
Posons dans $\mathbb{K}[X]$:

$$U(X) = \sum_{\left(\frac{i}{n}\right)=1} X^i ; V(X) = \sum_{\left(\frac{i}{n}\right)=-1} X^i$$

Alors on peut écrire :

$$1 + U(X) + V(X) = 1 + X + \cdots + X^{n-1} = \Phi_n(X)$$

$U(\alpha) - V(\alpha) = \sum_{i=0}^{n-1} \alpha^{i^2} = S(\alpha)$ (α ayant le sens précédent ...), d'où $S(\alpha) = 1 + 2U(\alpha)$ ($S(\alpha)$ est la somme de Gauss définie antérieurement).

Comme q est un carré modulo n, $(U(\alpha))^q = U(\alpha)$ (déjà vu) et de ce fait $U(\alpha) \in \mathbb{K}(= \mathbb{F}_q)$ (on rappelle que $X^q - X$ en tant qu'élément de $\mathbb{K}'[X]$ a toutes ses racines dans $\mathbb{K} = \mathbb{F}_q$) ; par conséquent $S(\alpha)$ est un élément du corps $\mathbb{K}$ et puisque $\alpha^n = 1$ avec $\alpha \neq 1$, nous avons, à bon droit, l'égalité dans $\mathbb{K}$:

$$(S(\alpha))^2 = n\varepsilon(n) = -n$$

ce qui veut dire que $-n$ est un carré modulo q.
Dans ces conditions soit a dans $\mathbb{F}_q$ tel que : $-n = a^2 \pmod q$; on a donc :

$$S(\alpha) = a \text{ ou } S(\alpha) = -a \pmod q$$

Le polynôme : $2U(X) + (1 - S(\alpha))$ s'annule en $X = \alpha$, tout comme le polynôme : $X^n - 1$; il en est donc de même pour leur pgcd, ce qui permet d'abaisser le degré et d'obtenir un polynôme s'annulent en α ; si le degré du pgcd est égal à m, le polynôme obtenu est le polynôme $g(X)$, sinon les deux polynômes : $X^n - 1$ et $2V(X) + (1 + S(\alpha))$ s'annulent également en $X = \alpha$; on peut donc, à nouveau rechercher leur pgcd, etc...etc...
Exemple : On prend $n = 11$ et $q = 3$. Constatons d'abord que $3 = 5^2 \pmod{11}$, et que $n = 3$ modulo 4 ; ici $\mathbb{K} = \mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$; enfin $n = 2 \times 5 + 1$; ici $m = 5$ est bien premier ; on peut donc appliquer ce qui précède.

$$\Phi_{11}(X) = 1 + X + \cdots + X^{10} = g(X)G(X)$$

avec $g(X)$ et $G(X)$ dans $\mathbb{F}_3[X]$, chacun de degré 5. Les carrés modulo 11 sont 1,3,4,5,9 d'où : $U(X) = X+X^3+X^4+X^5+X^9$, $V(X) = X^2+X^6+X^7+X^8+X^{10}$, $-11 = 1 \pmod 3$ et de ce fait $S^2(\alpha) = \bar{1}$ dans $\mathbb{F}_3$ ce qui impose $S(\alpha) = \bar{1}$ ou $S(\alpha) = \bar{2}$; ainsi un des deux polynômes :

$$X^8 + X^4 + X^3 + X^2 + 1, \text{ou } X^9 + X^5 + X^4 + X^3 + X + 1$$

s'annule en α. Un calcul facile laissé aux soins du lecteur montre que :

$$pgcd(X^{11} - 1; X^8 + X^4 + X^3 + X^2 + 1) = X^5 - X^3 + X^2 - X - 1$$

dans $\mathbb{F}_3[X]$.
Le polynôme : $X^5 - X^3 + X^2 - X - 1$ divise donc $X^{11} - 1$ dans $\mathbb{F}_3[X]$ et ne s'annule pas si $X = 1$; par conséquent il divise $\Phi_{11}(X)$ et comme il est de degré 5 c'est un des deux facteurs premiers de $\Phi_{11}(X)$; l'autre valant alors $-X^5\left(\frac{1}{X^5} - \frac{1}{X^3} + \frac{1}{X^2} - \frac{1}{X} - 1\right)$ *ie* étant égal à :

$$X^5 + X^4 - X^3 + X^2 - 1$$

D'où dans $\mathbb{F}_3[X]$, la factorisation du polynôme $\Phi_{11}(X)$:

$$1 + X + X^2 + \cdots + X^{10} = (X^5 - X^3 + X^2 - X - 1)(X^5 + X^4 - X^3 + X^2 - 1)$$

5.7.3 Etude du premier cas *ie* $n = 3 \pmod 4$ avec $q = 2$

Il s'agit de décomposer dans $\mathbb{F}_2[X]$ le polynôme cyclotomique $\Phi_n(X) = 1 + X + \cdots + X^{n-1}$ sachant que $\left(\frac{2}{n}\right) = 2^{\frac{n-1}{2}} = 1 \pmod n$, avec $n = 2m + 1$, m premier tout comme n.

On a toujours, ici dans $\mathbb{F}_2[X]$:

$$\Phi_n(X) = g(X)G(X)$$

avec g et G de degré m.

Les relations précédentes (*via* les même notations) restent valables et l'on a : $U(\alpha) = 0$ ou 1, $V(\alpha) = 0$ ou 1, dans le corps $\mathbb{F}_2$, et $S(\alpha) = 1$. On peut donc (quitte à changer α en $1/\alpha$) supposer $U(\alpha) = 0$ (en effet $U(1/\alpha) = V(\alpha)$ puisque $\left(\frac{i}{n}\right) = 1$ équivaut à $\left(\frac{-i}{n}\right) = -1$).

Le pgcd des polynômes $U(X)$ et $X^n - 1$ s'annule encore en α, si bien que c'est un multiple du polynôme $g(X)$, ce qui permettra en "affinant et diversifiant" les procédures de recherche des pgcd d'obtenir $g(X)$.

Exemple : On prend $n = 23 = 2 \times 11 + 1$ (ici $m = 11$) ; ensuite : $2 = 5^2 \pmod{23}$ est bien un carré modulo n et $n = 3 \pmod 4$; les conditions précédentes sont requises et on trouve aisément :

$$U(X) = X + X^2 + X^3 + X^4 + X^6 + X^8 + X^9 + X^{12} + X^{13} + X^{16} + X^{18}$$

$$V(X) = X^5 + X^7 + X^{10} + X^{11} + X^{14} + X^{15} + X^{17} + X^{19} + X^{20} + X^{21} + X^{22}$$

dans $\mathbb{F}_2[X]$ et :

$$\begin{aligned} &pgcd(X^{23} - 11; 1 + X + X^2 + X^3 + X^5 + X^7 + X^8 + X^{11} + X^{12} + X^{15} + X^{17}) \\ &\quad = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11} \end{aligned}$$

ainsi le polynôme $1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$ de $\mathbb{F}_2[X]$ divise $X^{23} - 1$ et ne s'annule pas en $X = 1$; il divise donc $\Phi_{23}(X)$, l'autre étant :
$X^{11}\left(1 + \frac{1}{X} + \frac{1}{X^5} + \frac{1}{X^6} + \frac{1}{X^7} + \frac{1}{X^9} + \frac{1}{X^{11}}\right)$ ce qui fournit dans $\mathbb{F}_2[X]$ la décomposition primaire cherchée, à savoir :

$$\Phi_{23}(X) = (X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)$$

Chapitre 6

Les nombres premiers

6.1 Le point de vue d'Euler et celui de Gauss

Il commence par une citation d'Euler :

> « *Les mathématiques ont tâché jusqu'ici, en vain, de découvrir quelque ordre dans la progression des nombres premiers, et on a lieu de croire que c'est un mystère auquel l'esprit humain ne saurait jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers, que quelques uns se sont donnés la peine de continuer au delà de cent mille et on s'apercevra d'abord qu'il n'y règne ni ordre ni règle.*
>
> *Cette circonstance est d'autant plus surprenante, que l'arithmétique nous fournit des règles sûres, par le moyen desquelles on est en état de continuer la progression de ces nombres aussi loin qu'on souhaite, sans pourtant nous y laisser la moindre marque de quelque ordre...* »

Et il continue par une citation de Gauss :

> « *Le problème de distinguer les nombres premiers de ceux qui ne le sont pas doit être considéré comme le plus important en arithmétique ; la dignité même de la science requiert que tous les moyens possibles soient explorés pour la résolution d'un problème aussi élégant et aussi célèbre.* »

Après les deux citations des plus illustres mathématiciens ayant largement contribué à l'essor de l'arithmétique, on peut, tout simplement, constater que l'esprit humain se pose des questions si étranges, surtout lorsque l'infini y entre, qu'on ne doit pas s'étonner s'il y a peine à en venir à bout...

6.2 Quelques résultats remarquables concernant les nombres premiers

a. Le théorème de raréfaction

Il est considéré comme le théorème fondamental des nombres premiers ; il a été démontré conjointement à la fois au XIX° siècle par Hadamard et De la Vallée Poussin, la même année ! Et il s'énonce en disant que, si $\Pi(x) = card\{p \leq x, p \text{ premier}\}$ on a l'équivalence :

$$\Pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}$$

Cela revient encore à dire que si $p_1 < p_2 < \cdots < p_n < \cdots$ est la suite infinie des nombres premiers, on a :

$$p_n \underset{n\to\infty}{\sim} n \ln n$$

(voir **6.12**)

Un théorème célébrissime lui aussi : le théorème de Dirichlet

Il a d'ailleurs été utilisé dans cet ouvrage lors de la présentation du cryptosystème de type El-Gamal construit sur $\mathbb{F}_p^n$ muni de la loi de convolution, le "masque" étant constitué par la "surface" de Frobénius (voir le chapitre **7**).

Il s'énonce en disant que si a et b sont deux entiers premiers entre eux ($b \geq 2$), il y a une infinité de nombres premiers dans la progression arithmétique :

$$a, a+b, a+2b, \ldots, a+kb, \ldots$$

A titre d'exemple nous allons montrer le théorème de Dirichlet lorsque $a = 1$ et $b = 2^m$ où m est un entier quelconque supérieur ou égal à 1. Cela revient donc à démontrer qu'il existe une infinité de nombres premiers égaux à 1 modulo 2^m.

Considérons le nombre de Fermat $F_m = 2^{2^m} + 1$ et désignons par p un facteur premier de F_m ; on a donc modulo p : $\bar{2}^{2^m} = -\bar{1}$ et ainsi $\bar{2}^{2^{m+1}} = \bar{1} \pmod{p}$; ainsi l'ordre de $\bar{2}$ modulo p est égal à 2^{m+1} ; comme $\bar{2}^{p-1} = \bar{1}$ modulo p, il s'ensuit que $p-1$ est un multiple de 2^{m+1} donc *a fortiori* de 2^m.

Les nombres de Fermat $F_{m+i} = 2^{2^{m+i}}+1$ pour $i = 1, 2, \ldots$ sont deux à deux premiers entre eux (la preuve a été fournie en **6.10**) ; donc pour tout i on peut trouver un nombre premier p_i égal à 1 modulo 2^m et les $p_i, i = 1, 2, \ldots$ étant deux à deux distincts puisque :

$$F_{m+i} \wedge F_{m+j} = 1 \text{ si } i \neq j$$

la preuve du théorème de Dirichlet, dans ce cas particulier, grâce à l'utilisation des nombres de Fermat, est terminée.

Un théorème de Lagrange sur les nombres premiers

Il s'énonce en disant que tout nombre premier p est la somme de quatre carrés ; en outre, si p est égal à 1 modulo 4, p est la somme de deux carrés.

Comme conséquence on obtient le fameux théorème de Lagrange, à savoir :

Tout entier naturel est la somme de quatre carrés

En effet : si $a, b, c, d, a', b', c', d'$ sont dans $\mathbb{Z}$, en constatant que l'on peut écrire :

$$(a^2+b^2+c^2+d^2)('a'^2+b'^2+c'^2+d'^2) = \det \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} \begin{pmatrix} a'+ib' & c'+id' \\ -c'+id' & a'-ib' \end{pmatrix}$$

on constate que l'on a l'égalité :

$$(a^2+b^2+c^2+d^2)('a'^2+b'^2+c'^2+d'^2) = (aa'-bb'-cc'-dd')^2 + (ab'+a'b+cd'- dc')^2 + (ac'-bd'+ca'+db')^2 + (bc'+ad'+a'd-b'c)^2$$

laquelle signifie que la somme de quatre carrés d'entiers est stable par multiplication d'où l'intérêt de se limiter aux nombres premiers pour prouver le théorème des quatre carrés de Lagrange.

6.3 Les nombres premiers jumeaux

Définition : On dit que deux nombres premiers sont jumeaux si l'un s'écrit p et l'autre $p+2$.

Autrement dit deux nombres premiers jumeaux sont deux nombres premiers consécutifs dont la différence est de valeur absolue égale à 2. Rappelons, afin de pouvoir caractériser les premiers jumeaux, le théorème de Wilson :

Proposition 1 : p est un nombre premier *si et seulement si* :

$$(p-1)! = -1 \pmod{p}$$

Démonstration : Si p est un nombre premier, dans $\mathbb{F}_p[X]$, on peut écrire :

$$X^{p-1} - 1 = \prod_{\bar{a} \in \mathbb{F}_p^*} (X - \bar{a})$$

puisque l'on sait que pour tout $\bar{a} \in \mathbb{F}_p^*$, $\bar{a}^{p-1} = 1$; en donnant à X la valeur 0 on a donc dans $\mathbb{F}_p$: $-1 = (-1)^{p-1}(p-1)!$ et comme $p-1$ est un nombre pair (sauf si $p=2$ auquel cas tout est évident) on a bien :

$$(p-1)! = -1 \pmod{p}$$

Réciproquement si $(p-1)! = -1 \pmod p$, soit d un diviseur de p autre que p lui-même ; d divise $(p-1)!+1$ et d appartient à $\{1, 2, \ldots, p-1\}$; donc d divise $(p-1)!$ et par suite d divisant 1, il reste $d = 1$; ainsi p est un nombre premier. Alors on peut énoncer :

Proposition 2 : Les entiers p et $p+2$ sont tous deux premiers *si et seulement si* :

$$4[(p-1)!+1] + p = 0 \pmod{(p(p+2))}$$

Démonstration :

(i) Supposons d'abord que la congruence énoncée soit satisfaite ; alors il s'ensuit que l'on peut écrire :

$$4(p-1)! + 2 = 0 \pmod{(p+2)}$$
$$4[(p-1)!+1] = 0 \pmod p$$

Supposons que p ne soit pas premier ; alors p est une puissance de 2 ; en effet soit d un facteur premier de p autre que 2 ; $d \in \{2, 3, \ldots, p-1\}$ et d divise $4(p-1)!+4$, donc d divise 4, et comme c'est impossible cela prouve bien que si p n'est pas premier p s'écrit $p = 2^r$ avec $r \geq 3$ (car $p = 2$ ou $p = 4$ sont impossibles) ; mais alors :

$$2^{r-2} \text{ divise } 1 + (p-1)!$$

et comme 2 divise $(p-1)!$, 2 doit diviser 1 ; ainsi p est premier.

Ceci étant acquis, afin de montrer que $p+2$ est lui aussi premier, il convient d'utiliser l'autre congruence modulo $p+2$; comme $4(p-1)! + 2 = 0 \pmod{p+2}$ on en déduit en multipliant par $p(p+1)$:

$$4[(p-1)!+1] + (2p^2 + 2p - 4) = 0 \pmod{(p+2)}$$

autrement dit :

$$4[(p-1)!+1] + (p+2)(2p-2) = 0 \pmod{(p+2)}$$

et alors :

$$4[(p-1)!+1] = 0 \pmod{(p+2)}$$

ce qui prouve comme précédemment que l'entier $p+2$ est premier.

(ii) Réciproquement supposons que p et $p+2$ soient des nombres premiers ; alors on peut écrire d'après le théorème de Wilson :

$$(p-1)! + 1 = 0 \pmod p, (p+1)! + 1 = 0 \pmod{(p+2)}$$

on peut écrire :

$$(p+1)! + 1 = [(p-1)!p(p+1)] + 1$$

et comme $p(p+1) = (p+2)(p-1)+2$ il en résulte que l'on peut écrire : $2(p-1)!+1 = k(p+2)$ avec k entier.

Comme : $(p-1)!+1=0 \pmod p$ il en résulte que p divise $(p-1)!-2k$ ou encore que $2k+1=0 \pmod p$. Ceci étant acquis on écrit alors :

$$4[(p-1)!]+2=2k(p+2)$$

et comme $2k=k'p-1$, avec k' entier, il reste :

$$4(p-1)!+2=-(p+2)+k'p(p+2)$$

d'où :

$$4(p-1)!+2=-(p+2) \pmod{p(p+2)}$$

ce qui prouve bien la congruence :

$$4(p-1)!+4+p=0 \pmod{p(p+2)}$$

ie :

$$4[(p-1)!+1]+p=0 \pmod{p(p+2)}$$

et achève la démonstration.

6.4 Polynômes générant des nombres premiers

Leur étude commence par la proposition suivante :

Proposition 3 : Si P est un polynôme non constant à coefficients dans l'anneau $\mathbb{Z}$, il existe une infinité d'entiers n tels que $P(n)$ n'est pas un nombre premier.

Démonstration : En effet pour $n \in \mathbb{Z}$ posons $P(n)=m$; alors pour tout entier k, $P(n+km)$ est divisible par m puisque $(n+km)^q=n^q+k_qm$ pour $q \geq 1$.

Si l'ensemble des entiers n tel que $P(n)$ n'est pas un nombre premier est supposé fini, alors pour tout n assez grand $P(n)=m$ est premier ; c'est en particulier vrai pour $P(n+km)$ avec $k \in \mathbb{N}$, qui est premier et divisible par m ; c'est donc m mais alors c'est en contradiction avec le fait que P n'étant pas constant, $|P(n+km)|$ tend vers $+\infty$ quand l'entier k tend vers $+\infty$.

Cette proposition montre déjà qu'il n'existe pas de fonction polynôme f à coefficients entiers telle que $f(n)$ est un nombre premier pour tout entier n.

Cependant il existe des fonctions f de $\mathbb{Z}[X]$ pour lesquelles $f(n)$ est premier pour $n=0,1,2,\ldots,m$ avec m "assez grand" ; la plus connue a été découverte par Euler ; il s'agit du polynôme P défini par :

$$P(X)=X^2+X+41$$

qui prend pour $k=0,1,\ldots,39$ uniquement des valeurs dans l'ensemble des nombres premiers.

6.5 Etude d'un cas particulier : suite de nombres premiers en progression arithmétique

Il peut se résumer dans la proposition suivante :

Proposition 4 : Soit p un nombre premier, a un entier et $f(X) = aX + p$; si $f(0), f(1), \ldots, f(n-1)$ sont des nombres premiers ($n \in \mathbb{N}^*$), soit q le plus grand nombre premier inférieur ou égal à n. Soit N l'entier naturel défini par :

$$N = \prod_{\substack{p_i \text{ premier} \\ p_i \leq q}} p_i$$

alors :
- ou bien N divise l'entier a
- ou bien $p = q$ et N/q divise a.

Démonstration : Supposons que l'entier N ne divise pas l'entier a ; il existe donc des nombres premiers inférieurs à q ne divisant pas a ; soit m le plus petit d'entre eux. Les entiers $p, p+a, \ldots, p+(m-1)a$ sont premiers et deux à deux distincts modulo m.

En effet soient $j, j' \in \{0, 1, \ldots, m-1\}$ avec $p + ja = p + j'a$ modulo m ; on a donc $(j'-j)a = 0 \pmod{m}$ et comme a est inversible modulo m cela impose $j' = j \pmod{m}$, d'où $j' = km + j \geq m + j$ ce qui n'est pas possible ; de ce fait puisque $\mathbb{F}_m$ possède m éléments il existe $i \in \{0, 1, \ldots, m-1\}$ tel que :

$$p + ia = 0 \pmod{m}$$

et comme $p + ia$ est premier cela impose :

$$p + ia = m$$

p ne divise pas l'entier a (puisque $p + a$ est premier) ; par conséquent la définition de m et le fait que $p \leq m$ entraînent :

$$p = m$$

Si on suppose $m = p < q$ alors $m \leq n-1$ et les entiers : $m, m+a, \ldots, m+(m-1)a, m+ma$ sont premiers, ce qui est absurde puisque $m + ma$ n'est pas premier ; ainsi :

$$p = m = q$$

et ainsi tous les p_i premiers, $p_i < q$, divisent a ; par conséquent N/p divise a, ce qui prouve bien ce que nous voulions.

Exemples : Avec : $p = 5$ et $a = 6$ on trouve : 5, 11, 17, 23, 29.

Avec $p = 7, a = 150$ on obtient : 7, 157, 307, 457, 607, 757 et 907.

6.6 Un aspect analytique des nombres premiers

Rappelons que si x est un réel strictement supérieur à 1, la série $\sum_{n=1}^{\infty} \frac{1}{n^x}$ converge et sa somme est notée $\zeta(x)$ (fonction zêta) ; alors si $2 = p_1 < p_2 < \cdots < p_n < \cdots$ est la suite des nombres premiers on peut énoncer :

Proposition 5 : Pour tout $x > 1$,

$$\zeta(x) = \lim_{n \to +\infty} \left(\prod_{i=1}^{n} \frac{1}{1 - \frac{1}{{p_i}^x}} \right)$$

Démonstration : En effet pour $i = 1, 2, \ldots, n$ on peut écrire :

$$\frac{1}{1 - \frac{1}{{p_i}^x}} = \sum_{m_i=0}^{\infty} \frac{1}{p_i^{m_i x}}$$

si bien que le produit $\prod_{i=1}^{n} \left(\frac{1}{1 - \frac{1}{{p_i}^x}} \right)$ est égal à la somme :

$$\sum_{\substack{m_1 \\ 0 \leq \vdots \leq +\infty \\ m_n}} \frac{1}{(p_1^{m_1} \cdots p_n^{m_n})^x}$$

il est bien clair que cette somme n'excède pas $\zeta(x)$ et comme de plus tout entier k compris entre 1 et n s'écrit de manière unique : $k = p_1^{m_1} \cdots p_n^{m_n}$ avec $m_i \geq 0$ on en déduit :

$$\sum_{k=1}^{n} \frac{1}{k^x} < \prod_{i=1}^{n} \frac{1}{1 - \frac{1}{{p_i}^x}} < \zeta(x)$$

d'où la preuve de l'égalité annoncée.

Remarque : Ce qui vient d'être fait reste encore partiellement valable si $x = 1$ et on a :

$$\prod_{i=1}^{n} \left(\frac{1}{1 - \frac{1}{p_i}} \right) > 1 + 1/2 + \cdots + 1/n$$

Cela signifie que la série numérique $\sum_{n=1}^{\infty} \ln(1 - \frac{1}{p_n})$ diverge et comme :

$$\ln(1 - \frac{1}{p_n}) \underset{n \to +\infty}{\sim} -\frac{1}{p_n}$$

la série : $\sum_{n=1}^{\infty} \frac{1}{p_n}$ est divergente ; on a coutume de dire, puisque la série numérique $\sum_{n=1}^{\infty} \frac{1}{n^2}$ est convergente, que les "nombres premiers ne sont pas aussi "clairsemés" que les carrés" (voir aussi le paragraphe 12 de ce chapitre).

6.7 Comment reconnaître qu'un nombre entier est premier ?

Soit p un nombre entier ; si p n'est pas premier il existe q premier, $q \leq \sqrt{p}$, divisant le nombre entier p ; c'est le principe du crible d'Erathostène ; *a contrario*, si p n'est divisible par aucun nombre premier inférieur à $\sqrt{p}$, alors p est un nombre premier ; mais cette méthode naïve est inutilisable lorsque p est un "grand" nombre entier.

Il faut donc avoir recours à d'autres techniques ; certaines, plus singulières que d'autres, font l'objet de l'étude des nombres de Mersenne, par exemple.

Remarquons d'abord que si p est un nombre premier, le groupe multiplicatif $\mathbb{F}_p^*$ est cyclique ; on peut donc trouver des entiers a tels que $\bar{a} \pmod p$ génère $\mathbb{F}_p^*$; ainsi : $\bar{a}^{p-1} = \bar{1}$ et pour tout diviseur m de $p-1$: $\bar{a}^m \neq 1$. Cette observation conduit alors à l'énoncé suivant :

Proposition 6 : Soit p un nombre entier ; alors les deux énoncés suivants sont équivalents :

(i) p est premier

(ii) Il existe $a \in \mathbb{Z}$ tel que $a^{p-1} = 1 \pmod p$ et $a^{\left(\frac{p-1}{q}\right)} \neq 1 \pmod p$ pour tout entier q premier divisant $p-1$.

Démonstration : (i)⇒(ii) En effet il suffit de prendre pour a un entier tel que $a \pmod p$ engendre le groupe cyclique $\mathbb{F}_p^*$ du corps de Frobénius $\mathbb{F}_p$.

Réciproquement supposons (ii) ; soit G le sous-groupe de $\mathbb{F}_p^*$ engendré par a modulo p ; m désignant son ordre, m est un diviseur de $p-1$; écrivons :

$$p - 1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

(décomposition en facteurs premiers) ; ainsi m peut s'écrire :

$$m = p_1^{\beta_1} \cdots p_r^{\beta_r} \text{ avec } 0 \leq \beta_i \leq \alpha_i$$

Si (par exemple) : $\beta_1 < \alpha_1$, l'entier $\frac{p-1}{p_1}$ est un multiple de m, et ainsi : $a^{\frac{p-1}{p_1}} = 1 \pmod p$ ce qui est impossible.

Le groupe des inversibles de l'anneau $\mathbb{Z}/p\mathbb{Z}$ est donc formé des $p-1$ éléments non nuls de cet anneau ; on a donc affaire à un corps ce qui signifie que p est un nombre premier.

De la proposition qui vient d'être établie, on déduit :

Proposition 7 : Soit p un entier impair ; alors les deux énoncés sont équivalents :

(i) p est premier

(ii) Il existe $a \in \mathbb{Z}$ tel que $a^{\frac{p-1}{2}} = -1 \pmod p$ et $a^{\frac{p-1}{q}} \neq 1 \pmod p$ pour tout q premier impair divisant $p-1$.

Démonstration : Si l'énoncé (i) est vrai il suffit de prendre pour a un entier tel que $\bar{a}$ engendre le groupe multiplicatif $\mathbb{F}_p^*$; réciproquement, on a *via* (ii) : $a^{p-1} = 1$

$(\text{mod } p)$; soit maintenant q premier, q divisant $p-1$; si q est impair (ie $q \geq 3$), on a bien : $a^{\left(\frac{p-1}{q}\right)} \neq 1 \ (\text{mod } p)$; si $q = 2$, on l'a aussi par hypothèse, d'où la preuve par application immédiate de la proposition 6.

Pratiquement, on "prouvera" d'abord par une méthode presque sûre : Miller-Rabin ou Solovay-Strassen, qu'un entier est un nombre premier ; ensuite on essaiera d'appliquer la proposition précédente ; bien évidemment, il faut connaître la décomposition en facteurs premiers de l'entier $p-1$, ce qui n'est pas toujours aisé, mais à force de "récursivité" il est parfois possible de conclure.

6.8 Les nombres premiers de Mersenne ; théorème de Lucas

6.8.1 Quelques préliminaires

a.

Soit $a \in \mathbb{Z}$ et $(u_n)_{n\geq 0}$ une suite $\mathbb{R} \to \mathbb{R}$ telle que :

$$\begin{cases} u_{n+1} + u_{n-1} = a u_n \\ \forall n \geq 1 \end{cases}$$

u_0 et u_1 étant donnés.

L'équation caractéristique associée à l'étude de cette suite est : $X^2 - aX + 1 = 0$; si on suppose que $a^2 - 4$ est non nul, il y a alors deux racines réelles ou complexes distinctes α et β et il existe λ et μ réels tels que :

$$\begin{cases} u_n = \lambda \alpha^n + \mu \beta^n \\ \forall n \geq 0 \end{cases}$$

Désignons par $v = (v_n)_{n\geq 0}$, la suite solution avec : $\lambda = \mu = 1$ ie : $v_0 = 2, v_1 = a$; ainsi : $v_n = \alpha^n + \beta^n = \alpha^n + (\alpha^{-1})^n$ car $\alpha\beta = 1$.

Proposition 8 : $v_{2m} = v_m^2 - 2$ et par suite :

$$v_{2^k} = (v_{2^{k-1}})^2 - 2$$

Tout se vérifie très aisément et est laissé aux soins du lecteur. Par conséquent si $(l_k)_{k\geq 1}$ est définie par : $l_k = v_{2^{k-1}}$ on obtient :

$$\begin{cases} l_{k+1} = l_k^2 - 2 \\ l_1 = a \end{cases}$$

b. Un cas particulier

C'est celui où $a = 4$; alors :

$$\begin{cases} v_m = (2+\sqrt{3})^m + (2-\sqrt{3})^m \\ \forall m \geq 0 \end{cases}$$

et v_m est, pour tout m, un nombre entier puisque :

$$v_m = 2 \sum_{0 \leq 2k \leq m} \binom{m}{2k} 2^{m-2k} 3^k$$

c. Une identité

Soit n un entier impair et $M = 2^n - 1$; alors on a :

$$\boxed{2^{\frac{M+1}{2}} l_n = (1+\sqrt{3})^{2^n} + (1-\sqrt{3})^{2^n}}$$

Démonstration : En effet :

$$\begin{aligned} l_n &= (2+\sqrt{3})^{2^{n-1}} + (2-\sqrt{3})^{2^{n-1}} \text{ et alors :} \\ 2^{\frac{M+1}{2}} l_n &= 2^{2^{n-1}} \left[(2+\sqrt{3})^{2^{n-1}} + (2-\sqrt{3})^{2^{n-1}} \right] \\ &= (4+2\sqrt{3})^{2^{n-1}} + (4-2\sqrt{3})^{2^{n-1}} \\ &= \left((1+\sqrt{3})^2 \right)^{2^{n-1}} + \left((1-\sqrt{3})^2 \right)^{2^{n-1}} \\ &= (1+\sqrt{3})^{2^n} + (1-\sqrt{3})^{2^n} \\ &= (1+\sqrt{3})^{M+1} + (1-\sqrt{3})^{M+1} \end{aligned}$$

comme annoncé.

6.8.2 De l'arithmétique

a. Le théorème de Lucas

On appelle *nombre de Mersenne* tout nombre du type $M = 2^n - 1$ avec $n \in \mathbb{N}^*$; on remarquera que c'est le plus grand entier que l'on peut écrire avec n bits.

Si $n = pq$ on a : $M = 2^{pq} - 1 = (2^p - 1)(1 + 2^p + \cdots + 2^{(q-1)p})$ et M n'est pas un nombre premier ; désormais on cherche à caractériser les entiers n tels que M est premier ; cela se fait par le théorème de Lucas :

Proposition 9 : Soit n un entier impair, $n \geq 3$, et $M = 2^n - 1$ un nombre de Mersenne ; si $(l_q)_{q \geq 1}$ est la suite définie modulo M par : $l_1 = 4$ et $l_{q+1} = l_q^2 - 2$, alors : l'entier $M = 2^n - 1$ est premier *si et seulement si* $l_{n-1} = 0 \pmod{M}$.

Démonstration :

1° pas : Supposons $M = 2^n - 1$ premier. On a : $\left(\frac{2}{M}\right) = 1$ car $M = -1 \pmod 8$ d'où : $2^{\frac{M-1}{2}} = 1 \pmod{M}$.

Or : $M = 1 \pmod 3$ d'où : $\left(\frac{3}{M}\right) = -\left(\frac{M}{3}\right) = -\left(\frac{1}{3}\right) = -1$, d'où :

$$3^{\frac{M-1}{2}} = -1 \pmod{M} \text{ (loi de réciprocité)}$$

Puis on peut écrire :

$$2^{\frac{M+1}{2}} l_n = 2 \sum_{0 \leq i \leq 2^{n-1} = \frac{M+1}{2}} \binom{M+1}{2i} 3^i$$

Et avec : $\binom{M+1}{2i} = \binom{M}{2i} + \binom{M}{2i-1}$ on a :

$$2^{\frac{M+1}{2}} l_n = 2(1 + 3^{\frac{M+1}{2}}) \pmod M = 2(1 + 3 \cdot 3^{\frac{M-1}{2}})$$

d'où : $2^{\frac{M+1}{2}} l_n = -4 \pmod M$ et comme : $2^{\frac{M+1}{2}} = 2 \pmod M$ il reste : $l_n = -2 \pmod M$; ainsi avec : $l_n = -2 = l_{n-1}^2 - 2$ il vient :

$$l_{n-1}^2 = 0 \ ie \ \ l_{n-1} = 0 \pmod M$$

ce qui achève le premier pas.

2° pas : Supposons désormais $l_{n-1} = 0 \pmod M$ et soit p un facteur premier de M ; on a $p \geq 5$; désignons par A l'anneau quotient :

$$A = \mathbb{F}_p[X]/(X^2 - 4X + 1)\mathbb{F}_p[X]$$

et posons $\alpha = \bar{X}$. On a alors $\alpha(\alpha - 4) = -1_A$ et donc : α^{-1} existe et : $\alpha + \alpha^{-1} = 4 \cdot 1_A$.

Pour m entier posons :

$$v_m = \alpha^m + \alpha^{-m}$$

ainsi $v_0 = 2 \cdot 1_A$ et $v_1 = 4 \cdot 1_A$ (on ne mettra plus 1_A désormais) ; de ce fait il vient : $v_{m+1} + v_{m-1} = 4v_m$ et alors on vérifie aisément que : $v_{2m} = \alpha^{2m} + \alpha^{-2m} = v_m^2 - 2$ ce qui entraîne : $v_{2j} = (v_{2j-1})^2 - 2$ dans A.

Montrons d'abord le :

Lemme : Dans l'anneau A : $\alpha^m + \alpha^{-m} = 2$ équivaut à $\alpha^m = 1$.

En effet, dans A, si $\alpha^m + \alpha^{-m} = 2$ cela équivaut à $(\alpha^m - 1)^2 = 0$; ainsi tout revient à prouver que si $\lambda \in A$ est tel que $\lambda^2 = 0$ alors $\lambda = 0$. Ecrivons : $\lambda = u + v\alpha$ avec $u, v \in \mathbb{F}_p$ et $\lambda^2 = 0 \Longleftrightarrow \begin{cases} u^2 = v^2 \\ v(2v + u) = 0 \end{cases}$ ce qui entraîne (sva) $u = v = 0$ *ie* $\lambda = 0$.

Le lemme étant acquis on constate que : $v_{2^{q-1}} = l_q \pmod p \cdot 1_A$ et l'hypothèse $l_{n-1} = 0 \pmod M$ entraîne, *a fortiori*, $l_{n-1} = 0 \pmod p$; de ce fait il reste :

$$v_{2^{n-2}} = 0 \text{ dans A}$$

d'où :

$$v_{2^{n-1}} = -2 \pmod p 1_A \text{ et } v_{2^n} = 2 \pmod p 1_A$$

ce qui, *via* le lemme entraîne : $\alpha_{2^n} = 1_A$ et comme $v_{2^{n-1}} = -2 \pmod p 1_A$, on a : $\alpha_{2^{n-1}} \neq 1$.

Si G est le groupe multiplicatif des éléments inversibles de l'anneau quotient A, $\alpha \in G$ et son ordre vaut : $2^n = M + 1$. Mais on a également :

$$\alpha^{p\pm 1} = 1_A$$

en effet, dans A, on a : $(\alpha - 2)^2 = 3$ et comme $3 \wedge p = 1$, $3^{p-1} = 1$, d'où : $3^{\frac{p-1}{2}} = 1$ ou $3^{\frac{p-1}{2}} = -1$ modulo p s'entend.

Notons, dans A, $\beta = \alpha - 2$ si bien que : $\alpha = \beta + 2$ et $\alpha^p = \beta^p + 2^p$ (la caractéristique de A est p...) d'où :

$$\alpha^p = \beta^p + 2$$

(car $2^{p-1} = 1 \pmod p$).

p est du type $p = 2r + 1$, d'où $\beta^p = \beta\beta^{2r} = \beta 3^r = 3^{\frac{p-1}{2}}\beta = \varepsilon\beta$.

En définitive il reste :

$$\alpha^p = 2 + \varepsilon\beta, \quad \varepsilon \in \{-1, 1\}$$

Si $\varepsilon = 1$, $\alpha^p = 2 + \beta = \alpha$, d'où : $\alpha^{p-1} = 1$.

Si $\varepsilon = -1$, $\alpha^p = 2 - \beta$ et alors :

$$\alpha^{p+1} = 2\alpha - \alpha\beta = 1$$

Bilan : $\alpha^{p\pm 1} = 1$; comme α est d'ordre $M + 1 = 2^n$, $M + 1$ doit diviser $p \pm 1$; or $M + 1 \geq p + 1$; cela fournit donc $\varepsilon = 1$ et $p + 1 = M + 1$ et ainsi $M = p$ est premier. La preuve du théorème de Lucas est complète.

Algorithmiquement le théorème de Lucas est exploitable car il a une complexité polynomiale et de ce fait, il est très efficace ; c'est la raison pour laquelle les plus grands nombres premiers connus sont des nombres de Mersenne. Actuellement on connaît 47 nombres de Mersenne qui sont premiers.

b. Application

En utilisant le théorème de Lucas, écrire un programme informatique permettant de savoir si $M = 2^n - 1$ est un nombre premier ; vérifiez vos résultats à l'aide de la liste fournie ci-après des 47 nombres premiers de Mersenne connus et indiquez jusqu'à quel stade votre ordinateur vous permet d'affirmer que $M = 2^n - 1$ est premier ; voici le tableau de 47 valeurs de n pour lesquelles on sait à ce jour que $2^n - 1$ est premier ; si m est le nombre de chiffres décimaux de l'entier $2^n - 1$ on a (sva) :

$$n\frac{\log 2}{\log 10} \leq m < 1 + n\frac{\log 2}{\log 10}$$

d'où le tableau suivant :

n	m	n	m
2		110 503	33 265
3		132 049	
5		216 091	
7		756 839	
13	4	859 433	258 716
17		1 257 787	
19		1 398 269	
31		2 976 221	
61		3 021 377	
89		6 972 593	
107		13 466 917	4 053 946
127	39	20 996 011	6 320 430
521	157	24 036 583	7 235 732
607		25 964 951	7 816 230
1279		30 402 457	9 152 052
2203		32 582 657	9 808 358
2281		37 156 667	11 185 272
3217		42 643 801	12 837 061
4253		43 112 609	12 978 189
4423			
9689			
9941			
11 213			
19 937			
21 701			
23 209			
44 497			
86 243	25 962		

Le lecteur curieux complètera le tableau donnant les valeurs de l'entier m ; l'entier $n = 127$, correspondant au nombre de Mersenne $2^{127} - 1$ fut pendant près d'un siècle (de 1876 à 1952) le plus grand nombre premier connu (découvert par Lucas) ; puis l'ordinateur s'en est mêlé et sa puissance jointe au théorème de Lucas a permis d'en arriver à ce fameux :

$$2^{43\ 112\ 609} - 1$$

qui est le plus grand nombre premier connu ; d'ailleurs dans le top 10 des 10 plus grands nombres premier connus, les 9 plus grands sont des nombres de Mersenne.

Remarques :

R_1 Toujours à propos des nombres du type : $M = 2^n - 1$ avec n premier (nombre de Mersenne). Soit p un facteur premier de M ; on a : $2^n = 1 \pmod{p}$; comme n est

premier l'ordre de $\bar{2}$ dans $\mathbb{F}_p^*$ est égal à n ; or : $2^{p-1} = 1 \pmod p$; donc :

$$p = 1 \pmod n \; ie \; : \; p = 1 + qn$$

En faisant varier q cela permet de déterminer, si n n'est pas trop grand, les facteurs premiers de M.

R_2

Soit M un nombre de Mersenne premier,

$$M = 2^n - 1 \text{ avec } M \geq 5$$

Alors $\left(\frac{3}{M}\right) = -1$ *ie* : $3^{\frac{M-1}{2}} = -1 \pmod M$.

Démonstration : En utilisant la formule : $\left(\frac{3}{M}\right) = -\left(\frac{M}{3}\right)$ puisque $M = -1 = 3 \pmod 4$ on obtient :

$$\left(\frac{3}{M}\right) = -\left(\frac{-2}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

ce qui fournit bien :

$$3^{\frac{M-1}{2}} = -1 \pmod M$$

et revient à dire que 3 n'est pas un carré modulo M lorsque le nombre de Mersenne M est premier.

R_3 Soit n un nombre premier impair et $M = 2^n - 1$ le nombre de Mersenne associé et p un facteur premier de M. Comme $2^n = 1 \pmod p$, n divise $p - 1$ (ordre de $\bar{2}$ dans $\mathbb{F}_p^*$) d'où : $p - 1 = 2nn'$; ainsi :

$$2^{\frac{p-1}{2}} = 2^{nn'} = 1 \pmod p$$

ce qui impose, d'après la loi de réciprocité concernant le symbole de Legendre, $p = \pm 1 \pmod 8$.

D'où le résultat :

Proposition 9 bis : Si n est un nombre premier impair et si m est un entier divisant le nombre de Mersenne $M = 2^n - 1$, l'entier m est égal à ± 1 modulo 8.

En effet c'est vrai pour chacun des facteurs premiers de m et cela "détermine" en quelque sorte la forme des facteurs des nombres de Mersenne : $M = 2^n - 1$, $n \geq 3$ premier, qui ne sont pas premiers.

R_4 On a aussi le résultat suivant :

Proposition 9 ter : Soit n un nombre premier et $M = 2^n - 1$; on suppose $n = 3 \pmod 4$, et que $2n + 1$ est aussi un nombre premier ; alors le nombre de Mersenne est divisible par $2n + 1$.

Démonstration : En effet $2n+1 = -1 \pmod 8$ et on sait qu'alors (voir le chapitre **5**) $\left(\frac{2}{2n+1}\right) = 2^n = 1 \pmod{(2n+1)}$ ce qui veut dire que $2^n - 1$ *ie* M est divisible par $2n+1$; nous invitons le lecteur curieux à étudier la réciproque.

Pour terminer juste quelques mots sur ce qu'on appelle les nombres parfaits qui ont (selon les spécialistes) motivé l'étude des nombres de Mersenne premiers.

Définition : n est dit parfait *si et seulement si* :

$$n = \sum_{\substack{d|n \\ 1\leq d<n}} d$$

On constate très facilement que si q est un entier tel que $2^q - 1$ est premier, alors le nombre $n = 2^{q-1}(2^q - 1)$ est parfait ; Euler a montré que tout nombre pair et parfait s'écrit sous la forme précédente.

On n'a pas encore trouvé de parfait impair et même on ne sait pas s'il en existe ; cependant on voit bien tout l'intérêt de la connaissance des nombres de Mersenne qui sont premiers pour l'étude des nombres parfaits.

6.9 Un exemple d'utilisation d'un nombre de Mersenne en cryptographie

a. Rappels mathématiques

Soit p un nombre premier et $\mathbb{K}$ un corps ayant $q = p^r$ éléments. Soit n un nombre premier ; pour x et y de $\mathbb{K}^n$ avec : $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1})$ on désigne par $x * y$ l'élément de $\mathbb{K}^n$ défini par :

$$(x*y)_k = \sum_{\substack{i+j=k \pmod n \\ 0\leq i,j\leq n-1}} x_i y_j$$

pour tout $k = 0, 1, 2, \ldots, n-1$. $*$ est le produit de convolution dans $\mathbb{K}^n$ et le couple $(\mathbb{K}^n, *)$ est un monoïde commutatif (voir le chapitre **1**) ; de plus : si F est la matrice de Frobénius de taille n sur $\mathbb{K}$ *ie* : $\left(F = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 1 & 0 & 0 & & 0 \end{pmatrix}\right)$ et si, pour tout $x = (x_0, x_1, \ldots, x_{n-1})$ de $\mathbb{K}^n$, $A(x)$ est la matrice définie par :

$A(x) = \sum_{i=0}^{n-1} x_i F^i$ on vérifie aisément que l'on a : $A(x*y) = A(x)A(y)$ pour tous x, y de $\mathbb{K}^n$.
Soit alors G l'ensemble des x de $\mathbb{K}^n$ vérifiant : $\det A(x) = 1$; le couple $(G, *)$ est un groupe abélien et : si de plus, $q \pmod n$ est un générateur du groupe multiplicatif du corps $\mathbb{F}_n$, alors le groupe $(G, *)$ est cyclique et possède : $q^{n-1} - 1$ éléments (voir le chapitre **7**, paragraphe **7**).

Des applications cryptographiques :

(i) On prend, dans cet exemple, $p = q = 2$ et $n = 509$. Comme : $509 = 5 \pmod 8$ la loi de réciprocité quadratique montre que : $\left(\frac{2}{n}\right) = -1$ *ie* : $2^{\frac{n-1}{2}} = 2^{254} = -1 \pmod{509}$.

Par conséquent $\bar{2}$ est d'ordre 508 dans le groupe $(\mathbb{F}_n^*, \times)$ et de ce fait le groupe surface $(G, *)$ associé est cyclique et possède $2^{508} - 1$ éléments.

Soit α un générateur de $(G, *)$ et $\beta = \alpha^a \in G$; a est le logarithme discret de β en base α.

On peut donc crypter dans $\mathbb{K}^n = \mathbb{F}_2^n$, à la mode "El-Gamal", (voir le chapitre **7**) en posant pour $x \in \mathbb{K}^n$:

$$e(x) = (y, z) \in G \times \mathbb{K}^n \text{ où } \begin{cases} y = \alpha^k, k \in \mathbb{N}^* \text{ quelconque choisi} \\ \text{par l'expéditeur du message } x \\ z = \beta^k * x \end{cases}$$

Pour décoder il suffit de poser :

$$d(y, z) = y^{-a} * z = (y^{-1})^a * z = x$$

Afin que la sécurité d'un tel cryptosystème soit assurée, il est nécessaire que les algorithmes de Shanks et Pohlig permettant de déterminer la partie a de la clé (seule connue du destinataire des messages $x \in \mathbb{K}^n$) soient inopérants (voir le chapitre **7**). Ce but est atteint lorsque le cardinal de G possède un "grand" facteur premier.

Or ici : $\#G = (2^{508} - 1) = (2^{127} - 1)(2^{127} + 1)(2^{254} + 1)$ et, comme : $2^{127} - 1$ est un nombre de Mersenne premier (et célébrissime) ayant 39 chiffres dans son écriture décimale, la sécurité du cryptosystème est assurée.

(ii) Le groupe cyclique $(G, *)$ ainsi obtenu permet aussi (puisque la recherche du logarithme discret est difficile) de réaliser un échange de clé selon le protocole de Diffie-Hellman (voir le chapitre **7**).

La clé à échanger est ici un élément de $\mathbb{K}^n = \mathbb{F}_2^n$; soit α un générateur (public) du groupe $(G, *)$.

Alice et Bob voulant échanger un élément de $\mathbb{F}_2^n$ vont procéder de la façon suivante :

(a) Alice (*resp.* Bob) choisit un entier quelconque a (*resp.* b) et calcule α^a (*resp.* α^b) dans le groupe $(G, *)$.

(b) Alice envoie α^a à Bob qui, lui, envoie α^b à Alice.

(c) Alice calcule $k = (\alpha^b)^a$ dans $(G, *)$ et obtient la même clé que Bob lorsqu'il détermine $(\alpha^a)^b$.

Remarques :

(a) Pour ce qui concerne le codage, il concerne, chaque fois, un flot binaire de 509 bits. Autrement dit, il permet de coder tout nombre entier ayant jusqu'à 154 chiffres décimaux, puisque : $2^{509} - 1 = \sum_{i=0}^{508} 2^i$ est un entier possédant 154 chiffres décimaux, et on a :

$$2^{509} - 1 = 167\ 597\ 599\ 124\ 28 \cdots 1$$

l'expression décimale intégrale de ce nombre de Mersenne étant laissée aux soins du lecteur.

(b) En outre : $card\ \mathbb{K}^n = card\ G + card\ G_0$ où :

$$G_0 = \{x \in \mathbb{K}^n : \det A(x) = 0\}$$

comme $card\ G = 2^{n-1} - 1$ il en résulte que : $card\ G_0 = 2^{n-1} + 1$.

Or, comme on peut le montrer aisément (voir le chapitre **7**, paragraphe **7**), G_0 contient l'hyperplan de $\mathbb{K}^n$ d'équation : $x_0 + x_1 + \cdots + x_{n-1}$ et le vecteur $(1, 1, \ldots, 1)$; en définitive la cardinalité de G_0 impose :

$$\det A(x) = 0 \Longleftrightarrow \begin{cases} x_0 + x_1 + \cdots + x_{n-1} = 0 \\ \text{ou} \\ x = (1, 1, \ldots, 1) \end{cases}$$

Ce qui permet d'obtenir aisément tous les éléments de G, et de trouver "rapidement" un générateur du groupe $(G, *)$; le lecteur curieux exploitera, s'il le souhaite, la conclusion de **6.12**.

6.10 Les nombres de Fermat et leurs diviseurs premiers

a. Une remarque

Proposition 10 : Soit $a \geq 2$, $a \in \mathbb{N}$ et $n \geq 1$ un entier ; si l'entier $b = a^n + 1$ est premier, alors n est une puissance de 2.

Démonstration : En effet si $n = 2m + 1$ on peut écrire :

$$b = a^{2m+1} - (-1)^{2m+1} = (a + 1)(a^{2m} + \cdots + 1)$$

De ce fait $b = a^{2n'} + 1 = (a^2)^{n'} + 1$, et encore une fois n' est pair ; et ainsi de suite... d'où la proposition 10.

Les nombres $F_n = 2^{2^n} + 1$ sont dits *nombres de Fermat*. Actuellement seuls : $F_0 = 3, F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\ 537$ sont connus comme étant premiers et peut être n'y en a-t-il pas d'autres... ?

b. Quelques propriétés des nombres de Fermat

P_1 : si $n \neq m$, $F_n \wedge F_m = 1$

En effet supposons $m = n + k$ et soit p premier divisant F_n et F_m. On a :

$$\begin{cases} \bar{2}^{2^n} = -\bar{1} \text{ dans } \mathbb{F}_p \\ \text{et} \\ \bar{2}^{2^m} = -\bar{1} \text{ dans } \mathbb{F}_p \end{cases}$$

or $\bar{2}^{2^m} = \left(\bar{2}^{2^n}\right)^{2^k} = (-1)^{2^k} = 1 \pmod{p}$ ce qui est impossible car $p \neq 2$; ainsi on retrouve qu'il y a une infinité de nombres premiers (le lecteur est invité à revoir le paragraphe **6.2** de ce chapitre).

P_2 : Soit p premier, p divisant F_n ; alors $p = 1 \pmod{2^{n+2}}$

En effet dans $(\mathbb{F}_p^*, \times)$, $\bar{2}^{2^{n+1}} = \bar{1}$ et $\bar{2}^{2^n} = -\bar{1}$; donc l'ordre de $\bar{2}$ dans $\mathbb{F}_p^*$ est égal à 2^{n+1} ; comme $\bar{2}^{p-1} = \bar{1}$ alors $p - 1 = 0 \pmod{2^{n+1}}$ d'où $p = 1 \pmod 8$; la formule $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ montre que $\left(\frac{2}{p}\right) = 1$ *ie* que dans $\mathbb{F}_p$, $\bar{2}$ est un carré ; ainsi :

$$\bar{2}^{\frac{p-1}{2}} = \bar{1}$$

dans $\mathbb{F}_p$ et alors : $p = 1 \pmod{2^{n+2}}$ comme annoncé.

Applications : $F_5 = 2^{32} + 1$; les p premiers égaux à $1 \pmod{128}$ sont : $p = 129, p = 257$ (à exclure car ici $p = F_3 \wedge F_5$), $p = 641$.... et on trouve que 641 divise F_5 d'où :

$$F_5 = 641 \times 6\ 700\ 417$$

Ecrire un programme pour F_6 et trouver la décomposition primaire :

$$F_6 = 274\ 177 \times 67\ 280\ 421\ 310\ 721$$

P_3 : Soit $F_n = 2^{2^n} + 1$ un nombre de Fermat. F_n est premier *si et seulement si* $3^{\left(2^{(2^n-1)}\right)} = -1 \pmod{F_n}$.

Démonstration de ce critère de primalité :

On a : $F_n = 2 \pmod 3$ et $F_n = 1 \pmod 4$; donc d'après le lemme chinois, $F_n = 5 \pmod{12}$. Pour pouvoir continuer on va utiliser le lemme suivant :

> Lemme : Si p est premier et si $p = 5 \pmod{12}$ alors : $3^{\frac{p-1}{2}} = -1 \pmod p$.

En effet comme $p = 1$ modulo 4 la formule "résiduelle" $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ est valable et de ce fait :

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$$

ce qui prouve bien $3^{\frac{p-1}{2}} = -1 \pmod p$.

Or ici si $p = 2^{2^n} + 1$ est premier, $\frac{p-1}{2} = \frac{1}{2}2^{2^n} = 2^{2^n-1}$.

Réciproquement, supposons avec $p = 2^{2^n} + 1$, que l'on a : $3^{\frac{p-1}{2}} = -1 \pmod{p = 2^{2^n} + 1}$ et montrons qu'alors le nombre de Fermat $2^{2^n} + 1$ est un nombre premier ; en effet : soit G le groupe des inversibles de l'anneau $\mathbb{Z}/p\mathbb{Z}$; $\bar{3}$ est dans ce groupe et l'ordre de $\bar{3}$ est précisément $p - 1$; donc p est premier.

c. Un exercice à effectuer *via* l'ordinateur

(i) Vérifiez, en utilisant l'algorithme de Miller-Rabin ou celui de Solovay-Strassen, que les quatre nombres suivants sont "premiers" : $p_1 = 319\,489$; $p_2 = 974\,849$; $p_3 = 167\,988\,556\,341\,760\,475\,137$; $p_4 = 3\,560\,841\,906\,445\,833\,920\,513$.

(ii) Calculer, en utilisant l'algorithme d'exponentiation rapide :

$$2^{2048} \pmod{p_i}$$

pour $i = 1, 2, 3, 4$. Qu'en résulte-t-il ?

Remarque : On montrera que les p_i sont premiers en utilisant les propositions établies dans le paragraphe **7** de ce chapitre.

6.11 Propriétés congruentielles identiques liant certains facteurs premiers des nombres de Mersenne et des nombres de Fermat

L'une d'entre elles peut s'énoncer de la façon suivante :

Proposition 11 : Si p est un nombre premier et si p^2 divise un nombre de Fermat (*resp.* un nombre de Mersenne) alors $2^{p-1} = 1 \pmod{p^2}$.

Démonstration : Supposons que l'entier premier p divise $F_n = 2^{2^n} + 1$ et qu'il en soit de même pour l'entier p^2 ; on a donc :

$$2^{2^n} = -1 \pmod{p^2}$$

et en élevant au carré il reste :

$$2^{2^{n+1}} = 1 \pmod{p^2}$$

si G_{p^2} désigne le groupe des inversibles de l'anneau $\mathbb{Z}/(p^2)$, $\bar{2}$ est d'ordre 2^{n+1} dans G_{p^2} ; mais on sait (proposition 8 du chapitre **3**) que G_{p^2} est un groupe cyclique dont le cardinal est égal à : $p(p-1)$; il en résulte que l'entier 2^{n+1} divise $p(p-1)$ et comme p est premier ($p \geq 3$) $p - 1$ est un multiple de 2^{n+1} ; si on écrit :

$$p - 1 = k2^{n+1}$$

il vient alors :

$$2^{p-1} = \left(2^{2^{n+1}}\right)^k = 1 \pmod{p^2}$$

comme annoncé.

La même congruence reste valable si p premier est tel que p^2 divise un nombre de Mersenne mais elle est bien plus difficile à prouver ; c'est la raison pour laquelle le lecteur est prié de consulter (s'il le désire) des ouvrages bien plus savants que celui-ci car, à ma connaissance, l'existence d'un nombre de Mersenne admettant un facteur carré reste un problème ouvert tout comme d'ailleurs la même éventualité concernant les nombres de Fermat.

Cependant si on conjecture qu'il existe une infinité de nombres de Fermat ayant un facteur carré, puisque les F_n sont deux à deux premiers entre eux, il existe alors une infinité de nombres premiers vérifiant la congruence :

$$2^{p-1} = 1 \pmod{p^2}$$

D'ailleurs un tel entier p premier est appelé *entier de Wieferich* et il est "bien connu" que cette congruence est extrêmement rare, et, sans aucune certitude, je crois que les deux plus petits entiers de Wieferich sont : $p_1 = 1093$ et $p_2 = 3511$; d'ailleurs le lecteur est invité à vérifier, *via* l'ordinateur et l'algorithme d'exponentiation modulaire, que l'on a bien :

$$2^{1092} = 1 \pmod{(1093)^2}$$
$$2^{3510} = 1 \pmod{(3511)^2}$$

Plus généralement, étant donné un entier a au moins égal à 2, l'existence de nombres premiers p vérifiant $a^{p-1} = 1 \pmod{p^2}$ est (et reste) un problème très difficile ; à titre d'exemple écrire un programme informatique lorsqu'on prend $a = 19$, et chercher les entiers p premiers, $p \leq 200$, tels que : $a^{p-1} = 1 \pmod{p^2}$ et constater que l'ensemble de ces entiers est $\{3, 7, 13, 43, 137\}$.

6.12 Développement asymptotique de la fonction : $x \to \sum_{\substack{p \ premier \\ p \leq x}} 1/p$ au voisinage de $+\infty$ - Applications

a. Posons $f(x) = \sum_{\substack{p \ premier \\ p \leq x}} 1/p$; cette fonction peut "s'estimer" au voisinage de $+\infty$ $\underset{x \geq 2}{}$ grâce à la formule sommatoire d'Abel, mais le lecteur pourra le constater, cette formule n'a aucun "contenu" arithmétique : elle peut s'énoncer de la façon suivante :

Proposition 12 : Si h est une application $\mathcal{C}^1$ de $[1, +\infty[$ dans $\mathbb{C}$ et si $u = (u_n)_{n \geq 1}$ est une suite de nombres complexes, on a l'égalité :

$$\sum_{1 \leq n \leq x} u_n h(n) = U(x)h(x) - \int_1^x U(t)h'(t)dt$$

où : $\begin{cases} U(x) = \sum_{1 \leq n \leq x} u_n \\ \forall x \geq 1 \end{cases}$

Démonstration : En effet on pose $V_n = u_1+u_2+\cdots+u_n$ et on écrit pour $x \in [n, n+1[$:

$$\begin{aligned}\int_1^x U(t)h'(t)dt &= \sum_{k=1}^{n-1}\int_k^{k+1} U(t)h'(t)dt + \int_n^x U(t)h'(t)dt\\ &= \sum_{k=1}^{n-1} V_k(h(k+1)-h(k)) + V_n(h(x)-h(n))\\ &= \sum_{k=2}^{n} h(k)V_{k-1} - \sum_{k=1}^{n-1} h(k)V_k + U(x)h(x) - V_n h(n)\\ &= -\sum_{k=2}^{n-1} h(k)u_k - u_1 h(1) + h(n)(V_{n-1}-V_n) + U(x)h(x)\end{aligned}$$

ce qui est la formule attendue (obtenue d'ailleurs grâce à une transformation d'Abel, si usuelle en spé MP*...).

Ceci étant acquis si on écrit pour $x \geq 2$:

$$f(x) = \frac{1}{2} + \sum_{\substack{\text{p premier}\\ 2<p\leq x}} 1/p = \frac{1}{2} + \sum_{\substack{p \text{ premier}\\ p\leq x}} \log(p)/p\frac{1}{\log(p)}$$

avec log désignant le logarithme népérien, en prenant $u_n = \frac{\log(n)}{n}$ et $h(x) = \frac{1}{\log(x)}$ pour $x \geq 2$ on a :

$$f(x) = \frac{1}{2} + \sum_{\substack{p \text{ premier}\\ 2<p\leq x}} u_p h(p)$$

ce qui fournit grâce à la formule sommatoire d'Abel précédemment établie :

$$f(x) = \frac{U(x)}{\log x} + \int_2^x \frac{U(t)}{t(\log t)^2}dt$$

avec, ici :

$$U(x) = \sum_{\substack{p \text{ premier}\\ 1\leq p\leq x}} \frac{\log p}{p}$$

On a alors besoin du lemme suivant (dont le preuve est laissée aux soins du lecteur) :

Lemme :

$$\sum_{\substack{p \text{ premier}\\ 1\leq p\leq x}} \frac{\log p}{p} \underset{\infty}{=} \log(x) + \mathcal{O}(1)$$

Ceci étant, on peut alors écrire :

$$f(x) = 1 + \frac{\mathcal{O}(1)}{\log x} + \int_2^x \frac{dt}{t(logt)} + \int_2^x \frac{\theta(t)}{t(\log t)^2}dt$$

avec θ bornée sur $[2, +\infty[$. Ainsi :

$$f(x) = 1 + \frac{\mathcal{O}(1)}{\log x} + \log(\log x) - \log(\log 2) + \int_2^{\infty} \frac{\theta(t)}{t(\log t)^2} dt + o(1)$$

ce qui nous prouve ce que nous voulions et :

$$C = 1 - \log(\log 2) + \int_2^{\infty} \frac{\theta(t)}{t(\log t)^2} dt \ \# \ 0.261...$$

b. Application : On a vu que **a.** permet de montrer l'existence de $\alpha > 0$ tel que $\varphi(n) \geq \frac{\alpha n}{\log n}$ (chapitre **3**, paragraphe 3) ; en fait on a mieux car :

$$\liminf_{\infty} \left(\frac{\varphi(n)}{n} (\log(\log n)) \right) = e^{-\gamma}$$

où γ est la constante d'Euler. Or : $e^{-\gamma} = 0.561459484073059...$ ce qui veut dire que (par exemple) pour tout entier n assez grand on a :

$$\varphi(n) \geq \frac{0.56 \cdot n}{\log(\log n)};$$

à titre d'exploitation numérique, dans l'appendice consacré au TIPE d'un élève admis à l'ENS Lyon, on dispose d'un groupe cyclique G ayant environ $6 \cdot 10^{86}$ éléments ; par application de l'inégalité précédente on obtient (calcul facile) : $\varphi(n) > 6 \cdot 10^{85}$; ainsi on peut dire que dans le groupe $(G, *)$ utilisé, il y a plus de $6 \cdot 10^{85}$ générateurs et en choisissant "au hasard" un élément de G, on dispose au moins d'une chance sur 10 d'obtenir un générateur de G.

De façon générale, si p est un nombre premier et si $(G, *)$ est un groupe cyclique ayant $p^{n-1} - 1$ éléments (voir chapitre **7**, paragraphe 7) la probabilité pour qu'en choisissant "au hasard" un élément de G on dispose d'un générateur, est au moins égale (si p et n sont bien choisis) à :

$$\frac{0.56}{\log(n-1) + \log(\log p)}$$

c'est ainsi que, pour l'exemple décrit en **7.7.4** avec : $n = 23$ et $p = 5297$ on obtient, à nouveau, une probabilité supérieure à 0.1.

En pratique, après au plus dix essais à partir d'un élément du groupe, on est "presque certain" d'obtenir un générateur du groupe considéré.

Chapitre 7

Arithmétique modulaire et cryptologie

7.1 Les grands systèmes cryptographiques

7.1.1 Introduction

a. Des définitions

Commençons par rappeler que la *cryptologie* est constituée par l'ensemble des sciences des écritures secrètes, des documents chiffrés, la *cryptographie* en constituant un sous-ensemble dont le but est, grâce à un procédé technique de codage (on dit aussi d'encodage), de rendre un message indéchiffrable à toute personne autre que son émetteur ou son destinataire.

Pratiquement tout message à transmettre est numérisé selon un protocole partagé par l'émetteur du message ainsi que par le (ou les) destinataire(s) du courrier ; c'est la raison pour laquelle, dans tout ce qui suit, un message est très souvent constitué par une liste de nombres entiers...

Dans un premier temps nous allons nous intéresser à la cryptographie et chercher quelles sont les techniques mathématiques dans lesquelles il est possible d'introduire un "mécanisme" de secret.

Exemple : Le protocole d'échange de Diffie-Hellman.

Soit $(G, \bullet)$ un groupe cyclique et α un générateur de G ; désignons par A et B deux correspondants ; ils peuvent partager un "secret" commun en procédant de la façon suivante :

- A choisit un entier a (secret), calcule $\beta = \alpha^a$ et transmet β à B.
- B choisit un entier b (secret), calcule $\beta' = \alpha^b$ et transmet β' à A.

Comme $\beta^b = \beta'^a$ cet élément de G constitue un secret partagé par A et B.

Dès qu'un tel mécanisme est opérationnel alors, bien naturellement, on cherche des protocoles mathématiques permettant de "casser" la technique cryptographique en question ; c'est le but de la *cryptanalyse* qui est, par définition, l'ensemble des procédés

scientifiques visant à casser tout système bâti autour de la notion de codage secret ; la cryptanalyse n'a été que très peu envisagée dans ce livre. Ce que nous avons fait dans cet ouvrage en arithmétique modulaire va nous permettre, comme la suite permet de le constater, de créer des *cryptosystèmes*, c'est-à-dire des procédés mathématiques de "transports sécurisés" d'information.

b. Notion de fonction à sens unique ("one way - function")

Si f est une application d'un ensemble E dans un ensemble E' on dit que f est une fonction *à sens unique* si connaissant $y = f(x)$ il est "pratiquement" impossible, en un temps raisonnable, de déterminer x, à partir des capacités mathématiques et informatiques valables actuellement.

Afin d'illustrer tout l'intérêt de cette notion donnons l'exemple suivant. Supposons disposer d'un réseau informatique pourvu d'un disque mémoire et à partir duquel on peut utiliser n logiciels $L_1, L_2, \ldots, L_n$; soit f une fonction à sens unique d'un ensemble E dans un ensemble E' ; à chaque logiciel associons un élément $y_i = f(x_i)$; les éléments $y_1, y_2, \ldots, y_n$ figurant en mémoire tandis que les éléments $x_1, x_2, \ldots, x_n$ de E sont maintenus secrets et connus uniquement des utilisateurs (autorisés) de ces logiciels.

Lorsqu'on veut utiliser le logiciel L_i il est alors demandé le code d'accès (ou mot de passe, si l'on veut) c'est-à-dire l'élément x_i de E ; comme le logiciel contient la fonction f il lui est facile de vérifier si x est le code d'accès fourni, que $f(x) = y_i$ et autoriser l'utilisation du logiciel L_i ; dans le cas contraire, *ie* si $x \in E$ est un mauvais code d'accès, il y a refus.

N'importe quel intrus capable de lire le disque mémoire obtiendra aisément les y_i, $i = 1, 2, \ldots, n$, mais comme f est réputée à sens unique, il lui est impossible de déterminer les "mots de passe" $x_1, x_2, \ldots, x_n$ dans un temps raisonnable et par voie de conséquence de se servir des logiciels $L_1, L_2, \ldots, L_n$.

c. Les principales fonctions à sens unique en cryptographie

(i) Désignons par $\mathcal{P}$ l'ensemble des nombres premiers ; alors l'application :

$$(p, q) \in \mathcal{P} \times \mathcal{P} \longrightarrow p \cdot q \in \mathbb{N}$$

est une fonction à sens unique dès lors que p et q sont choisis suffisamment grands et distincts ; en d'autres termes si p et q sont des entiers premiers distincts $(p, q \geq 2^{256})$ et si on connaît uniquement le produit $n = pq$, il est "actuellement" difficile de déterminer les entiers p et q ; le cryptosystème RSA détaillé plus loin est basé sur cette observation.

(ii) Soit p un "grand" nombre premier ; le corps de Frobénius $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est tel que $(\mathbb{F}_p^*, \times)$ est cyclique ; si on désigne par α un générateur du groupe multiplicatif $\mathbb{F}_p^*$ *ie* une racine $(p-1)$-ième primitive de l'unité modulo p, l'application de $\mathbb{N}^*$ dans $\mathbb{F}_p^*$ définie par :

$$f(x) = \alpha^x$$

est une fonction à sens unique.
Autrement dit si $\beta = \alpha^x$ est connu dans $\mathbb{F}_p^*$ il est "calculatoirement" difficile de déterminer l'entier x défini modulo $p-1$; on note alors :

$$x = \log_\alpha \beta \text{ (logarithme discret de } \beta \text{ en base } \alpha)$$

Le cryptosystème El-Gamal, ainsi que sa variante sur une courbe elliptique, sont basés sur cette remarque, même s'il existe des techniques cryptanalytiques ayant pour but de casser ces cryptosystèmes, comme nous le verrons dans cet ouvrage (algorithme de Shanks, et algorithme de Pohlig-Hellman).

(iii) Si p est un "grand" nombre premier l'application : $x \in \mathbb{F}_p \longrightarrow x^2 \in \mathbb{F}_p$ est aussi une fonction "difficile à inverser" car, s'il est facile, grâce à l'utilisation de la loi de réciprocité quadratique (voir le chapitre **5** de cet ouvrage) de vérifier que $a \in \mathbb{F}_p$ est un résidu quadratique, il est par contre, beaucoup plus mal aisé de déterminer b modulo p tel que $b^2 = a$ (pseudo-cryptosystème de Rabin).

7.1.2 Les systèmes cryptographiques à clé publique

a. Instance du problème

Une entité physique ou administrative souhaite pouvoir recevoir des informations (messages) de la part de divers expéditeurs dûment identifiés, ces informations devant circuler sous le sceau du secret, seul le destinataire étant capable de les déchiffrer. Pour résoudre techniquement la situation ainsi décrite on a recours à la *cryptographie à clé publique* ; c'est ainsi que le destinataire des messages va créer un "cryptosystème à clé publique" utilisable par n'importe quel expéditeur et permettant de sécuriser le transport d'information jusqu'à lui, seul apte à pouvoir décoder les messages reçus

b. Définition d'un cryptosystème à clé publique

Définition On appelle *système cryptographique à clé publique* tout quintuplet

$$(K, E, E', e, d)$$

où :

(i) K est une liste finie de paramètres mathématiques constituant ce qu'on appelle la *clé* du cryptosystème et nécessaire à son élaboration ; certains éléments de la clé sont publics et par conséquent à la disposition de tout expéditeur de message, les autres étant secrets, c'est-à-dire connus uniquement du destinataire des informations et propriétaire de la clé K.

(ii) E est l'ensemble des messages ou encore des textes à chiffrer (coder).

(iii) E' est un ensemble dit ensemble des textes codés (chiffrés).

(iv) e est une application de E dans E' appelée *fonction de codage* (ou de chiffrement) "calculable" par tout expéditeur à l'aide des éléments publics de la clé K.

(v) d est une application de E' dans E telle que :

$$\forall x \in E, d(e(x)) = x$$

appelée *fonction de déchiffrement* (décodage) et seulement "calculable" par le destinataire grâce aux paramètres maintenus secrets de la clé K de son cryptosystème.

La sécurité d'un tel protocole réside, bien naturellement, dans le fait que si un intrus peut intercepter $y = e(x)$ il lui est impossible, en un temps raisonnable, de déterminer x, c'est-à-dire le message envoyé par l'expéditeur ; bien évidemment la fonction e est injective, mais doit être, comme nous l'avons souligné précédemment "à sens unique"...

Remarque importante : La clé du cryptosystème est parfois suffisamment élaborée pour qu'il existe plusieurs fonctions d'encodage admettant la même inverse à gauche d ; l'expéditeur des messages est donc libre d'utiliser la fonction de chiffrement de son choix parmi toutes celles qui sont possibles ; on dit alors que le chiffrement est *probabiliste*.

7.1.3 Etude d'un exemple : le cryptosystème de Merkle-Hellman

Commençons d'abord par donner la définition suivante :

Définition : Une suite d'entiers $(u_1, u_2, \ldots, u_n)$ est dite *supercroissante* si pour tout $i = 2, 3, \ldots, n$ on a :

$$u_i > u_1 + u_2 + \cdots + u_{i-1}$$

Alors si tel est le cas, on peut énoncer :

Proposition 1 : Si $(u_1, u_2, \ldots, u_n)$ est une suite de longueur n d'entiers supercroissante l'application e :

$$(x_1, x_2, \ldots, x_n) \in \{0,1\}^n \xrightarrow{e} \sum_{i=1}^{n} u_i x_i \in \mathbb{N}$$

est injective.

Démonstration : En effet supposons : $u_1x_1 + \cdots + u_nx_n = u_1x'_1 + \cdots + u_nx'_n$ avec $x_i, x'_i \in \{0,1\}$; si, par exemple, $x_n = 1$, alors $x'_n = 1$ également, car si on suppose $x'_n = 0$ on peut écrire :

$$u_n = u_{n-1}(x'_{n-1} - x_{n-1}) + \cdots + u_1(x'_1 - x_1) > u_{n-1} + \cdots + u_1$$

(puisque la suite u_n est supercroissante) ; or :

$$\left| \sum_{k=1}^{n-1} u_k(x'_k - x_k) \right| \leq \sum_{k=1}^{n-1} u_k$$

il y a donc contradiction ; ainsi $x_n = 1$ équivaut à $x'_n = 1$ et, de proche en proche, on obtient $x_i = x'_i$ pour $i = 1, 2, \ldots, n$.

Ceci étant dit, cette fonction est facile à inverser ; en effet si on connaît y entier et si on sait qu'il existe $x \in \{0,1\}^n$ tel que $y = u(x)$, l'algorithme ci-dessous permet effectivement de déterminer x :

Pour i allant de n à 1 faire : – Si $y \geq u_i$ alors $x_i = 1$ et $y := y - u_i$ – Si $y < u_i$ alors $x_i = 0$ Fin

Ceci étant acquis, l'idée qui a prévalu dans la construction du cryptosystème de Merkle-Hellman est celle d'une fonction de codage e associée à une suite d'entiers supercroissante mais perturbée.

Or si la multiplication usuelle dans $\mathbb{N}$ conserve l'ordre (naturel) des éléments d'une suite, il n'en est plus de même lorsqu'on effectue des multiplications dans un anneau du type $\mathbb{Z}/p\mathbb{Z}$, d'où l'idée de Merkle et Hellman d'élaborer le cryptosystème décrit ci-dessous :

(i) La clé K est constituée par la liste :

$$K = (n, u, p, a, v)$$

où :
- n est un nombre entier au moins égal à 5
- u est une suite d'entiers supercroissante et de longueur n : $(u_1, u_2, \ldots, u_n)$
- p un nombre premier vérifiant l'inégalité :

$$p > u_1 + u_2 + \cdots + u_n$$

- a est un entier compris entre 2 et $p-1$
- $v = (v_1, v_2, \ldots, v_n)$ est la suite d'entiers de $\{0, 1, 2, \ldots, p-1\}$ définie par :

$$v_i = au_i \pmod{p}$$

p, u et a sont secrets, n et v sont publics.

(ii) E est $\mathbb{F}_2^n$ c'est-à-dire l'ensemble des flots binaires de longueur n.

(iii) E' est l'ensemble des entiers compris entre 0 et $n(p-1)$.

(iv) e est la fonction définie par :

$$e(x_1, x_2, \ldots, x_n) = v_1x_1 + v_2x_2 + \cdots + v_nx_n = y$$

(la suite supercroissante u ayant été remplacée par la suite superperturbée v)

(v) La fonction d de décodage est alors élaborée selon le protocole décrit ci-dessous :

(a) Le destinataire reçoit $y = v_1x_1 + \cdots + v_nx_n$; il détermine alors l'unique entier z de $\{0, 1, \ldots, p-1\}$ tel que $z = a^{-1} \cdot y$ modulo p ; ainsi :

$$z = (a^{-1}v_1x_1) \pmod{p} + \cdots + (a^{-1}v_nx_n) \pmod{p}$$

ce qui fournit :

$$z = u_1x_1 + u_2x_2 + \cdots u_nx_n$$

(b) Afin de décoder le flot binaire expédié $(x_1, x_2, \ldots, x_n)$ le destinataire utilise alors l'algorithme précédent que nous indiquons à nouveau :

Pour i allant de n à 1 faire : – Si $z \geq u_i$ alors $x_i = 1$ et $z := z - u_i$ – Si $z < u_i$ alors $x_i = 0$ Fin

Remarque : L'idée "très séduisante" de la perturbation de l'ordre par la multiplication modulaire n'a malheureusement pas suffit puisque la cryptanalyse en est venu à bout et a réussi à le "casser".

7.1.4 Deux grands cryptosystèmes basés sur la factorisation : le RSA et le cryptosystème de Rabin

a. Le cryptosystème RSA

Sa clé est constituée par la liste $K = (n, p, q, a, b)$ où :
- p et q sont deux nombres premiers distincts du même ordre de grandeur (environ 256 bits) et $n = pq$.
- a et b sont deux entiers de l'ensemble $\{1, 2, \ldots, n\}$ vérifiant $ab = 1 \pmod{[\varphi(n)]}$ où φ est l'indicateur d'Euler.

La partie publique de la clé est constituée par n et a ; p, q et b sont tenus secrets par le propriétaire de la clé qui calculant $\varphi(n) = (p-1)(q-1)$ peut, grâce à l'algorithme d'Euclide étendu, ayant fixé $a \in \{1, \ldots, n\}$ premier avec $\varphi(n)$, déterminer l'entier b tel que :

$$ab = 1 \pmod{[\varphi(n)]}$$

L'ensemble E des messages coïncide, tout comme E', avec l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$. La fonction de codage e est alors définie par :

$$e(\bar{x}) = \bar{x}^a \pmod{n}$$

pour tout $\bar{x} \in \{\bar{0}, \bar{1}, \ldots, \bar{n}\}$. Alors on peut écrire :

Proposition 2 : Pour tout $\bar{x} \in E, e(\bar{x})^b = \bar{x}$; en d'autres termes la fonction de déchiffrement est celle définie sur $\mathbb{Z}/n\mathbb{Z}$ par $d(\bar{x}) = \bar{x}^b$.

Démonstration : Il s'agit de prouver que $\bar{x}^{ab} = \bar{x} \pmod{n}$, ou ce qui revient au même, que c'est vrai modulo p et modulo q ; en effet :
- si $\bar{x} = 0 \pmod{p}$ l'égalité est vraie modulo p
- sinon $\bar{x}$ est inversible dans le corps de Frobénius $\mathbb{F}_p$ et on a : $\bar{x}^{(p-1)} = \bar{1}$; comme $\varphi(n) = (p-1)(q-1)$ on a bien dans $\mathbb{F}_p$: $\bar{x}^{\varphi(n)} = \bar{1}$ et comme $ab = 1$ modulo $\varphi(n)$ il reste bien : $\bar{x}^{ab} = \bar{x}$ dans $\mathbb{F}_p$; la preuve est donc terminée.

Pratiquement pour "envoyer" le message $\bar{x}$ de $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ ou, ce qui revient au même, le message numérique $x \in \{0, 1, \ldots, n-1\}$ il suffit d'effectuer une exponentiation modulaire modulo n qui sera, bien évidemment, réalisée grâce à l'algorithme d'exponentiation rapide dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Pour "casser" éventuellement ce mode de codage il faut savoir factoriser n, car pour n très grand (200 chiffres décimaux) il est impensable de calculer $\varphi(n)$ par une méthode naïve ; or factoriser les très grands nombres, surtout lorsqu'ils sont le produit de deux nombres premiers distincts du même ordre de grandeur, reste encore difficile malgré l'existence de techniques : algorithme de Pollard, algorithme de Lenstra utilisant les courbes elliptiques, crible quadratique et crible algébrique ; le lecteur intéressé est prié de consulter les ouvrages spécialisés en la matière.

b. Le pseudo-cryptosystème de Rabin

Sa clé est le triplet $K = (n, p, q)$ où p et q sont deux entiers premiers distincts du même ordre de grandeur tous deux égaux à 3 modulo 4, et l'entier n est leur produit, *ie* :

$$n = pq$$

Seul n est public ; p et q sont secrets et seuls connus par le dépositaire de la clé K.

Les ensembles E et E' coïncident, comme pour le RSA, avec l'anneau $\mathbb{Z}/n\mathbb{Z}$ où, encore si l'on veut, avec $\{0, 1, 2, \ldots, n-1\}$.

La fonction de codage e est définie par :

$$e(\bar{x}) = \bar{x}^2 \text{ dans } \mathbb{Z}/n\mathbb{Z}$$

ou encore pour $x \in \{0, 1, \ldots, n-1\}$ par :

$$e(x) = x^2 \pmod{n}$$

avec $e(x) \in \{0, 1, \ldots, n-1\}$.

Le décodage s'effectue en procédant comme il suit : le destinataire reçoit $\bar{y} = \bar{x}^2$, à charge pour lui de trouver $\bar{x}$. Puisque p et q sont premiers et distincts, on peut trouver (par exemple en utilisant l'algorithme d'Euclide) p' et q' entiers tels que :

$$pp' + qq' = 1 \text{ (relation de Bezout)}$$

On sait que l'application :

$$\bar{x} \in \mathbb{Z}/n\mathbb{Z} \xrightarrow{f} (\bar{\bar{x}}, \bar{\bar{\bar{x}}}) \in \mathbb{F}_p \times \mathbb{F}_q$$

est un isomorphie d'anneau et que :

$$f^{-1}(\bar{\bar{t}}, \bar{\bar{\bar{t}}}) = \overline{pp't' + q'qt}$$

Pour résoudre $\bar{y} = \bar{x}^2$ dans $\mathbb{Z}/n\mathbb{Z}$ on résoudra donc $y = x^2 \pmod{p}$, puis $y = x^2 \pmod{q}$ et à l'aide de f^{-1} on en déduira x modulo n.

Dans le corps $\mathbb{F}_p$ l'équation : $y = x^2 \pmod p$ admet deux solutions opposées : z et $-z$ et si $y \neq 0$ modulo p on a, puisque $p = 3$ modulo 4 :

$$\left(y^{\frac{p+1}{4}}\right)^2 = y^{\frac{p+1}{2}} = y^{\frac{p-1}{2}} y = y = x^2 \pmod p$$

($y^{\frac{p-1}{2}} = 1$ modulo p puisque y est un carré modulo p).

Ainsi $z \in \{\pm y^{\frac{p+1}{4}}\}$ et c'est même vrai si $y = 0$ modulo p.

On fait pareil modulo q et les solutions dans $\mathbb{F}_q$ de l'équation $y = x^2$ modulo q sont $\pm u$ avec $u = y^{\frac{q+1}{4}}$ modulo q.

En utilisant la fonction f^{-1} on en déduit que dans $\mathbb{Z}/n\mathbb{Z}$:

$$\bar{x} \in \{\overline{pp'u + qq'z}, -\overline{pp'u + qq'z}, \overline{pp'u - qq'z}, -\overline{pp'u - qq'z}\}$$

il y a donc quatre messages qui se chiffrent en $\bar{y} = \bar{x}^2$, à charge pour le destinataire d'éliminer ceux qui ne sont pas bons.

En quelque sorte ce chiffrement de Rabin ne devrait pas figurer dans la rubrique des systèmes cryptographiques puisque, à l'évidence, la fonction de chiffrement n'est pas injective, c'est pourquoi nous l'avons qualifié de pseudo-cryptosystème ; par contre on a la proposition suivante :

Proposition 3 : Si $n = pq$ avec p, q premiers distincts égaux à 3 modulo 4, et si Ω_n désigne l'ensemble des résidus quadratiques modulo n l'application :

$$\bar{x} \in \Omega_n \longrightarrow \bar{x}^2 \in \Omega_n$$

est bijective.

Démonstration : Soient z et $-z$ les deux solutions modulo p de la congruence $y = z^2$, avec $y \neq 0$; une seule des deux racines, z ou $-z$, est un résidu quadratique modulo p ; en effet supposons $z^{\frac{p-1}{2}} = 1$ modulo p ; alors :

$$(-z)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} z^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = -1 \pmod p$$

puisque $\frac{p-1}{2}$ est un nombre impair.

En procédant de la même façon modulo q on voit que x modulo n est égal à $pp'u+qq'z$ où u est le résidu quadratique dans $\mathbb{F}_q$ tel que $u^2 = y$ et z est le résidu quadratique de $\mathbb{F}_p$ tel que $z^2 = y$.

C'est pourquoi, si l'on veut par la technique de Rabin créer un "vrai" cryptosystème, il faut alors se limiter au cas où $E = E'$ est constitué par l'ensemble des résidus quadratiques modulo n (le lecteur aura constaté que $x \in \{1, 2 \cdots, n\}$ est un résidu quadratique modulo n *si et seulement si* c'est à la fois un résidu quadratique modulo p et modulo q..).

En tout état de cause, et même dans le cas du "pseudo-cryptosystème" correspondant au cas où $E = \mathbb{Z}/n\mathbb{Z}$, "casser" le mode de chiffrement n'est possible que si on sait factoriser un grand nombre entier produit de deux nombres premiers du même ordre de grandeur ; la problématique est donc identique à celle de la cryptanalyse du RSA.

7.1.5 Le cryptosystème El-Gamal basé sur le logarithme discret

a. Un rappel

Soit $(G, \bullet)$ un groupe cyclique ayant m éléments et α un générateur de G ; pour tout $\beta \in G$, il existe a unique modulo m tel que $\beta = \alpha^a$; a porte le nom de *logarithme discret* de β en base α.

b. Le cryptosystème El-Gamal

Sa clé est définie par : $K = (G, \alpha, \beta, a)$ où G est un groupe cyclique, α un générateur de G, β un élément de G avec $\beta = \alpha^a$, a étant fixé modulo m où $m = card\ G$.

G, α, β sont publics ; a est tenu secret par le propriétaire de la clé K.

L'ensemble E, c'est-à-dire l'ensemble des messages à coder est le groupe G ; l'ensemble E' des messages chiffrés est $G \times G$.

C'est, comme nous allons le voir, un cryptosystème à chiffrement probabiliste au sens qui a été donné à cette locution au début de ce chapitre (voir page **106**).

En effet soit x un élément de G, on pose alors :

$$e(x) = (\alpha^k, \beta^k \cdot x)$$

où k est un entier choisi arbitrairement par l'expéditeur et variable selon son gré lorsque x décrit le groupe G.

Pour décoder, si on pose $y = \alpha^k$ et $z = \beta^k x$, il suffit de constater que : $z = \alpha^{ak} x = y^a x$ ce qui fournit :

$$x = zy^{-a}$$

par conséquent la fonction de décodage d, valable quelle que soit la fonction e utilisée pour le chiffrement, est définie par :

$$d(y, z) = y^{-a} z$$

Bien évidemment, sans la possession de l'entier a (partie cachée de la clef du cryptosystème) il est impossible pour un intrus captant $e(x) = (y, z)$ d'en déduire x, sauf s'il dispose d'un procédé cryptanalytique efficace permettant de déterminer a.

Le problème de la détermination de a, dit aussi problème du logarithme discret, est en général un problème difficile lorsque la loi du groupe G est "tordue" ; c'est en particulier vrai si G est le groupe cyclique des inversibles d'un corps de Frobénius $\mathbb{F}_p$ où p est un "grand" entier premier (200 chiffres décimaux).

D'ailleurs, en général, le chiffrement El-Gamal s'effectue sur le groupe $(\mathbb{F}_p^*, \bullet)$ où p est un nombre premier ; mais nous allons voir, dans ce qui suit, que ce protocole mathématique sait s'adapter et permettre de chiffrer d'autres "messages" que ceux d'un groupe cyclique G. Nous résumons schématiquement ci-dessous les trois cryptosystèmes à clé publique, dont nous venons de faire état.

RSA : $K = (n, p, q, a, b)$, $n = pq$, p, q premiers distincts, $ab = 1$ modulo $\varphi(n)$.
n, a sont publics ; p, q, et b sont secrets.
$E = E' = \mathbb{Z}/n\mathbb{Z}$ (ou $E = E' = \{0, 1, \ldots, n-1\}$)
$e(\bar{x}) = \bar{x}^a$ (ou $e(x) = x^a$ modulo n)
$d(\bar{x}) = \bar{x}^b$ (ou $d(x) = x^b$ modulo n)

Rabin : $K = (n, p, q)$, $n = pq$, p, q premiers distincts égaux à 3 modulo 4. p et q sont cachés ; n est public.
$E = \Omega_n = E'$ (résidus quadratiques modulo n)
$e(\bar{x}) = \bar{x}^2$,
$d(y) = \overline{pp'u + qq'z}$ où : $u^2 = y \pmod q$, où $z^2 = y \pmod p$
et $pp' + qq' = 1,\ u, v \in \Omega_n$.

El-Gamal : $K = (G, \alpha, \beta, a)$ où G est un groupe cyclique, α un générateur de G, a un entier et $\beta = \alpha^a$. (G, α, β) sont publics ; a est tenu secret.
$E = G$, $E' = G \times G$.
Une fonction de codage est du type : $x \in G \xrightarrow{e} (\alpha^k, \beta^k \cdot x) \in E'$ où k est un entier dépendant *a priori* de x (codage probabiliste). La fonction de décodage valable quelle que soit la fonction d'encodage e, est définie par $d(y, z) = y^{-a} z$.

c. Exemple simple et pratique de chiffrement El-Gamal

(i) $\mathbb{K} = \mathbb{Z}/3\mathbb{Z}$ et $P = X^3 - X^2 + 1$ est irréductible dans $\mathbb{K}[X]$; soit $\mathbb{K}' = \mathbb{K}[X]/(P)$; $\mathbb{K}'$ est le corps standard à 27 éléments ; soit $G = \mathbb{K}'^*$; $(G, \bullet)$ est cyclique et possède 26 éléments ; $\alpha = \bar{X}$ est une racine primitive 26-ième de l'unité dans $\mathbb{K}'$; en effet, un calcul facile prouve que : $\alpha^9 = \alpha^6 - 1, \alpha^{12} = \alpha^2 + 2\alpha, \alpha^{13} = -1$...
Ainsi $\alpha = \bar{X}$ engendre le groupe multiplicatif G ; convenons de "classer" les éléments de G dans "l'ordre lexicographique" modulo $X^3 - X^2 + 1$ et de les faire correspondre ainsi aux 26 lettres de l'alphabet A...Z. Ainsi on a la correspondance :

$$A \to \bar{1},\ B \to \bar{2},\ C \to \bar{x},\ D \to \overline{X+1}, E \to \overline{X+2}...$$
$$V \to \overline{2X^2 + X + 1},\ W \to \overline{2X^2 + X + 2},\ X \to \overline{2X^2 + 2X},$$
$$Y \to \overline{2X^2 + 2X + 1},\ Z \to \overline{2X^2 + 2X + 2}$$

On prend alors $a = 11$; vérifier que $\beta = \alpha^{11} = \overline{X+2}$ et décoder le message suivant :

(J,S), (W,Y), (I,B), (B,G), (K,A), (B,B), (B,W), (H,D), (E,I), (L,E), (E,V)

(ii) Comme $\alpha = \bar{X}$ génère G, $P = X^3 - X^2 + 1$ est un facteur premier de $\Phi_{26}(X)$ dans $\mathbb{K}[X]$, d'après la proposition 19 du chapitre **2** ; $1/\alpha$ est aussi un générateur de G, et $1/\alpha^3 - 1/\alpha + 1 = 0$; cela prouve que le polynôme $X^3 - X + 1$ est aussi un facteur premier dans $\mathbb{K}[X]$ de $\Phi_{26}(X)$; tous les facteurs premiers dans $\mathbb{K}[X]$ du polynôme cyclotomique $\Phi_{26}(X)$ (qui est de degré $12 = \varphi(26)$) sont de degré 3 puisque $3^3 = 1$ modulo 26 (proposition 4 du chapitre **4**).

Comme $5 \wedge 26 = 1, \alpha' = \alpha^5$ génère également G ; or on peut écrire :

$$\alpha'^3 + \alpha'^2 - \alpha' + 1 = 0$$

d'où $X^3 + X^2 - X + 1$ est encore un facteur premier de $\Phi_{26}(X)$ et comme $1/\alpha'$ engendre aussi G, $X^3 - X^2 + X + 1$ est le "dernier" facteur premier de $\Phi_{26}(X)$; d'où : dans $\mathbb{K}[X]$ où $\mathbb{K} = \mathbb{Z}/3\mathbb{Z}$ on a :

$$\begin{aligned}\Phi_{26}(X) &= X^{12} - X^{11} + X^{10} - X^9 + X^8 - X^7 + X^6 - X^5 + \\ &\quad X^4 - X^3 + \\ &\quad X^2 - X + 1 \\ &\quad = (X^3 - X^2 + 1)(X^3 - X + 1)(X^3 + X^2 - X + 1) \times \\ &\quad (X^3 - X^2 + X + 1)\end{aligned}$$

Et, aussi surprenant que cela paraisse, on récupère sans effort la décomposition en facteurs premiers de $\Phi_{26}(X)$ dans $\mathbb{Z}/3\mathbb{Z}[X]$

Remarques :

(i) Lorsque p est premier, $p \geq 3$, $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$ et, par application de la proposition 20 du chapitre **2**, on a : $\Phi_{2p}(X) = \sum_{k=0}^{p-1} (-1)^k X^k$, d'où le calcul de $\Phi_{26}(X)$.

(ii) Comme nous l'avons dit et comme la suite de cet ouvrage l'atteste, le système cryptographique El-Gamal est susceptible d'être notablement amélioré ; ces améliorations sont indiquées dans les deux paragraphes suivants de cette partie, mais aussi dans la partie de ce chapitre consacrée à la cryptologie définie à partir des courbes elliptiques.

7.1.6 Généralisation du protocole El-Gamal dans $\mathbb{Z}/n\mathbb{Z}$ avec n du type p^m ou $2p^m$, p premier, $p \geq 3$

Ce paragraphe montre, sur un exemple, que l'on peut élaborer un système cryptographique dans un monoïde commutatif pourvu qu'il existe une partie de ce monoïde constituée en groupe cyclique. En effet soit n un entier du type p^m ou $2p^m$ avec p premier, $p \geq 3$, et $m \geq 1$; on sait que le groupe $(G_n, \bullet)$ des inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \bullet)$ est un groupe cyclique ; il va nous permettre, en jouant le rôle de masque, de définir un protocole cryptographique en tout point semblable à celui d'un El-Gamal dans un groupe cyclique.

La clé K est définie par la liste : $K = (n, \bar{\alpha}, \bar{\beta}, a)$ avec :

- n entier du type indiqué
- $\bar{\alpha}$ un générateur de G_n
- a entier
- $\bar{\beta} = \bar{\alpha}^a$

$n, \bar{\alpha}, \bar{\beta}$ sont publics ; seul l'entier a est conservé secret par le créateur du cryptosystème.

L'ensemble E des textes à coder est ici défini par : $E = \mathbb{Z}/n\mathbb{Z}$ et l'ensemble E' des textes chiffrés est $E' = G_n \times E$.

Le chiffrement est probabiliste et défini pour $\bar{x} \in E$ par : $e(\bar{x}) = (\bar{\alpha}^k, \bar{\beta}^k \cdot \bar{x})$ où k est un entier arbitrairement choisi par l'expéditeur du message $\bar{x}$.

Le déchiffrement s'effectue grâce à la fonction d de décodage, valable quelle que soit la fonction d'encodage e, définie par :

$$d(\bar{y}, \bar{z}) = ((\bar{y})^{-1})^a \bar{z} = (\bar{y})^{-a} \cdot \bar{z}$$

Ainsi l'ensemble des textes clairs est "plus important" que le groupe cyclique ayant permis la réalisation du mécanisme de secret ; dans le paragraphe suivant, une étude extrêmement détaillée d'un tel protocole permet de voir la richesse du point de vue mis en valeur à travers cet exemple.

Etude d'un exemple numérique :

(i) On prend $p = 5, m = 3$ et $n = 2 \times 125 = 250$.
2 modulo 125 génère G_{125} et comme : $1 = 125 - 2 \times 62$ il s'ensuit que : $-\overline{248 + 125} = \overline{127}$ modulo 250 génère G_{250} (qui est un groupe cyclique ayant 100 éléments) ; il en résulte que : $\overline{33}$ modulo 250 génère G_{250} (on a calculé $\overline{127}^i$ avec $i \wedge 250 = 1$, jusqu'à obtenir $\overline{33}$ modulo 250).

(ii) On prendra donc : $\bar{\alpha} = \overline{33}$ et pour partie cachée a de la clé l'entier : $a = 32$; on trouve alors :
$$\beta = \overline{33}^{32} = \overline{61} \pmod{250}$$
D'où :
$$K = (\mathbb{Z}/250\mathbb{Z}; \overline{33}, \overline{61}, 32)$$

(iii) Supposons qu'on veuille coder $x = \overline{97}$; on choisit $k = 3$ et alors on obtient :
$$e(\bar{x}) = (\overline{227}, \overline{157}), y = \overline{227}, z = \overline{157}$$

(iv) Pour décoder on calcule $y^{-1} = \overline{123}$ puis $(y^{-1})^a = \overline{123}^{32}$ et on trouve : $(y^{-1})^a = \overline{123}^{32} = \overline{171} \pmod{250}$ et alors :
$$171 \times 157 = 97 \pmod{250}$$
on retrouve bien le message initial.

7.1.7 Etude exhaustive d'un cryptosystème El-Gamal sur un $\mathbb{F}_p^n$

7.1.7.1 Un protocole général de création d'un cryptosystème

Soit E un ensemble fini (ensemble des messages à transmettre) ; on suppose disposer sur E d'une loi de composition interne :

$$(x, y) \in E \times E \longrightarrow x * y \in E$$

associative, commutative et possédant un élément neutre ; E est donc un monoïde commutatif.

On suppose également l'existence d'un sous ensemble G de E tel que $(G, *)$ est un groupe cyclique (non réduit à l'élément neutre). Alors le quintuplet :

$$(K, E, E', e, d)$$

avec :

(i) $K = (\alpha, \beta, a)$, α étant un générateur de G, $\beta = \alpha^a$, a entier, α, β sont publics, a est secret.

(ii) $E' = E \times G$

(iii) $\forall x \in E, e(x) = (y, z)$ où : $z = \alpha^k$, k entier choisi arbitrairement, et $y = \beta^k * x$ $(\alpha^k = \alpha * \alpha * \cdots * \alpha, k \text{ fois})$

(iv) $d(y, z) = z'^a * y$ où z' est l'inverse dans $(G, *)$ de z.

constitue un cryptosystème basé sur l'utilisation du logarithme discret (El-Gamal), à chiffrement probabiliste, le groupe G servant à "masquer", à chaque étape, le message x.

7.1.7.2 Sécurité d'un tel système

Elle repose sur la difficulté, pour un intrus, à découvrir l'entier a *ie* le log discret de β en base α dans G. A ce propos rappelons :

a. L'algorithme de Shanks

Soit $m = card\, G$; a est, bien évidemment, défini modulo m, puisque dans G, $x^m = 1$; l'algorithme de Shanks est construit comme il suit :

(i) Soit q la partie entière par excès de $\sqrt{m}$; par division euclidienne, on écrit : $a = \log_\alpha \beta = qj + i$ où $\begin{cases} i \in \{0, 1, \ldots, q-1\} \\ 0 \leq j \leq q-1 \end{cases}$; de ce fait on peut écrire :

$$\alpha^{qj} = \beta * \alpha^{-i}$$

ce qui entraîne (algorithme) :

(ii) Calculer les éléments α^{qj} pour : $0 \leq j \leq q-1$.
Ecrire les couples (j, α^{qj}), $j = 0, 1, \ldots, q-1$.
Calculer les $\beta * \alpha^{-i}$ pour : $0 \leq i \leq q-1$ et écrire les couples $(i, \beta * \alpha^{-i})$.
Déterminer les couples du type (j, y) et (i, y).
Ecrire : $a = \log_\alpha \beta = qj + i \pmod m$

b. L'algorithme de Pohlig

Il établit une technique pour obtenir $a = \log_\alpha \beta$ dans $(G, *)$. Ecrivons avec : $m = card\ G$:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

avec p_i premier, et $\alpha_i \geq 1$ entier.

Dans cet algorithme, il y a deux étapes :

(i) Première étape : on calcule $a \pmod{p_i^{\alpha_i}}$ $i = 1, 2, \ldots, k$.

(ii) Deuxième étape : on applique le théorème des restes chinois pour calculer a modulo m.

Nous allons décrire la première étape seulement, car le seconde est beaucoup plus facile à mettre en œuvre.

Il s'agit de savoir calculer a modulo q^c où q est premier tel que $m = 0 \pmod{q^c}$ et $m \neq 0 \pmod{q^{c+1}}$.

Posons alors : $x = a \pmod{q^c}$ avec $0 \leq x \leq q^c - 1$; alors on peut écrire :

$$x = a_0 + a_1 q + \cdots + a_{c-1} q^{c-1}$$

où $0 \leq a_i \leq q - 1$; de ce fait :

$$a = x + sq^c \text{ avec } s \in \mathbb{N}$$

On montre, dans ce qui suit, comment on peut successivement déterminer les entiers $a_0, a_1, \ldots, a_{c-1}$.

1° pas :

On a :

$$\beta^{m/q} = \alpha^{ma_0/q} \text{ dans } (G, *)$$

En effet, on peut écrire : $\beta^{m/q} = \alpha^{am/q} = \alpha^{(x+sq^c)\frac{m}{q}}$; on veut montrer que : $\alpha^{(x+sq^c)\frac{m}{q}} = \alpha^{ma_0/q}$ ce qui revient à montrer que :

$$\frac{m}{q}(x + sq^c - a_0) = 0 \pmod{m}$$

Or nous avons : $\frac{m}{q}(x + sq^c - a_0) = \frac{m}{q}(sq^c + \sum_{i=1}^{c-1} a_i q^i) = 0 \pmod{m}$.

De ce fait, pratiquement pour calculer a_0 :

- on calcule d'abord $\beta^{m/q}$ dans $(G, *)$
- puis en posant $b = \alpha^{m/q}$ on calcule b^i jusqu'à l'obtention de $\beta^{m/q}$, ce qui fournit $a_0 = i$ $(0 \leq i \leq q - 1)$.

2° pas : Pour calculer $a_1, ...$ on procède de même ; ainsi :
on pose : $x_1 = x - a_0$ et $\beta_1 = \beta\alpha^{-a_0}$ et on a :

$$\beta_1 = \alpha^{x_1+sq^c} \text{ dans } (G, *)$$

Dans ces conditions, à nouveau on a :

$$\beta_1^{m/q^2} = \alpha^{a_1 m/q}$$

en effet cela revient à prouver :

$$\alpha^{\frac{m}{q^2}(x_1+sq^c)} = \alpha^{a_1 m/q}$$

ie que :

$$\frac{m}{q}\left(\frac{a_1 + sq^c}{q} - a_1\right) = 0 \pmod m$$

Or :

$$\frac{m}{q^2}(x_1 + sq^c - qa_1) = \frac{m}{q^2}\left(sq^c + \sum_{i=2}^{c-1} a_i q^i\right) = 0 \pmod m$$

Par conséquent, à nouveau, on cherche $i \in \{0, 1, \ldots, q-1\}$ tel que :

$$\alpha^{im/q} = \beta_1^{m/q^2} \cdots \text{ et } i = a_1$$

De façon générale... on itère... autant de fois que c'est possible, et on s'aperçoit que cela revient par force brute à déterminer c fois le logarithme discret dans un groupe cyclique (générique ?) ayant q éléments.

c. La morale

La morale que l'on peut tirer de ces deux algorithmes c'est que dans un groupe cyclique ayant m éléments, le logarithme discret est difficile à casser si m est un grand nombre entier ayant au moins un facteur premier qui lui-même est un grand nombre entier

7.1.7.3 Le cryptosystème dans $\mathbb{K}^n$ engendré par la matrice de Frobénius

a. Généralités

$\mathbb{K}$ est un corps ayant q éléments et n un entier, $n \geq 3$.

F est l'élément de $M_n(\mathbb{K})$ défini par : $F = \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & 0 & \ddots & \\ 0 & \vdots & \ddots & 1 \\ 1 & 0 & & 0 \end{pmatrix}$ et pour $x \in \mathbb{K}^n$, $A(x) = \sum_{i=0}^{n-1} x_i F^i$. On rappelle que $X^n - 1$ est le caractéristique et le minimal de F.

Alors on a :

Pour $x = (x_0, x_1, \cdots, x_{n-1})$ et $y = (y_0, y_1, \cdots, y_{n-1})$ de $\mathbb{K}^n$ il existe z unique dans $\mathbb{K}^n$, $z = (z_0, z_1, \ldots, z_{n-1})$ tel que :

$$A(x)A(y) = A(z)$$

On pose alors $z = x * y$; l'application $*$ fournit sur $\mathbb{K}^n$ une loi de composition interne associative, commutative admettant $e = (1, 0, \ldots, 0)$ pour élément neutre ; en outre :

$$z_i = \sum_{\substack{k+l=i \pmod n \\ 0 \le k,l \le n-1}} x_k y_l$$

(la loi $*$ porte le nom de *loi de convolution* dans $\mathbb{K}^n$)

Tout se vérifie aisément ; alors on peut énoncer :

Si $G = \{x \in \mathbb{K}^n : det\ A(x) = 1\}$ le couple $(G, *)$ est un groupe ; en outre si $n \wedge (q-1) = 1$ *ie* si n et $q-1$ sont premiers entre eux, $card\ G \le q^{n-1}$ et, dans le cas où en plus $n \notin p\mathbb{Z}$, (on suppose $q = p^r$ avec p premier) on a : $card(G) \le q^{n-1} - 1$

Démonstration :

1° pas : L'application $\lambda \in \mathbb{K} \longrightarrow \lambda^n \in \mathbb{K}$ est une bijection. En effet soient $\lambda, \mu \in \mathbb{K}$ avec $\lambda^n = \mu^n$; si $\lambda^n = \mu^n = 0$, $\lambda = \mu = 0$, sinon : $(\lambda\mu^{-1})^n = 1$ *ie* $z^n = 1$ avec $z = \lambda\mu^{-1}$; soit d l'ordre de z dans $\mathbb{K}^*$; d divise $q-1$ (Lagrange..) et d divise n ; donc $d = 1$ *ie* $\lambda = \mu$ (fin du 1° pas).

2° pas : Pour $\lambda \in \mathbb{K}$, soit $\Omega_\lambda = \{x \in \mathbb{K}^n : det\ A(x) = \lambda\}$; alors si $\lambda \neq 0$, $card\ \Omega_\lambda = card\ G$.

En effet si $\lambda \neq 0$, il existe μ unique tel que : $\lambda = \mu^n$ et alors l'application $x \in G \longrightarrow \mu x \in \Omega_\lambda$ est une bijection (fin du 2° pas).

3° pas : Ainsi $card\ \mathbb{K}^n = q^n = (q-1) card\ G + card\ G_0$ (***) et : on a toujours :

$$card\ \Omega_0 \ge q^{n-1}$$

car, à l'évidence, Ω_0 contient toujours l'hyperplan $x_0 + x_1 + \cdots + x_n = 0$ et ainsi $card\ G \le q^{n-1}$. De plus si $u \in \mathcal{L}(\mathbb{K}^n)$ est tel que :

$$Mat(u; b_c) = F$$

on a :

$$u(\varepsilon) = \varepsilon\ si\ \varepsilon = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

et si H est l'hyperplan de $\mathbb{K}^n$ d'équation :

$$x_0 + x_1 + \cdots + x_{n-1} = 0$$

on a : $u(H) \subseteq H$ (b_c est la base canonique de $\mathbb{K}^n$).

Comme les vecteurs : $\begin{pmatrix} 1 \\ -1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \cdots \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \\ 1 \\ -1 \end{pmatrix}$ forment une base de H, F est donc, si $n \notin p\mathbb{Z}$, dans $M_n(\mathbb{K})$, semblable à :

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ \vdots & & & \end{array}\right)$$

où :

$$B = \begin{pmatrix} -1 & 1 & & & 0 \\ -1 & 0 & \ddots & & \\ \vdots & \vdots & 0 & \ddots & \\ \vdots & \vdots & & \ddots & 1 \\ -1 & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

dont le caractéristique, égal au minimal, est le polynôme : $X^{n-1} + X^{n-2} + \cdots + X + 1$.

Ainsi :

$$det(A(x)) = (x_0 + \cdots + x_{n-1}) det(x_0 I_{n-1} + x_1 B + \cdots + x_{n-1} B^{n-1})$$

et donc on retrouve : $H \subseteq \Omega_0$, d'où encore :

$$card\ \Omega_0 \geq card\ H = q^{n-1}$$

(fin du 3° pas)

4° pas : Si $q = p^r$, p premier, et si $n \notin p\mathbb{Z}$, tous les vecteurs : $(\lambda, \lambda, \ldots, \lambda)$ de $\mathbb{K}^n$ avec $\lambda \neq 0$ sont dans Ω_0 et pas dans H, ainsi :

$$card\ \Omega_0 \geq q^{n-1} + q - 1$$

ce qui entraîne, dans ce cas :

$$\boxed{card\ G \leq q^{n-1} - 1}$$

(fin du 4° pas)

b. Le cas intéressant et le cryptosystème associé

On rappelle le résultat suivant (voir proposition 6 chapitre **4**) :

Si $\mathbb{K}$ est un corps ayant q éléments, dans $\mathbb{K}[X]$, le polynôme cyclotomique $\Phi_n(X)$ où $q \wedge n = 1$, est irréductible, *si et seulement si* $\bar{q} \pmod n$ est un générateur du groupe multiplicatif des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Alors cela nous permet d'énoncer :

Soient $\mathbb{K}$ un corps ayant q éléments et n un entier premier ; si $[\bar{q}(n)] = (\mathbb{F}_n^*, \times)$ le groupe G est cyclique d'ordre $q^{n-1} - 1$.

Démonstration : En effet on sait que $\mathbb{K}[B]$ est isomorphe à $\mathbb{K}[X]/(1 + X + \cdots + X^{n-1})\mathbb{K}[X]$ et comme n est premier on a, puisque $\Phi_n(X) = 1 + X + \cdots + X^{n-1}$:

$$\mathbb{K}[B] \cong \mathbb{K}[X]/\Phi_n(X)\mathbb{K}[X]$$

c'est donc un corps ; à ce moment là, $\mathbb{K}[B]/\{0\}$ est un groupe cyclique (proposition 15 du chapitre **2**) ayant $q^{n-1} - 1$ éléments ; on peut donc trouver $\lambda_0, \lambda_1, \ldots, \lambda_{n-2} \in \mathbb{K}$ tels que , dans ce groupe, $M = \sum_{i=0}^{n-2} \lambda_i B^i$ est d'ordre $q^{n-1} - 1$; ceci étant dit on a :

$$A(x) \sim \left(\begin{array}{c|ccc} x_0 + x_1 + \cdots + x_{n-1} & 0 & \cdots & 0 \\ \hline 0 & & \sum_{i=0}^{n-2}(x_i - x_{n-1})B^i & \end{array}\right)$$

pour tout x de $\mathbb{K}^n$. Prenons :

$$\begin{gathered} x_0 = \lambda_0 + x_{n-1} \\ x_1 = \lambda_1 + x_{n-1} \\ \vdots \\ x_{n-2} = \lambda_{n-2} + x_{n-1} \\ \text{et } x_{n-1} \text{ tel que :} \\ (\lambda_0 + \cdots + \lambda_{n-2} + n x_{n-1}) \det M = 1 \end{gathered}$$

ce qui est toujours possible puisque n n'est pas un multiple de la caractéristique de $\mathbb{K}$.

Dans ces conditions, $A(x)^k \sim \left(\begin{array}{c|c} \mu^k & 0 \\ \hline 0 & M^k \end{array}\right)$ où $\mu = \lambda_0 + \cdots + \lambda_{n-2} + n x_{n-1}$ et ce, quel que soit l'entier k ; par conséquent $A(x)^k = I_n$ entraîne : $M^k = I_{n-1}$ et $\mu^k = 1$; ainsi k est un multiple de $q^{n-1} - 1$; par conséquent l'ordre de x dans $(G, *)$ est $q^{n-1} - 1$ ce qui prouve bien ce que nous voulions.

7.1.7.4 Mise en forme pratique

On prend toujours $q = p$ nombre premier *ie* on suppose que $\mathbb{K}$ est un $\mathbb{F}_p$ avec p bien choisi comme la suite l'explique.

a. *D'abord on fixe* n qui détermine la longueur des séquences à crypter ; n est bien sûr un nombre premier.
Ensuite on fait rapidement le choix d'un $u \in \{2, \ldots, n-1\}$ tel que $\bar{u} \pmod{n}$ engendre le groupe $(\mathbb{F}_n^*, \times)$.

b. *Il s'agit ensuite* d'ajuster k entier naturel tel que : $p = kn+u$ soit premier et tel que : $p^{n-1}-1$ soit un "grand" nombre ayant au moins un "grand" facteur premier afin de mettre en échec les algorithmes de Shanks et de Pohlig (ici *card* $G = p^{n-1}-1$).
Remarquons d'abord que dans la suite arithmétique :

$$u, u+n, u+2n, \ldots, u+kn, \cdots$$

il existe une infinité de nombres premiers (théorème de Dirichlet, voir **6.2** chapitre **6**). Eh bien, tout simplement, on effectue plusieurs tentatives.
Par exemple, nous avons construit notre cryptosystème en fixant : $n = 23$; et en prenant $p = 5297$, nous disposons d'un groupe G dans $\mathbb{K}^n$ ($\mathbb{K} = \mathbb{F}_p$) ayant un nombre d'éléments associé à un entier ayant plus de 82 chiffres dans son écriture décimale ; en outre l'entier $p^{n-1}-1$ possède un facteur premier ayant 23 chiffres dans son écriture décimale : ainsi *la sécurité du système est assurée.*

c. Le plus grand diviseur premier de $p^{n-1}-1$ est ici égal à :

$$67\ 585\ 421\ 723\ 399\ 741\ 283\ 909$$

Pour générateur, on a pris :

$$\alpha = (2779, 4090, 599, 34, 2175, 4744, 227, 2940, 2412, 4192, 2214, 2299,$$
$$980, 2004, 4005, 3886, 2127, 4161, 4168, 2320, 3697, 1310, 1511)$$

et avec : $a = 28283825546122715902313389778118927299372360541527709337227499529864732300674599 37$ on obtient β défini par :

$$\beta = (771, 953, 4839, 3096, 241, 2146, 2398, 3910, 2142, 2410, 5026, 4933,$$
$$2311, 2544, 3592, 2150, 5002, 4821, 4738, 111, 3135, 3602, 3360)$$

Les multiplications dans $(G, *)$ s'effectuant *via* l'algorithme d'exponentiation rapide.

d. *Afin de décoder rapidement :* il faut savoir, pour $x \in G$, trouver dans les plus brefs délais $x' \in G$, avec $x * x' = (1, 0, ...)$ *ie* tel que : $A(x)A(x') = I_n$; or la matrice :

$$A(x) = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & \cdots & x_{n-2} \\ \vdots & & & \vdots \\ x_1 & \cdots & \cdots & x_0 \end{pmatrix}$$

est une matrice de $M_n(\mathbb{K})$, circulante de déterminant 1 ; donc $A(x')$ qui est circulante vaut : $A(x') = \widetilde{com\ A(x)}$ (transposée de la comatrice) et, de ce fait, pour trouver le vecteur x' il suffit de calculer les n mineurs des éléments de la première colonne de $A(x)$.

e. *Conclusion* : Ce cryptosystème est donc d'une utilisation particulièrement souple et sécurisée, et il travaille en temps réel, c'est-à-dire avec une très grande rapidité car, contrairement à beaucoup de cryptosystèmes qui nécessitent l'utilisation de très grands nombres premiers, on peut ici, en jouant sur les entiers n et p, obtenir de très "grands" nombres avec $p \leq 2000$; comme les calculs sont effectués modulo p, ils sont instantanés et en tout cas plus rapides que s'ils étaient effectués modulo un entier premier ayant 100 chiffres dans son écriture décimale, ce qui est le cas dans beaucoup de cryptosystèmes usuels.

En plus, si on songe au cryptosystème de Vanstone à partir d'une courbe elliptique sur $\mathbb{F}_p$, celui-ci ne crypte que des éléments de $\mathbb{K}^2$ ($\mathbb{K} = \mathbb{F}_p$) ; ici on crypte dans $\mathbb{K}^n$ avec n premier choisi comme on le veut.

Remarque 1 : Elle concerne le décodage

Si $x \in G$, on veut déterminer rapidement $x' \in G : x * x' = (1, 0 \cdots)$. Posons :

$$A(x) = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & \cdots & x_{n-2} \\ & \ddots & \ddots & \\ & & & x_0 \end{pmatrix}$$

si $x = (x_0, x_1, \ldots, x_{n-1})$ on peut écrire :

$$(A(x))^{-1} = A(x') = \begin{pmatrix} x'_0 & x'_1 & \cdots & x'_{n-1} \\ x'_{n-1} & x'_0 & \cdots & x'_{n-2} \\ & \ddots & \ddots & \\ & & & x'_0 \end{pmatrix}$$

Si $P(X) = X^n + \alpha_1 X^{n-1} + \cdots + \alpha_{n-1} X + \alpha_n$ est le caractéristique de $A(x)$, $P(X) = \det(XI_n - A(x))$ et $\alpha_n = (-1)^n \det A(x) = (-1)^n$, ($\det A(x) = 1$). Les coefficients $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ seront calculés par les formules de Fadeev :

$$\begin{cases} tr\ A^i(x) + \alpha_1 tr\ A^{i-1}(x) + \cdots + \alpha_{i-1} tr\ A(x) + i\alpha_i = 0 \\ i = 1, 2, \ldots, n \end{cases}$$

comme la suite l'indique ; $tr\ A(x) = nx_0$ et plus généralement si $x^i = \underbrace{x * \cdots * x}_{i \text{ fois}} = (x_0(i), x_1(i), \cdots)$ on a : $tr\ A^i(x) = nx_0(i)$.

Donc *pratiquement* pour calculer $x' = x^{-1}$ on calcule (dans $(G, *)$) $x^i = \underbrace{x * \cdots * x}_{i \text{ fois}} = (x_0(i), x_1(i), \ldots, x_{n-1}(i))$ pour $i = 0, 1, 2, \ldots, n-1, n$ et puis avec Fadeev (on supposera toujours $n < p$), on détermine les coefficients $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ ($\alpha_n = (-1)^n$ et $\alpha_0 = 1$) tels que :

$$nx_0(i) +, n\alpha_1 x_0(i-1) + \cdots + nx_0\alpha_{i-1} + i\alpha_i = 0 \qquad (**)$$

Comme, via Cayley-Hamilton, on a :

$$(A(x))^n + \alpha_1(A(x))^{n-1} + \cdots + \alpha_{n-1}A(x) = (-1)^{n+1}I_n$$

il vient :

$$(A(x))^{-1} = (-1)^{n+1}\left[\left(\sum_{i=1}^{n-1}\alpha_i A(x)^{n-i-1}\right) + (A(x))^{n-1}\right]$$

ie :

$$\boxed{(A(x))^{-1} = (-1)^{n+1}[(A(x))^{n-1} + \alpha_1((A(x))^{n-2} + \cdots + \alpha_{n-1}I_n]}$$

si : $x' = x^{-1} = (x'_0, x'_1, \ldots, x'_{n-1})$ on a donc :

$$\boxed{x'_j = (-1)^{n+1}[x_j(n-1) + \alpha_1 x_j(n-2) + \cdots + \alpha_{n-2}x_j(1) + \alpha_{n-1}\delta_{0,j}] \qquad (***)}$$

où $\delta_{0,j}$ est le symbole de Kronecker.

L'intérêt de ce calcul c'est qu'il évite d'élever la matrice $A(x)$ à la puissance k $(k = 0, 1, \ldots, n-1)$ et, par conséquent, il améliore la rapidité de la procédure car, en fin de compte, tout se ramène pour $x = (x_0, x_1, \ldots, x_{n-1})$ à calculer x^k dans le groupe G, où $x^k = (x_0(k), x_1(k), \ldots, x_{n-1}(k))$; il n'y a pas de déterminant à calculer ; tout est donc facile à écrire et instantané dans l'exécution.

Remarque 2 : Elle concerne la recherche d'un générateur du groupe G

D'abord, constatons que l'on a "une chance sur p" d'obtenir un élément de G si cet élément est choisi arbitrairement dans $\mathbb{K}^n$. Cependant, puisque $card\ G = p^{n-1} - 1$ on a donc, *via* les notations utilisées : $card\ \Omega_0 = (p-1) + p^{n-1}$ ce qui signifie que, pour $x \in \mathbb{K}^n$, $\det A(x) = 0$, *si et seulement si* : $x_0 + x_1 + \cdots + x_{n-1} = 0$ ou $x = (\lambda, \lambda, \ldots, \lambda)$ avec $\lambda \neq 0$ (***)

On choisira donc $x \in \mathbb{K}^n$ arbitraire ne vérifiant pas (***).

Ensuite, si $\alpha \in G$, on peut tester rapidement le fait que α génère ou non le groupe $(G, *)$ en procédant comme il suit. Soit $m = p^{n-1} - 1 = card\ G = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers ; si α n'engendre pas G, son ordre m' divise m, donc il existe $i \in \{1, 2, \ldots, r\}$ tel que $\alpha^{m/p_i} = (1, 0, \ldots, 0)$; par conséquent on calcule, *via* l'algorithme d'exponentiation rapide dans $(G, *)$, $\alpha^{m/p_1}, \alpha^{m/p_2}, \ldots, \alpha^{m/p_r}$ et s'ils sont tous distincts de $(1, 0, \ldots, 0)$, α est un générateur du groupe $(G, *)$; cela va très vite et on rappelle que si α engendre $(G, *)$ les autres générateurs de G sont les α^i avec $i \wedge m = 1$.

7.1.7.5 En résumé et pour conclure une remarque

a. Résumé

Les entiers n et p étant premiers, distincts, et "bien choisis", on peut alors constituer un système cryptographique dont les textes clairs sont les éléments de $\mathbb{K}^n$, dont les textes

codés appartiennent à $\mathbb{K}^n \times G$, où G est ("le masque") le sous-ensemble de $\mathbb{K}^n$ des x tels que $\det A(x) = 1$; l'ensemble G possède $p^{n-1} - 1$ éléments et G est un groupe cyclique relativement à la loi $*$ *ie* relativement à la convolution dans $\mathbb{K}^n$.

La technique de codage est celle d'un El-Gamal classique ; celle de décodage s'en déduisant bien naturellement ; le groupe surface G sert alors à "masquer" les cryptogrammes.

Toutes les astuces (Shanks, Pohlig) de la cryptanalyse sont inopérantes si n et p sont bien choisis ; en tout état de cause il existe une infinité de choix possibles concernant les entiers n et p qui peuvent être ajustés selon les besoins et la fiabilité souhaitée...

Ce cryptosystème est d'une utilisation particulièrement souple et il travaille en temps réel, car contrairement à beaucoup de cryptosystèmes qui nécessitent l'utilisation de très grands nombres premiers, on peut ici, en jouant sur les entiers n et p, obtenir le groupe-masque G très peuplé avec $p \leq 10000$; comme les calculs sont effectués modulo p ils sont instantanés et plus rapides que s'ils étaient effectués modulo un entier premier ayant 100 chiffres dans son écriture décimale ce qui est le cas dans certains cryptosystèmes actuels...

En outre, si on pense au cryptosystème de Vanstone sur une courbe elliptique, celui-ci ne code que des éléments de $\mathbb{K}^2$, alors qu'ici on code dans $\mathbb{K}^n$, avec n premier choisi comme on le souhaite...

Enfin, les opérations à effectuer vis à vis de la loi $*$ sont très faciles à mettre en œuvre même et y compris lorsqu'il s'agit du calcul de l'inverse ; reste à savoir, s'il existe un algorithme sous-exponentiel spécifique à ce groupe permettant de casser le logarithme discret.

b. Une remarque

On peut chiffrer sur $\mathbb{K}^n$ où $\mathbb{K} = \mathbb{F}_p$ et n un entier quelconque en procédant comme suit.

Soit $P(X)$ un polynôme unitaire irréductible dans $\mathbb{K}[X]$ de degré n et $\mathbb{K}'$ le corps $\mathbb{K}' = \mathbb{K}[X]/(P)$; $\mathbb{K}'$ s'identifie à $\mathbb{K}^n$ par l'application :

$$(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{K}^n \longrightarrow a_0 + a_1\bar{X} + \cdots + a_{n-1}\bar{X}^{n-1}$$

Les éléments inversibles de ce corps forment un groupe cyclique G' sur lequel on peut instaurer un El-Gamal ; l'ensemble des messages est alors G' *ie* $\mathbb{K}^n \backslash \{0\}$; si α génère $(G', \bullet)$, pour $x = \alpha^i$ et $y = \alpha^j$ de G' le produit xy et l'inverse x^{-1} sont, en théorie, faciles à calculer puisque :

$$xy = \alpha^{i+j},\ x^{-1} = x^{-i} = x^{m-i}$$

si m est le nombre d'éléments de G' $(m = p^n - 1)$.

En réalité, comme dans G' le problème du logarithme discret est réputé difficile, il est mal aisé pour $x = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{K}^n$ de trouver k tel que : $\alpha^k = \sum_{i=0}^{n-1} a_i \bar{X}^i$. Or, lorsqu'on chiffre dans $\mathbb{K}^n$ on utilise les "mots" $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{K}^n$ et par conséquent

la multiplication et surtout la division dans $(G', \bullet)$ doivent s'effectuer en calculant dans $\mathbb{K}[X]$, soit un produit AB modulo $P(X)$, soit A' tel que $AA' = 1$ modulo $P(X)$ (voir le corollaire de la proposition 8 du chapitre **4**).

En termes cryptographiques, le codage et surtout le décodage sont ralentis par la lourdeur du protocole algébrique associé. Par contre le système cryptographique El-Gamal précédent (et longuement détaillé) ne souffre pas de ces handicaps. D'abord, l'ensemble des messages ne reste pas cantonné dans une structure de groupe cyclique mais utilise, dans un ensemble plus vaste, à savoir le monoïde $(\mathbb{K}^n, *)$, un sous-ensemble G organisé en groupe cyclique vis à vis de la loi $*$, et des notions d'algèbre linéaire sur $\mathbb{K}^n$ en liaison avec la matrice de Frobénius.

Plusieurs procédures, aussi élémentaires les unes que les autres, issues de l'algèbre linéaire, permettent, nous l'avons vu, de coder et de décoder rapidement ; enfin le groupe surface G permettant de masquer les textes clairs, *ie* les éléments de $\mathbb{K}^n$, a une signification algébrique facile à utiliser pour accélérer le décodage, soit grâce aux formules de Fadeev, ou soit, tout simplement, grâce à la notion de comatrice judicieusement utilisée...

C'est pourquoi nous considérons que le groupe surface $(G, *)$ dans $\mathbb{K}^n$ permet de réaliser avec une grande efficacité un cryptosystème de type El-Gamal dans le monoïde $(\mathbb{K}^n, *)$ en évitant les calculs des produits et des inverses modulo un polynôme dans $\mathbb{K}[X]$ et le lecteur curieux pourra montrer que, pour un élément de $\mathbb{K}^n$, le codage a un coût en $\mathcal{O}(n^2 \log p)$ et le décodage un coût en $\mathcal{O}(n^3 \log n (\log p)^2)$.

Remarque importante : Le lecteur est invité à consulter, en annexe, le travail effectué en TIPE au cours de l'année $2009 - 2010$ par un élève de la classe de spéciale MP* (cet élève a intégré l'ENS Lyon).

7.2 Le cryptosystème El-Gamal adapté aux courbes elliptiques

7.2.1 Instance du problème et introduction

Etant donné un groupe cyclique G, le problème du logarithme discret dans G est d'autant plus difficile à résoudre que la loi du groupe G est "diffuse" ; le cadre des courbes elliptiques, comme la suite va le montrer, permet effectivement de construire des groupes cycliques ayant une "représentation" compliquée rendant ainsi difficile le problème du logarithme discret et par voie de conséquence efficace le cryptosystème El-Gamal.

7.2.2 Les courbes elliptiques sur un corps fini $\mathbb{K}$ de caractéristique ≥ 5

a.

Etablissons d'abord un lemme dont l'utilisation sera justifiée par ce qui suit :

Lemme : Soit $\mathbb{K}$ un corps de caractéristique au moins égale à 5 (*ie* distincte de 2 ou de 3) et $P(X) = X^3 + aX + b$ un élément de $\mathbb{K}[X]$; alors les deux énoncés suivants sont équivalents :

(i) P est sans racine double

(ii) $4a^3 + 27b^2 \neq 0$

Démonstration du lemme : Tout revient à prouver que P admet une racine double *si et seulement si* $4a^3 + 27b^2 = 0$; en effet :

Si $x \in \mathbb{K}$ est racine double de P, on a simultanément : $x^3+ax+b = 0$ et $3x^2+a = 0$; il s'ensuit que $x = -3b/2a$ et en écrivant que $3x^2 + a = 0$ on obtient $4a^3 + 27b^2 = 0$.

Réciproquement si $4a^3 + 27b^2 = 0$ soit x dans $\mathbb{K}$ défini par $x = -3b/2a$; alors $3x^2 + a = \frac{4a^3+27b^2}{4a^2} = 0$ et en outre : $x^3 + ax + b = \frac{2ax}{3} + b = -b + b = 0$, ce qui achève la preuve du lemme.

Ceci étant acquis, nous sommes alors en mesure de fournir la définition d'une courbe elliptique sur un corps $\mathbb{K}$.

b. Définition

On appelle *courbe elliptique* sur le corps $\mathbb{K}$ de caractéristique au moins égale à 5, l'ensemble (E) des couples (x, y) de $\mathbb{K}$ solutions de :

$$y^2 = x^3 + ax + b$$

où a et b sont dans $\mathbb{K}$ tels que : $4a^3 + 27b^2 \neq 0$, auquel on adjoint un point Ω appelé "point à l'infini" de la courbe elliptique (E).

Autrement dit, hormis le point à l'infini, une courbe elliptique sur $\mathbb{K}$ est l'ensemble $(x, \pm\sqrt{P(x)})$ où P est un polynôme unitaire du troisième degré sans racine double et où $x \in \mathbb{K}$ est tel que $P(x)$ est un résidu quadratique de $\mathbb{K}$.

On peut montrer, et nous l'admettrons, le très important théorème suivant :

Proposition 6 (théorème de Hasse) : Si (E) est une courbe elliptique sur le corps fini $\mathbb{K}$ de caractéristique ≥ 5 ayant q éléments, on a toujours l'inégalité :

$$|card\ (E) - (q + 1)| \leq 2\sqrt{q}$$

Cela montre, en particulier, que si $\mathbb{K}$ est un corps ayant les propriétés indiquées, pour a et b dans $\mathbb{K}$, il existe toujours des x de $\mathbb{K}$ tels que $x^2 + ax + b$ est un résidu quadratique de $\mathbb{K}$; rappelons, à ce propos, que $x \in \mathbb{K}^*$ est un résidu quadratique *si et seulement si* : $x^{\frac{q-1}{2}} = 1$ (voir le chapitre consacré aux corps finis).

Exemple : Cela vaut, en particulier, si $\mathbb{K}$ est un corps de Frobénius $\mathbb{F}_p$ avec $p \geq 5$, et c'est tout à fait remarquable car, par exemple, dans $\mathbb{Z}$, avec $P(X) = X^3 + 7$, $P(x)$ n'est jamais le carré d'un entier (la démonstration étant laissée aux soins du lecteur) alors que quel que soit l'entier p premier $p \geq 3$, il existe des $\bar{x} \in \mathbb{F}_p$ tels que $\bar{x}^3 + 7$ est

un carré, ce qui revient à dire qu'il existe des entiers a ($a \in \mathbb{Z}$) tels que a^3+7 est un carré modulo p (par exemple si $p=31$, il y a dans $\mathbb{F}_{31}$, 10 classes $\bar{x}$ telles que $\bar{x}^3+7$ est un carré...).

Même si ce théorème est admis, nous allons dégager quelques idées permettant de compter, dans certains cas, le nombre d'éléments d'une courbe elliptique sur un corps de Frobénius $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; l'une d'elles peut s'énoncer de la manière suivante :

Proposition 7 : Soit $p \geq 5$ un nombre premier égal à 2 modulo 3. Si $b \neq 0$ est dans $\mathbb{F}_p$ la courbe elliptique sur $\mathbb{F}_p$ d'équation : $y^2 = x^3 + b$ possède exactement $p+1$ éléments.

Démonstration : Soit f le morphisme du groupe multiplicatif $\mathbb{F}_p^*$ défini par : $f(\bar{x}) = \bar{x}^3$; si $\bar{a} \in Ker\ f$, et si $\bar{a} \neq 1$, $\bar{a}$ est d'ordre 3 dans le groupe multiplicatif $\mathbb{F}_p^*$; comme 3 ne peut pas diviser l'entier $p-1$ cardinal du groupe $\mathbb{F}_p^*$, ce cas de figure n'est donc pas possible ; par conséquent f est injectif, donc bijectif ; ainsi, pour tout $y \in \mathbb{F}_p$ il existe x unique dans $\mathbb{F}_p$ tel que $x^3 = y^2 - b$ ce qui prouve, à condition de ne pas oublier le point à l'infini Ω, que le cardinal de (E) est égal à $p+1$ (on dit qu'on à affaire à une courbe elliptique *supersingulière*).

De même on a :

Proposition 7 bis : Soit $\mathbb{K}$ un corps fini de caractéristique au moins égale à 5 et (E) la courbe elliptique sur $\mathbb{K}$ d'équation :

$$y^2 = x^3 + ax + b$$

Si λ appartient à $\mathbb{K}^*$ et n'est pas un carré (*ie* si $\lambda^{\frac{q-1}{2}} = -1$) notons (E_λ) la courbe elliptique de $\mathbb{K}$, d'équation :

$$y^2 = x^3 + \frac{ax}{\lambda^2} + \frac{b}{\lambda^3}$$

Alors on a :

$$card(E) + card(E_\lambda) = 2q + 2$$

Démonstration : En effet, si on pose : $g(x) = x^3 + ax + b$ et $h(x) = x^3 + \frac{a}{\lambda^2}x + \frac{b}{\lambda^3}$ on a la relation :

$$g(\lambda x) = \lambda^3 h(x)$$

ainsi on peut écrire : si $g(\lambda x)$ est un carré non nul, $h(x)$ n'est pas un carré. Si $g(\lambda x)$ n'est pas un carré de $\mathbb{K}^*$, $h(x)$ est alors un carré de $\mathbb{K}^*$. Si $g(\lambda x) = 0$, $h(x) = 0$ et réciproquement ; le résultat énoncé en découle alors immédiatement.

De même, la proposition suivante, nous fournit un renseignement très précieux ; sa preuve est laissée aux soins du lecteur et elle peut être admise dans un premier temps.

Proposition 7 ter : Soit p un entier premier, $p \geq 5$ et $(E,+)$ le groupe additif de la courbe elliptique sur $\mathbb{F}_p$ définie par l'équation : (*) $y^2 = x^3 + ax + b$; on désigne par m le cardinal de ce groupe et on écrit : $m = p + 1 - \sigma$.
Alors, si n est un entier quelconque, $n \geq 1$, et si $\mathbb{K}$ est "le corps" à p^n éléments, le groupe $(E',+)$ de la courbe elliptique définie sur $\mathbb{K}$ par la même relation (*) possède :

$$p^n + 1 - S_n$$

éléments où $S = (S_n)_{n\geq 0}$ est la suite d'entiers définie par : $S_0 = 2, S_1 = \sigma$ et $S_{n+1} = \sigma S_n - pS_{n-1}$.

Par exemple sur $\mathbb{F}_5$ la courbe $y^2 = x^3+3$ possède 6 éléments (ne pas oublier Ω...) ; par conséquent sur le corps standard à 25 éléments cette courbe dispose de 26+10=36 éléments (ils ont été énumérés dans la liste d'exemples suivant la proposition 10) ; d'ailleurs, dans les exemples fournis à cette occasion, le lecteur attentif pourra constater que les groupes obtenus ont un ordre compatible avec l'énoncé de la proposition précédente.

A titre d'exemple complémentaire, le groupe de la courbe elliptique $y^2 = x^3 + 3$, sur un corps ayant 5^{50} éléments, possède $(5^{50} + 1) + (2 \times 5^{25})$ éléments (maximum possible via le théorème de Hasse...).

On vérifie, aisément, aussi l'énoncé suivant :

Proposition 7 quarto : Soit $\mathbb{K}$ un corps ayant q éléments et $(E,+)$ le groupe d'une courbe elliptique sur $\mathbb{K}$; on peut écrire si $y^2 = x^3 + ax + b$ est "l'équation" de cette courbe :

$$card(E,+) = q + 1 + \sum_{x\in\mathbb{K}} \chi(x^3 + ax + b)$$

où la fonction χ, appelée "caractère" quadratique, est définie sur $\mathbb{K}$ par :

$$\chi(t) = \begin{cases} 1 \text{ si } t \text{ est un carré de } \mathbb{K} \text{ non nul} \\ 0 \text{ si } t = 0 \\ -1 \text{ si } t \text{ n'est pas un carré de } \mathbb{K} \end{cases}$$

Pour en finir avec cette rubrique, des remarques :

Remarques :

a. Si on prend $q = 31$ le réel $q + 1 - 2\sqrt{q}$ est "voisin" de 20,864... ; par conséquent d'après le théorème de Hasse, toute courbe elliptique sur $\mathbb{F}_{31}$ possède au moins 21 éléments, ce qui est le cas avec celle donnée en exemple à la suite de la proposition 6.

Plus simplement, sur $\mathbb{F}_5$ ($q = 5$ et $q + 1 - 2\sqrt{q}\#1,527...$) toute courbe elliptique sur $\mathbb{F}_5$ possède au moins deux points ; c'est la cas, par exemple, sur celle définie par $y^2 = x^3 + 2x$ qui est constituée du point $(0,0)$ et de Ω (point à l'infini).

On conseille au lecteur de lire attentivement l'étude la courbe elliptique $y^2 = x^3 + 3$ sur le corps à 25 éléments faisant suite à la proposition 10 de ce chapitre.

b. Il existe, pour p entier premier, un algorithme de complexité $\mathcal{O}((\log p)^8)$, appelé algorithme de Schoof, qui permet, par une utilisation judicieuse du théorème des restes chinois, de dénombrer les éléments constituants le groupe d'une courbe elliptique sur le corps de Frobénius $\mathbb{F}_p$; encore une fois on peut constater la nécessité de l'arithmétique modulaire en cryptologie...

7.2.3 La loi de groupe (additif) d'une courbe elliptique sur $\mathbb{K}$ de caractéristique ≥ 5

a. Un lemme

Il est d'abord nécessaire, comme la suite va le justifier, de prouver d'abord les résultats suivants.

Lemme : Soit p un entier premier, $p \geq 5$, et $\mathbb{K}$ un corps de caractéristique p. On désigne par (E) la courbe elliptique de $\mathbb{K}$ d'équation :

$$y^2 = x^3 + ax + b \text{ avec } 4a^3 + 27b^2 \neq 0$$

alors :

(i) Si (x, y) et (x', y') sont deux éléments de (E) avec $x \neq x'$, le point (u, v) de $\mathbb{K}^2$ défini par : $u = \lambda^2 - (x + x'), v = \lambda(x - u) - y$ où $\lambda = \frac{y'-y}{x'-x}$, appartient à (E).

(ii) Si (x, y) appartient à (E) avec $y \neq 0$, le point (u, v) de $\mathbb{K}^2$ défini par : $u = \lambda^2 - 2x$, $v = \lambda(x - u) - y$, où $\lambda = \frac{3x^2+a}{2y}$, est un point de la courbe elliptique (E).

Démonstration : Plaçons-nous d'abord dans le cas (i) et considérons alors le polynôme P de $\mathbb{K}[X]$ défini par :

$$P(X) = X^3 + aX + b - [y + \lambda(X - x)]^2$$

l'hypothèse s'écrit : $P(x) = P(x') = 0$ ce qui légitime alors, dans $\mathbb{K}[X]$, la factorisation : $P(X) = (X - x)(X - x')(X - x'')$ avec $x + x' + x'' = \lambda^2$; comme $P(x'') = 0$ on a donc :

$$[y + \lambda(x'' - x)]^2 = x''^3 + ax'' + b$$

ce qui prouve bien que le point (u, v) du lemme appartient à (E).

Ensuite, si nous sommes dans le cas envisagé en (ii) considérons maintenant le polynôme P de $\mathbb{K}[X]$ défini par :

$$P(X) = X^3 + aX + b - [\lambda(X - x) + y]^2$$

avec $\lambda = \frac{3x^2+a}{2y}$. Dans ce cas, l'hypothèse formulée signifie : $P(x) = 0$ et $P'(x) = 0$, P' désignant le polynôme dérivé du polynôme P dans $\mathbb{K}[X]$; x est donc racine double de P et ainsi nous obtenons la factorisation :

$$P(X) = (X - x)^2(X - u)$$

où $u = \lambda^2 - 2x$ et pour $X = u$ on a :

$$y + \lambda(X - x) = y + \lambda(u - x) = -v$$

où $v = \lambda(x - u) - y$; ainsi on a bien : $u^3 + au + b = v^2$ ce qui achève la preuve du lemme.

Remarques "géométriques" : Dans le cas (i) (*resp.* (ii)) le point (u, v) défini par le lemme est le "symétrique par rapport à l'axe des x" du point d'intersection de la "droite joignant" les points $(x, y), (x', y')$ (*resp.* de la droite "tangente" au point (x, y) à E) avec la courbe elliptique.

b. La loi de groupe (additif) de (E)

Elle est définie par utilisation immédiate du lemme précédent et est schématisée par le tableau suivant :

$M = (x, y)$ et $M' = (x', y')$ sont deux points de (E) ; alors :

(i) $M + \Omega = \Omega + M = M$ quel que soit M

(ii) Si M et M' sont distincts de Ω on pose : $M + M' = M''$ avec :

a. si $x = x'$ et $y = -y'$, $M'' = \Omega$

b. Sinon soit λ l'élément de $\mathbb{K}$ défini par : $\lambda = \frac{y'-y}{x'-x}$ si $x \neq x'$, $\lambda = \frac{3x^2+a}{2y}$ si $x = x'$ et $y \neq 0$; alors : $M'' = (u, v)$ où le couple (u, v) a été défini dans le lemme précédent *ie* :

$$\begin{cases} u = \lambda^2 - (x + x') \\ v = \lambda(x - u) - y \end{cases}$$

Alors on peut montrer :

Proposition 8 : L'ensemble (E) muni de l'addition ainsi définie est un groupe abélien.

Seule la vérification (ou preuve) de l'associativité est laborieuse ; c'est la raison pour laquelle elle est laissée aux soins du lecteur et on peut dire, *via* ce qui précède, que M, M', M'' de (E) sont "alignés" *si et seulement si* l'un quelconque de ces trois points est l'opposé de la somme des deux autres, autrement dit *si et seulement si* :

$$M + M' + M'' = \Omega$$

L'ensemble $((E), +)$ constituant un groupe abélien fini c'est le moment de rappeler (sans démonstration) le théorème fondamental sur les groupes abéliens finis.

Proposition 9 : Soit G un groupe abélien fini ; alors il existe des entiers $n_1, n_2, \ldots, n_r$ avec $n_1 \geq 2$ et n_i divisant n_{i+1}, pour $i = 1, 2, \ldots, r-1$, tels que :

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

(n_r est l'exposant de G et chacun des $\mathbb{Z}/n_i\mathbb{Z}$ étant muni de l'addition).

Admettons aussi le résultat suivant relatif à toute courbe elliptique sur un corps fini $\mathbb{K}$ de caractéristique $p \geq 5$.

Soit m un entier divisant l'ordre du groupe de la courbe elliptique (E) ; alors il y a au plus m^2 points de (E) d'ordre m ; ceci étant admis nous pouvons alors énoncer :

Proposition 10 : Soit (E) une courbe elliptique sur un corps $\mathbb{K}$ fini de caractéristique ≥ 5 ; soit le groupe $(E,+)$ est cyclique, soit il existe deux entiers n_1 et n_2, $n_1 \geq 2$, n_1 divisant n_2 tel que :

$$((E),+) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

En outre si le cardinal de $((E),+)$ est égal au produit de deux nombres premiers distincts, le groupe $((E),+)$ est cyclique.

Démonstration : Cette proposition est "algébriquement" intéressante car elle précise particulièrement bien la structure du groupe additif d'une courbe elliptique sur un corps fini $\mathbb{K}$.

(i) Supposons, avec les notations utilisées dans la proposition précédente, que l'entier r soit supérieur strictement à 1, *ie* que le groupe $((E),+)$ n'est pas cyclique et montrons qu'alors $r = 2$.

En effet, si nous supposons $r \geq 3$, soit p un facteur premier de n_1 ; dans chacun des groupes cycliques $(\mathbb{Z}/n_i\mathbb{Z},+)$ il existe, puisque p divise n_i, un et un seul sous-groupe (cyclique d'ailleurs) G_i d'ordre p et si $x = (a_1, a_2, \ldots, a_r) \in \prod_{i=1}^{n} G_i$, x est d'ordre p dans $\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$, sauf si $x = (0, 0, \ldots, 0)$; par conséquent il y a : $p^r - 1 \geq p^3 - 1$ éléments du groupe $((E),+)$ qui sont d'ordre p et comme $p^3 - 1 > p^2$ cela n'est pas possible, d'où la preuve de la première partie de la proposition.

Remarque 1 : n_2 est alors l'ordre maximum de tout sous-groupe cyclique du groupe de la courbe elliptique (E) ; c'est donc l'exposant du groupe.

(ii) Supposons maintenant en désignant par n le nombre d'éléments du groupe $((E),+)$ que l'on ait $n = pq$ avec p et q premiers distincts et montrons qu'alors on a affaire à un groupe cyclique.

En effet, cela résulte du corollaire de la proposition 10 établie dans cet ouvrage dans le chapitre des groupes abéliens.

Remarque 2 : Soit p un nombre premier, $p \geq 7$ et $(\mathcal{L},+)$ une courbe elliptique sur $\mathbb{F}_p$; s'il existe un élément du groupe $(\mathcal{L},+)$ d'ordre p, $(\mathcal{L},+)$ est cyclique et possède alors p éléments. En effet, si $m = card\ \mathcal{L}$, p divise m (Lagrange) et $m < 2p$ puisque $p \geq 7$; d'où $p = m$ ce qui prouve ce que nous voulions.

Par contre, si $p = 5$, le groupe de la courbe elliptique définie par : $y^2 = x^3 + 3x$ possède 10 éléments ; il est donc isomorphe à $\mathbb{Z}/(2) \times \mathbb{Z}/(5) = \mathbb{Z}/(10)$ et possède 4 éléments d'ordre 5 mais, bien que cyclique, n'est pas un groupe à 5 éléments.

Remarque 3 : Admettons, (la preuve étant laissée aux soins du lecteur), que si $((E),+)$ est le groupe additif d'une courbe elliptique sur le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, l'entier n_1 (voir proposition 10) divise $p - 1$.

On suppose, en outre, que les hypothèses de la proposition 7 sont valables, c'est-à-dire que p est égal à 2 modulo 3, et que l'équation de E est du type :

$$y^2 = x^3 + b$$

On a donc affaire à une courbe supersingulière.

Comme : $n_1 n_2 = p + 1$, n_1 divise à la fois $p - 1$ et $p + 1$; ainsi soit $n_1 = 1$ et alors $(E, +)$ est cyclique et isomorphe à $(\mathbb{Z}/(p+1), +)$; soit $n_1 = 2$ et alors $(E, +)$ est isomorphe au groupe produit (additif) : $\mathbb{Z}/(2) \times \mathbb{Z}/(\frac{p+1}{2})$.

$p \geq 5$ étant égal à 2 modulo 3, sur toute courbe elliptique sur $\mathbb{F}_p$ d'équation $y^2 = x^3 + b$ ($b \neq 0$) il y a un seul élément d'ordre 2 *ie* du type $(\alpha, 0)$, par conséquent :

(i) Si $\frac{p+1}{2}$ est pair de la forme : $\frac{p+1}{2} = 2m$, le groupe additif $\mathbb{Z}/(2) \times \mathbb{Z}/(2m)$ possède trois éléments d'ordre 2, à savoir : $(\bar{1}, \bar{\bar{0}})$, $(\bar{0}, \bar{\bar{m}})$, $(\bar{1}, \bar{\bar{m}})$; dans ces conditions le groupe $(E, +)$ associé à la courbe elliptique ne peut pas être isomorphe à $\mathbb{Z}/(2) \times \mathbb{Z}(2m)$; il est donc cyclique.

(ii) Si $\frac{p+1}{2}$ est impair, 2 et $\frac{p+1}{2}$ sont premiers entre eux et $\mathbb{Z}/(2) \times \mathbb{Z} \Big/ \left(\frac{p+1}{2}\right)$ est isomorphe à $\mathbb{Z}/(p+1)$; ainsi :

Si $(E, +)$ est le groupe associé à la courbe elliptique $y^2 = x^3 + b$ sur $\mathbb{F}_p$ avec $p = 2 \pmod 3$, $(E, +)$ est cyclique et isomorphe à $\mathbb{Z}/(p+1)\mathbb{Z}$.

Etude de quelques exemples : Le polynôme $X^2 + 2$ est irréductible dans l'anneau $\mathbb{F}_5[X]$; par conséquent le quotient $\mathbb{F}_5[X]/(X^2+2)$ où (X^2+2) désigne l'idéal engendré dans $\mathbb{F}_5[X]$ par ce polynôme, est un corps que nous notons $\mathbb{K}$ (dans cet exemple), de caractéristique 5 et ayant 25 éléments ; si $\alpha = \bar{X}$ (classe de X) l'élément générique de $\mathbb{K}$ s'écrit $a + b\alpha$ avec $a, b \in \mathbb{F}_5$; nous conviendrons de le noter (a, b) ; ainsi dans $\mathbb{K}$: $(a, b) + (a', b') = (a + a', b + b')$; $(a, b) \bullet (a', b') = (aa' - 2bb' ; ab' + a'b)$.

Exemple 1 :

Prenons maintenant sur le corps $\mathbb{K}$ la courbe $\mathcal{L} : y^2 = x^3 + x + 3$ et déterminons ses points à l'aide du tableau ci-dessous :

x	x^2	$x^3 + x + 3$	Points de $\mathcal{L}$
$(0,0)$	$(0,0)$	$(3,0)$	$((0,0);(0,4));((0,0);(0,1))$
$(0,1)$	$(-2,0)$	$(3,4)$	$((0,1);(1,2));((0,1);(4,3))$
$(0,2)$	$(2,0)$	$(3,1)$	$((0,2);(1,3));((0,2);(4,2))$
$(0,3)$	$(2,0)$	$(3,4)$	$((0,3);(1,2));((0,3);(4,3))$
$(0,4)$	$(3,0)$	$(3,1)$	$((0,4);(4,2));((0,4);(1,3))$
$(1,0)$	$(1,0)$	$(0,0)$	$((1,0);(0,0))$
$(1,1)$	$(-1,2)$	$(4,2)$	$((1,1);(4,4));((1,1);(1,1))$
$(1,2)$	$(-2,4)$	$(1,2)$	$((1,2);(3,2));((1,2);(2,3))$
$(1,3)$	$(-2,1)$	$(1,3)$	$((1,3);(3,3));((1,3);(2,2))$
$(1,4)$	$(-1,3)$	$(4,3)$	$((1,4);(4,1));((1,4);(1,4))$

x	x^2	x^3+x+3	Points de $\mathcal{L}$
$(2,0)$	$(4,0)$	$(3,0)$	$((2,0);(0,4));((2,0);(0,1))$
$(2,1)$	$(2,4)$	$(1,1)$	aucun
$(2,2)$	$(-4,3)$	$(0,0)$	$((2,2);(0,0))$
$(2,3)$	$(1,2)$	$(0,0)$	$((2,3);(0,0))$
$(2,4)$	$(-3,1)$	$(1,4)$	aucun
$(3,0)$	$(4,0)$	$(3,0)$	$((3,0);(0,4));((3,0);(0,1))$
$(3,1)$	$(2,1)$	$(0,1)$	aucun
$(3,2)$	$(1,2)$	$(1,0)$	$((3,2);(4,0));((3,2);(1,0))$
$(3,3)$	$(1,3)$	$(1,0)$	$((3,3);(4,0));((3,3);(1,0))$
$(3,4)$	$(2,4)$	$(0,4)$	aucun
$(4,0)$	$(1,0)$	$(1,0)$	$((4,0);(1,0));((4,0);(4,0))$
$(4,1)$	$(4,3)$	$(2,2)$	aucun
$(4,2)$	$(3,1)$	$(0,2)$	aucun
$(4,3)$	$(3,4)$	$(0,3)$	aucun
$(4,4)$	$(4,2)$	$(2,3)$	aucun

Sans oublier le point Ω ; en définitive $\mathcal{L}$ possède 32 éléments.

On voit que sur le corps $\mathbb{K}$, le polynôme X^3+X+3 est scindé et admet pour racine $(1,0),(2,2)$ et $(2,3)$; il y a donc trois éléments d'ordre 2 dans le groupe $(\mathcal{L},+)$; par conséquent le groupe $(\mathcal{L},+)$ n'est pas cyclique (car sinon il n'y aurait qu'un seul élément d'ordre 2 d'après la proposition 5 du chapitre 2).

Cette remarque, jointe à la proposition précédente, montre que $(\mathcal{L},+)$ est isomorphe au groupe $\mathbb{Z}/2\times\mathbb{Z}/16$ dont les 3 éléments d'ordre 2 sont $(\bar{1},\bar{\bar{0}})$,$(\bar{0},\bar{\bar{8}})$, $(\bar{1},\bar{\bar{8}})$.

Exemple 2 : Sur $\mathbb{F}_5[X]/(X^2+2)$, $\mathcal{L}'$ est définie par : $y^2=x^3+2x+1$.

x	x^2	x^3+2x+1	Points de $\mathcal{L}'$
$(0,0)$	$(0,0)$	$(1,0)$	$((0,0);(1,0));((0,0);(4,0))$
$(0,1)$	$(3,0)$	$(1,0)$	$((0,1);(1,0));((0,1);(4,0))$
$(0,2)$	$(2,0)$	$(1,3)$	$((0,2);(3,3));((0,2);(2,2))$
$(0,3)$	$(2,0)$	$(1,2)$	$((0,3);(2,3));((0,3);(3,2))$
$(0,4)$	$(3,0)$	$(1,0)$	$((0,4);(1,0));((0,4);(4,0))$
$(1,0)$	$(1,0)$	$(4,0)$	$((1,0);(2,0));((1,0);(3,0))$
$(1,1)$	$(4,2)$	$(3,3)$	aucun
$(1,2)$	$(3,4)$	$(0,4)$	aucun
$(1,3)$	$(3,1)$	$(0,1)$	aucun
$(1,4)$	$(4,3)$	$(3,2)$	aucun

x	x^2	x^3+3	Points de $\mathcal{L}''$
$(2,0)$	$(4,0)$	$(3,0)$	$((2,0);(0,4));((2,0);(0,1))$
$(2,1)$	$(2,4)$	$(1,2)$	$((2,1);(2,3));((2,1);(3,2))$
$(2,2)$	$(1,3)$	$(0,2)$	aucun
$(2,3)$	$(1,2)$	$(0,3)$	aucun
$(2,4)$	$(2,1)$	$(1,3)$	$((2,4);(3,3));((2,4);(2,2))$
$(3,0)$	$(4,0)$	$(4,0)$	$((3,0);(3,0));((3,0);(2,0))$
$(3,1)$	$(2,1)$	$(1,2)$	$((3,1);(3,2));((3,1);(2,3))$
$(3,2)$	$(1,2)$	$(2,2)$	aucun
$(3,3)$	$(1,3)$	$(2,3)$	aucun
$(3,4)$	$(2,4)$	$(1,3)$	$((3,4);(2,2));((3,4);(3,3))$
$(4,0)$	$(1,0)$	$(3,0)$	$((4,0);(0,4));((4,0);(0,1))$
$(4,1)$	$(4,3)$	$(4,3)$	$((4,1);(4,1));((4,1);(1,4))$
$(4,2)$	$(3,1)$	$(2,4)$	$((4,2);(2,1));((4,2);(3,4))$
$(4,3)$	$(3,4)$	$(2,1)$	$((4,3);(2,4));((4,3);(3,1))$
$(4,4)$	$(4,2)$	$(4,2)$	$((4,4);(4,4));((4,4);(1,1))$
		$+\Omega$	

Bilan : $card\ \mathcal{L}' = 35 = 5 \times 7$; donc $(\mathcal{L}', +) \cong \mathbb{Z}/(5) \times \mathbb{Z}/(7) = \mathbb{Z}/(35)$ est cyclique.

Exemple 3 : sur le même corps : $\mathcal{L}'' : y^2 = x^3 + 3$.

x	x^2	x^3+3	Points de $\mathcal{L}''$
$(0,0)$	$(0,0)$	$(3,0)$	$((0,0);(0,4));((0,0);(0,1))$
$(0,1)$	$(3,0)$	$(3,3)$	aucun
$(0,2)$	$(2,0)$	$(3,4)$	$((0,2);(1,2));((0,2);(4,3))$
$(0,3)$	$(2,0)$	$(3,1)$	$((0,3);(4,2));((0,3);(1,3))$
$(0,4)$	$(3,0)$	$(3,2)$	aucun
$(1,0)$	$(1,0)$	$(4,0)$	$((1,0);(2,0));((1,0);(3,0))$
$(1,1)$	$(4,2)$	$(3,1)$	$((1,1);(4,2));((1,1);(1,3))$
$(1,2)$	$(3,4)$	$(0,0)$	$((1,2);(0,0))$
$(1,3)$	$(3,1)$	$(0,0)$	$((1,3);(0,0))$
$(1,4)$	$(4,3)$	$(3,4)$	$((1,4);(4,3));((1,4);(1,2))$
$(2,0)$	$(4,0)$	$(1,0)$	$((2,0);(1,0));((2,0);(4,0))$
$(2,1)$	$(2,4)$	$(4,0)$	$((2,1);(2,0));((2,1);(3,0))$
$(2,2)$	$(1,3)$	$(3,3)$	aucun
$(2,3)$	$(1,2)$	$(3,2)$	aucun
$(2,4)$	$(2,1)$	$(4,0)$	$((2,4);(2,0));((2,4);(3,0))$
$(3,0)$	$(4,0)$	$(0,0)$	$((3,0);(0,0))$
$(3,1)$	$(2,1)$	$(2,0)$	$((3,1);(0,2));((3,1);(0,3))$
$(3,2)$	$(1,2)$	$(3,3)$	aucun
$(3,3)$	$(1,3)$	$(3,2)$	aucun
$(3,4)$	$(2,4)$	$(2,0)$	$((3,4);(0,2));((3,4);(0,3))$

x	x^2	x^3+3	Points de $\mathcal{L}''$
$(4,0)$	$(1,0)$	$(2,0)$	$((4,0);(0,2));((4,0);(0,3))$
$(4,1)$	$(4,3)$	$(3,1)$	$((4,1);(4,2));((4,1);(1,3))$
$(4,2)$	$(3,1)$	$(1,0)$	$((4,2);(1,0));((4,2);(4,0))$
$(4,3)$	$(3,4)$	$(1,0)$	$((4,3);(1,0));((4,3);(4,0))$
$(4,4)$	$(4,2)$	$(3,4)$	$((4,4);(4,3));((4,4);(1,2))$

Bilan : Le cardinal de $\mathcal{L}''$ est maximum (d'après le théorème de Hasse) puisque $\mathcal{L}''$ possède 36 points : $36 = 2\sqrt{q} + (q+1)$ avec $q = 25$.

Pour finir l'étude de la courbe elliptique $\mathcal{L}''$ il est nécessaire d'en préciser la structure algébrique.

Compte tenu du théorème fondamental (proposition 11 chapitre **2**) relatif aux groupes abéliens, le groupe $(\mathcal{L}'', +)$ ne peut être isomorphe qu'à un des 4 groupes additifs suivants :

$$\mathbb{Z}/(2) \times \mathbb{Z}/(18),\ \mathbb{Z}/(3) \times \mathbb{Z}/(12),\ \mathbb{Z}/(6) \times \mathbb{Z}/(6),\ \text{ou } \mathbb{Z}/(36)$$

Comme il y a trois éléments d'ordre 2 (voir le tableau) dans $(\mathcal{L}'', +)$ il est impossible que $(\mathcal{L}'', +)$ soit isomorphe au groupe cyclique $\mathbb{Z}/(36)$; en effet, on sait que dans un groupe cyclique ayant n éléments il n'existe pour d divisant n qu'un sous-groupe ayant d éléments (proposition 5 chapitre **2**).

Le groupe produit $\mathbb{Z}/(3) \times \mathbb{Z}/(12)$ n'a qu'un élément d'ordre 2, à savoir $(\bar{0}, \bar{\bar{6}})$, il n'est donc pas isomorphe à $(\mathcal{L}'', +)$.

Les éléments : $\alpha = ((1,4),(1,2)), \alpha' = ((2,1),(2,0)), \alpha'' = ((0,2),(1,2))$, $\alpha''' = ((4,0),(0,2))$ sont d'ordre 6 dans $(\mathcal{L}'', +)$ (vérification aisée).

On a, en outre : $2\alpha = ((4,2),(1,0)) = 2\alpha'$, $2\alpha' = ((2,0),(1,0))$ et : $2\alpha'' = ((0,0),(0,2))$.

Ainsi, il y a dans $(\mathcal{L}'', +)$ au moins trois éléments distincts d'ordre 3 ; dans le groupe $\mathbb{Z}/(2) \times \mathbb{Z}/(18)$ les seuls éléments d'ordre 3 sont $(\bar{0}, \bar{\bar{6}})$, $(\bar{0}, \bar{\bar{12}})$; il n'y en a que deux.

Bilan :

$$(\mathcal{L}'', +) \cong \mathbb{Z}/(6) \times \mathbb{Z}/(6)$$

Exemple 4 : Prenons le corps $\mathbb{F}_{71}$ et considérons sur ce corps la courbe elliptique d'équation :

$$y^2 = x^3 - x$$

Un travail effectué par l'ordinateur prouve que le groupe additif de cette courbe possède 72 éléments ; c'est donc une courbe supersingulière ; l'exposant du groupe considéré est égal à 36 ; par conséquent par application de la proposition 10 ce groupe est isomorphe au groupe additif du produit $\mathbb{Z}/(2) \times \mathbb{Z}/(36)$; or comme : $\mathbb{Z}/(36)$ est isomorphe à $\mathbb{Z}/(4) \times \mathbb{Z}/(9)$ (proposition 4 du chapitre **3**) il en résulte que le groupe additif de cette courbe est isomorphe à $\mathbb{Z}/(4) \times \mathbb{Z}/(18)$.

7.2.4 Le cryptosystème El-Gamal à partir d'une courbe elliptique.

a. Cas où le corps est un $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ avec $p \geq 5$ premier

(i) Sa clé est définie par le quintuplet : $K = (p, \alpha, \beta, m, \mathcal{L})$ où $p \geq 5$ est un nombre premier, $\mathcal{L}$ une courbe elliptique sur le corps de Frobénius $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, α un élément de $\mathcal{L}$ engendrant un sous-groupe cyclique H d'ordre maximum ($\mathcal{L}$ si possible, *ie* dans le cas où le groupe $(\mathcal{L}, +)$ est lui-même cyclique), et β l'élément de H défini par $\beta = m\alpha$.

p, α, β et $\mathcal{L}$ sont publics ; m est la partie cachée de la clé K.

(ii) L'ensemble E des textes à coder est ici défini par : $E = \mathbb{F}_p \times \mathbb{F}_p$; l'ensemble E' des textes codés est alors défini par : $E' = \mathcal{L} \times E$.

(iii) La fonction de codage est, comme dans tout système cryptographique de type El-Gamal, de nature probabiliste, et se constitue de la façon suivante : si $x = (x_1, x_2) \in E$, l'expéditeur du message choisit un entier k arbitraire et calcule y_0, y_1, y_2 tels que :

$$\begin{cases} y_0 = k\alpha \\ y_1 = c_1 x_1 \pmod p \\ y_2 = c_2 x_2 \pmod p \end{cases}$$

où le couple (c_1, c_2) est défini par : $k\beta = (c_1, c_2)$ et $c_1 c_2 \neq 0 \pmod p$; si jamais le choix de l'entier k conduit à $c_1 c_2 = 0 \pmod p$, l'expéditeur change d'entier k ; au terme de ces calculs il définit alors $e(x)$ par l'égalité :

$$e(x) = (y_0, y_1, y_2)$$

(iv) La fonction de déchiffrement, commune à toutes les fonctions de codage possibles, est alors définie, comme on le vérifie aisément, par :

$$d(y_0, y_1, y_2) = (y_1 c_1^{-1} \pmod p, y_2 c_2^{-1} \pmod p)$$

où le couple (c_1, c_2) est calculé par le destinataire à l'aide de la partie cachée m de sa clé K, puisque :

$$(c_1, c_2) = m y_0$$

En définitive la courbe elliptique $\mathcal{L}$ a joué le rôle de "masque" dans le protocole de transmission du message $x = (x_1, x_2)$; ce masque est d'autant plus difficile à "casser" que le problème du logarithme discret est difficile dans le groupe H engendré par α, ce qui est assez souvent réalisé, car la loi de groupe (additive) d'une courbe elliptique est, comme nous l'avons déjà souligné, "diffuse".

Exemples :

$$(p = 251; \alpha = (183, 21); \beta = (221, 141); \mathcal{L} : y^2 = x^3 + 2x + 4; m = 58)$$

ou :

$$(p = 251; \alpha = (130, 38); \beta = (4, 1171); \mathcal{L} : y^2 = x^3 + 11x + 17; m = 85)$$

sont deux jeux de clés d'un El-Gamal elliptique, où dans chaque cas, le groupe $(\mathcal{L}, +)$ est cyclique avec 231 (*resp.* 258) éléments.

b. Cas où le corps $\mathbb{K}$ a p^n éléments, $p \geq 5$ premier et $n \geq 2$

On peut, si on le souhaite, constituer un système cryptographique, du même type, à partir d'une courbe elliptique non plus définie sur un corps de Frobénius $\mathbb{F}_p$ mais sur un corps de caractéristique $p \geq 5$ ayant p^n éléments avec n entier, $n \geq 2$.

Dans ces conditions, la clé K du cryptosystème est définie par la liste : $K = (\mathbb{K}; \alpha; \beta; m; \mathcal{L})$ où $\mathbb{K}$ est un corps (ayant p^n éléments) à préciser afin que soit connue la règle de multiplication dans $\mathbb{K}$; $\mathbb{K}$ sera toujours constitué en "quotientant" l'anneau $\mathbb{F}_p[X]$ par un polynôme unitaire irréductible de degré n de l'anneau $\mathbb{F}_p[X]$.

Il est important d'apporter la précision fixant la multiplication dans $\mathbb{K}$ car, même si tous les corps ayant p^n éléments sont isomorphes, il n'y a pas de "règle standard" définissant la multiplication dans $\mathbb{K}$ une fois pour toutes.

α est alors un élément de la courbe elliptique $(\mathcal{L}, +)$ et $\beta = m\alpha$, α ayant été choisi de telle sorte, encore une fois, que le sous-groupe de $\mathcal{L}$ engendré par α soit le plus "gros" possible. $\mathbb{K}, \mathcal{L}, \alpha$ et β sont publiés ; seul m est maintenu secret. L'ensemble des messages est $E = \mathbb{K} \times \mathbb{K}$, et l'ensemble E' des textes codés est : $\mathcal{L} \times E$.

Pour coder $x = (x_1, x_2) \in \mathbb{K}^2$, l'expéditeur effectue alors les opérations suivantes :

- il calcule, k étant un entier arbitraire, $y_0 = k\alpha \in \mathcal{L}$ et $k\beta = (c_1, c_2)$ en veillant que $c_1 c_2 \neq 0$ sinon il change d'entier k.
- il calcule ensuite sans le corps $\mathbb{K}$: $y_1 = c_1 x_1, y_2 = c_2 x_2$ et il envoie $e(x) = (y_0, y_1, y_2) \in \mathcal{L} \times \mathbb{K}^2$;

Le protocole de décodage est alors, bien évidemment, défini par :

$$d(y_0, y_1, y_2) = (y_1 c_1^{-1}, y_2 c_2^{-1})$$

les éléments c_1 et c_2 de $\mathbb{K}$ étant déterminés par le destinataire des messages puisque :

$$m y_0 = (c_1, c_2)$$

Etude d'un exemple : on reprend $p = 5$ et on construit le corps $\mathbb{K}$ en posant : $\mathbb{K} = \mathbb{F}_5[X]/(X^2 + 2)$ puisque $X^2 + 2$ est un polynôme irréductible de $\mathbb{F}_5[X]$; l'idéal $(X^2 + 2)$ engendré par ce polynôme est donc maximal dans l'anneau $\mathbb{F}_5[X]$ et, de ce fait, le quotient algébrique $\mathbb{K}$ est un corps ayant 25 éléments.

Il constitue l'unique (à un isomorphisme près) corps $\mathbb{K}$ ayant 25 éléments qui sont du type :

$$a + b\omega \text{ où } \omega^2 = -2$$

un tel élément sera encore représenté schématiquement par le couple (a, b) avec $a, b \in \mathbb{F}_5$. Alors on peut écrire comme nous l'avons vu précédemment :

$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b) \times (a', b') = (aa' - 2bb'; ab' + ba')$$

Considérons alors la courbe elliptique, sur le corps $\mathbb{K}$, définie par l'équation :

$$y^2 = x^3 + x + 1$$

le tableau ci-dessous détermine les points de cette courbe elliptique sur $\mathbb{K}$.

x	x^2	x^3	x^3+3	Points de $\mathcal{L}$
$(0,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$((0,0);(1,0));((0,0);(4,0))$
$(0,1)$	$(-2,0)$	$(0,-2)$	$(1,4)$	aucun
$(0,2)$	$(2,0)$	$(0,-1)$	$(1,1)$	aucun
$(0,3)$	$(2,0)$	$(0,1)$	$(1,4)$	aucun
$(0,4)$	$(3,0)$	$(0,-3)$	$(1,1)$	aucun
$(1,0)$	$(1,0)$	$(1,0)$	$(3,0)$	$((1,0);(0,4));((1,0);(0,1))$
$(1,1)$	$(-1,2)$	$(0,1)$	$(2,2)$	aucun
$(1,2)$	$(-2,4)$	$(-3,0)$	$(-1,2)$	$((1,2);(1,1));((1,2);(4;4))$
$(1,3)$	$(-2,1)$	$(-3,0)$	$(-1,3)$	$((1,3);(1,4));((1,3);(4,1))$
$(1,4)$	$(-1,3)$	$(0,4)$	$(2,3)$	aucun
$(2,0)$	$(4,0)$	$(3,0)$	$(1,0)$	$((2,0);(1,0));((2,0);(4,0))$
$(2,1)$	$(2,4)$	$(1,0)$	$(4,1)$	aucun
$(2,2)$	$(-4,3)$	$(0,3)$	$(3,0)$	$((2,2);(0,4));((2,2);(0,1))$
$(2,3)$	$(1,2)$	$(0,2)$	$(3,0)$	$((2,3);(0,4));((2,3);(0,1))$
$(2,4)$	$(-3,1)$	$(1,0)$	$(4,4)$	aucun
$(3,0)$	$(4,0)$	$(2,0)$	$(1,0)$	$((3,0);(1,0));((3,0);(4,0))$
$(3,1)$	$(2,1)$	$(-1,0)$	$(3,1)$	$((3,1);(1,3));((3,1);(4,2))$
$(3,2)$	$(1,2)$	$(0,-2)$	$(4,0)$	$((3,2);(2,0));((3,2);(3,0))$
$(3,3)$	$(-4,3)$	$(0,-3)$	$(4,0)$	$((3,3);(2,0));((3,3);(3,0))$
$(3,4)$	$(2,4)$	$(-1,0)$	$(4,0)$	$((3,4);(4,3));((3,4);(1,2))$
$(4,0)$	$(1,0)$	$(-1,0)$	$(4,0)$	$((4,0);(2,0));((4,0);(3,0))$
$(4,1)$	$(-1,3)$	$(0,-4)$	$(0,-3)$	aucun
$(4,2)$	$(-2,1)$	$(3,0)$	$(3,2)$	aucun
$(4,3)$	$(-2,4)$	$(3,0)$	$(3,3)$	aucun
$(4,4)$	$(-1,2)$	$(0,-1)$	$(0,3)$	aucun

Sans oublier le point Ω de $\mathcal{L}$; nous allons préciser la structure algébrique du groupe $(\mathcal{L},+)$.

Soit $A=((2,3);(0,1))$ on obtient (calculs laissés aux soins du lecteur) $2A=((3,3);(2,0));4A=((3,1);(4,2))$; $9A=\Omega$; avec le point A' de $\mathcal{L}$ défini par $A'=((3,4);(1,2))$ on constate que A' est lui aussi d'ordre 9 ; si $(\mathcal{L},+)$ qui a 27 éléments était cyclique, il possèderait un seul sous-groupe d'ordre 9 et donc 6 éléments d'ordre 9, ce qui n'est pas le cas ici ; ainsi on peut écrire :

$$(\mathcal{L},+)\cong\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$$

De ce fait le plus "gros" sous-groupe cyclique de $(\mathcal{L},+)$ possède 9 éléments ; soit $H=\{A,2A,\ldots,8A,\Omega\}$. On choisit donc, ici, *via* les notations utilisées :

$$\alpha=((2,3);(0,1))$$

Choisissons ensuite $m = 7$; alors $\beta = 7A = ((3,3);(3,0))$. La clé K de notre cryptosystème est définie par :

$$K = (\mathbb{K} = \mathbb{F}_5[X]/(X^2+2); \alpha = ((2,3);(0,1)); \beta = ((3,3);(3,0)); m = 7;$$
$$\mathcal{L} = \{(x,y) \in \mathbb{K}^2 : y^2 = x^3 + x + 1\})$$

seul l'entier 7 constitue la partie cachée de la clé K et c'est le logarithme discret de $((3,3);(3,0))$ en base $((2,3);(0;1))$ dans le sous-groupe cyclique H de la courbe elliptique $\mathcal{L}$ définie sur le corps $\mathbb{K}$, comme il vient d'être dit.

Supposons que l'on veuille coder le message : $x = ((4,1);(3,2))$ de $\mathbb{K} \times \mathbb{K}$; ici $x_1 = (4,1)$ et $x_2 = (3,2)$. Choisissons : $k = 4$, ainsi : $y_0 = 4A = ((3,1);(4,2)) = 4\alpha$.

Puis il faut calculer $k\beta = 4\beta$ et on trouve :

$$k\beta = ((2,3);(0,1))$$

d'où :

$$y_1 = (4,1) \cdot (2,3) = (2,4)$$

et

$$y_2 = (3,2) \cdot (0,1) = (1,3)$$

Pour décoder il faut calculer $7y_0 = y_0 + 2y_0 + 2(2y_0)$ et on trouve : $2y_0 = ((2,3);(0,4))$, $4y_0 = ((3,3);(3,0))$; $3y_0 = ((2,0);(1,0))$ et enfin : $7y_0 = ((2,3);(0,1)) = (c_1, c_2)$, ce qui permet de terminer, pour le destinataire, le déchiffrement du message $x = ((4,1);(3,2))$.

Nous renvoyons le lecteur au paragraphe **6.9** de cet ouvrage où l'utilisation concomitante de la loi de réciprocité quadratique et des nombres premiers de Mersenne a permis de construire un système cryptographique de type El-Gamal sur $\mathbb{F}_2^n$ avec $n = 509$, sécurisé, en ce sens qu'il n'est pas "cassable", en un temps raisonnable, à l'aide des algorithmes de Shanks ou de Pohlig.

La morale de tout ce qui vient d'être dit c'est qu'il n'est pas possible d'étudier la cryptologie si l'on se prive de la richesse de l'arithmétique modulaire, ce qui justifie, encore une fois, *nolens volens*, l'organisation programmatique de cet ouvrage.

Chapitre 8

Protocoles de signature et d'identification numériques

8.1 Définitions et exemples

a. Introduction

Soit x un message transmis (*via* un canal de communication numérique) à partir du cryptosystème (en général à clé publique) du destinataire ; afin que celui-ci soit capable d'identifier l'expéditeur du message qu'il vient de recevoir, il convient que ce dernier signe de manière incontestable et qu'il soit possible, à tout moment, de vérifier la signature de l'expéditeur, par toute personne ou autorité connaissant l'algorithme public de vérification des signatures.

Toutes ces contraintes sont satisfaites, comme la suite va le montrer, dès lors que la signature du message "dépend" du message envoyé.

b. Protocole de signature numérique

Définition : On appelle *protocole de signature électronique (numérique)* un quintuplet :

$$(K, E, E', s, \sigma)$$

où :

- K est la clé du protocole c'est à dire un ensemble fini de paramètres mathématiques nécessaires à l'élaboration des signatures et des vérifications
- E est l'ensemble fini des messages à signer
- E' est l'ensemble fini des signatures
- s est une application de E dans E', appelée *fonction signature*, qui à tout $x \in E$ associe $s(x) \in E'$

– σ est une application de $E \times E'$ dans $\{0,1\}$, appelée *fonction de vérification*, définie par :

$$\sigma(x,y) = 1 \textit{ si et seulement si } y = s(x)$$
$$\sigma(x,y) = 0 \text{ sinon } \textit{ie} \text{ si } y \neq s(x)$$

La clé K du protocole de signature doit être telle que seul l'expéditeur du message x est capable de calculer (en un temps raisonnable) la signature $y = s(x)$; par contre n'importe qui doit être en mesure (connaissant le message) de vérifier la signature ; autrement dit le protocole de signature est privé mais celui de sa vérification est public.

Dans tout ce qui suit, nous invitons le lecteur à constater que tous les protocoles mathématiques présentés utilisent uniquement et essentiellement l'arithmétique modulaire dans l'anneau $\mathbb{Z}$.

c. Signatures numériques associées aux grands cryptosystèmes

c.1. La signature RSA

La clé de ce procédé de signature K est définie : $K = (n, p, q, a, b)$ où $n = pq$, p et q étant deux nombres premiers distincts, du même ordre de grandeur (*ie* ayant le même nombre de bits) a et b étant deux entiers de $\{1, 2, \ldots, n\}$ tels que :

$$ab = 1 \pmod{\varphi(n)}$$

où $\varphi(n) = (p-1)(q-1) = \varphi(p)\varphi(q)$ est l'indicateur d'Euler de l'entier n.

Les entiers n et a sont publics, les autres (p, b et q) sont tenus secrets et connus seulement du signataire des messages.

E et E' sont ici égaux à l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ des classes résiduelles modulo n dans $\mathbb{Z}$.

Un message est donc du type $\bar{x}$ avec $1 \leq x \leq n$; dans ces conditions la fonction de signature s est définie par :

$$s(\bar{x}) = \bar{x}^b = x^b \pmod{n}$$

et la fonction de vérification σ est alors définie par :

$$\sigma(x,y) = 1 \Longleftrightarrow y^a = x \pmod{n}$$
$$\sigma(x,y) = 0 \text{ sinon}$$

c.2. Un standard de signature lié au logarithme discret : le D.S.S.

i. La clé du signataire de ce protocole est du type :

$$K = (n, p, \alpha, \beta, a)$$

où : n et p sont des entiers premiers, l'entier p étant un facteur premier du nombre $n-1$ (on peut prendre, par exemple, $n = 2p+1$). L'anneau $\mathbb{Z}/n\mathbb{Z}$ est le corps de Frobénius

$\mathbb{F}_n$; le groupe multiplicatif de ce corps *ie* $(\mathbb{F}_n^*, \times)$ est un groupe cyclique possédant $n-1$ éléments puisque n est premier.

Comme p divise le cardinal de $\mathbb{F}_n^*$, il existe, on le sait, un et un seul sous-groupe cyclique de $\mathbb{F}_n^*$ ayant p éléments (proposition 5 du chapitre **2**).

On suppose que le problème du logarithme discret est difficile à résoudre dans ce sous groupe. Désignons alors par α un générateur de ce sous-groupe *ie* une racine primitive p-ième de 1 dans le corps de Frobénius $\mathbb{F}_n$.

Ensuite on choisit $a \in \{1, 2, \ldots, p\}$ et on pose : $\beta = \alpha^a$ dans $\mathbb{F}_n$.

n, p, α, β sont publics, a est caché (en pratique, n possède 512 bits et p en a 160 dans le cas du **D**igital **S**ignature **S**tandard).

ii. La signature

Ici : $E = \mathbb{F}_n^*$, $E' = \mathbb{F}_p \times \mathbb{F}_p$ où $\mathbb{F}_p$ est le corps de Frobénius $\mathbb{Z}/p\mathbb{Z}$. Soit alors $x \in \mathbb{F}_n^*$ un message ; on prend alors un entier k arbitraire dans l'ensemble $\{1, 2, \ldots, p-1\}$ et on pose : $U = \alpha^k \pmod n$ et ensuite on désigne par u un entier de $\{1, 2, \ldots, p-1\}$ tel que $u = U \pmod p$. Comme k est inversible modulo p, soit v défini modulo p par : $v = (x + au)k^{-1} \pmod p$ et on s'assure que v est non nul modulo p sinon on change d'entier k.

La fonction s est alors définie par :

$$s(x) = (\bar{u}, \bar{v}) \in \mathbb{F}_p \times \mathbb{F}_p$$

où $\bar{u}$ (*resp.* $\bar{v}$) est la classe de u (*resp.* v) modulo p ; cette signature nécessite $2m$ bits si m est le nombre de bits de l'entier premier p.

iii. La fonction σ de vérification

Le destinataire du message calcule alors dans le corps $\mathbb{F}_p$ $\bar{u}_1 = \bar{x}(\bar{v})^{-1}$ et $\bar{v}_1 = \bar{u}(\bar{v})^{-1}$ et ensuite (u_1 et v_1 étant choisis dans $\{1, 2, \ldots, p\}$) :

$$V = \alpha^{u_1}\beta^{v_1} \pmod n$$

Or on a : $V = \alpha^{u_1 + av_1} \pmod n$ et comme dans $\mathbb{F}_p$, $\bar{u}_1 + \bar{a}\bar{v}_1 = (\bar{x} + \bar{a}\bar{u})(\bar{v})^{-1} = \bar{k}\bar{v}(\bar{v})^{-1} = \bar{k}$, l'entier $u_1 + av_1$ est égal à k modulo p ; comme $\alpha^p = 1$ dans $\mathbb{F}_n$, il vient alors :

$$V = \alpha^k \pmod n = U \pmod n$$

et par conséquent :

$$V \pmod p = U \pmod p = \bar{u}$$

D'où : $\sigma(x, (\bar{u}, \bar{v})) = 1$ *si et seulement si* $V = u \pmod p$, et $\sigma(x, (\bar{u}, \bar{v})) = 0$ sinon, et alors la signature est rejetée.

8.2 Un procédé de signature élaboré lié au logarithme discret et à clé jetable

Définition : On dira qu'une signature électronique ne peut être contrefaite si le protocole de signature permet d'élaborer une procédure numérique utilisable par le signataire au terme de laquelle il prouvera qu'il y a eu usurpation de signature.

Autrement dit, si le destinataire du message x possède un couple (x, y) avec $\sigma(x, y) = 1$, la procédure évoquée doit permettre au signataire supposé de prouver éventuellement la contrefaçon.

C'est en ce sens que le protocole de signature qui suit est qualifié de "protocole élaboré".

a. La clé K du procédé de signature

Elle se décline à l'aide de la liste suivante :

$$K = (m, p, \alpha, \beta, a, \delta, \gamma, u, v, u', v')$$

où :

(i) m et p sont deux nombres premiers avec p divisant $m - 1$ (en général on prend $m = 2p + 1$). Comme p divise $m - 1$, dans le groupe multiplicatif du corps $\mathbb{F}_m$, il existe un et un seul sous-groupe G ayant p éléments et il est supposé que l'entier m est tel que le problème du logarithme discret dans $\mathbb{F}_m^*$ est difficile.

(ii) α désigne un générateur du groupe G c'est-à-dire une racine primitive p-ième de 1 modulo m ; a est un entier de $\{1, 2, \ldots, p-1\}$ avec : $\beta = \alpha^a \pmod m$ (a est défini modulo p, $a = \log_\alpha \beta$).
Le quintuplet (m, p, α, β, a) est, par hypothèse, la propriété d'une autorité indépendante ; seul l'entier a est caché, les autres entiers m, p, α, β étant publics *ie* fournis par l'autorité dépositrice du protocole.

(iii) A ce quintuplet, tout signataire adjoint le sextuplet $(\delta, \gamma, u, v, u', v')$ afin de compléter la clé du protocole de signature ; les entiers u, v, u', v' de $\{1, 2, \ldots, p-1\}$ sont cachés, δ et γ étant publiés avec :

$$\delta = \alpha^{u'} \beta^{v'} \pmod m$$
$$\gamma = \alpha^u \beta^v \pmod m$$

b. La fonction de signature

L'ensemble des messages à signer, est ici $E = \mathbb{F}_p$ et l'ensemble E' des signatures est $E \times E$.

Soit donc un x dans $\mathbb{F}_p$; on pose alors :

$$s(x) = (y, z) \text{ où } \begin{cases} y = u + u'x \pmod p \\ z = v + v'x \pmod p \end{cases}$$

c. La fonction σ de vérification

On constate aisément que l'on a :

$$\alpha^y \beta^z \pmod m = \gamma \delta^x \pmod m$$

Par conséquent on posera : $\sigma(x,(y,z)) = 1$ *si et seulement si* $\gamma\delta^x = \alpha^y\beta^z \pmod m$, sinon $\sigma(x,(y,z)) = 0$ (signature rejetée).

d. Etude mathématique de ce mode de signature

(i) Remarquons d'abord qu'il y a plusieurs quadruplets (u,v,u',v') possibles permettant d'obtenir γ et δ ; plus précisément si (u,v,u',v') est l'un d'entre eux, un calcul facile, laissé aux soins du lecteur, montre que tout autre quadruplet (u_1,v_1,u_1',v_1') de $\mathbb{F}_p$ fournissant γ et δ est défini par :

$$u_1 = u - a\lambda, v_1 = v - \lambda, \lambda \in \mathbb{F}_p$$
$$u_1' = u - a\lambda', v_1' = v - \lambda', \lambda' \in \mathbb{F}_p$$

il y en a donc en tout p^2.

(ii) Soit $(\gamma,\delta,u,v,u',v')$ un complément de la clé permettant de signer et x un message de signature $(y,z) = s(x)$; alors il existe p compléments de clé $(\gamma,\delta,u_1,v_1,u_1',v_1')$ tels que $(y,z) = s(x)$. En effet écrivons : $\gamma = \alpha^i, \delta = \alpha^j$ et avec $\beta = \alpha^a$ (tout cela modulo m) on peut écrire matriciellement dans $\mathbb{F}_p$:

$$\begin{pmatrix} i \\ j \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 0 & 1 & a \\ 1 & 0 & x & 0 \\ 0 & 1 & 0 & x \end{pmatrix} \begin{pmatrix} u \\ v \\ u' \\ v' \end{pmatrix} \qquad (**)$$

et la matrice $\begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 0 & 1 & a \\ 1 & 0 & x & 0 \\ 0 & 1 & 0 & x \end{pmatrix}$ a un déterminant nul ; or la sous matrice $\begin{pmatrix} 1 & a & 0 \\ 0 & 0 & 1 \\ 1 & 0 & x \end{pmatrix}$ est inversible ; en d'autres termes, puisque le rang de cette matrice est égal à 3, les solutions de (**) forment un $\mathbb{F}_p$-espace affine de dimension 1 ; il y a donc, comme nous l'annoncions, p compléments de clé possibles tels que $s(x) = (y,z)$; en termes de cryptanalyse, si un intrus connaît x,y,z il n'a qu'une chance sur p de déterminer entièrement la partie utile de la clé du protocole de signature.

(iii) Supposons maintenant que le destinataire du message x reçoive la signature (y',z') venant d'un intrus avec néanmoins $\sigma(x,(y',z')) = 1$; l'expéditeur présumé peut prouver qu'il y a eu usurpation de signature en procédant de la façon suivante .

Soit (y, z) sa propre signature du message x ; on a : $\gamma\delta^x = \alpha^y\beta^z$ et $\gamma\delta^x = \alpha^{y'}\beta^{z'}$ et par conséquent :

$$\alpha^y\beta^z = \alpha^{y'}\beta^{z'}$$

ce qui implique : $(y-y')+a(z-z') = 0 \pmod p$, c'est à dire : $y-y' = a(z'-z)$ dans $\mathbb{F}_p$; comme $z \neq z'$ on a : $a = (y-y')(z'-z)^{-1}$ modulo p et comme l'expéditeur présumé ignore la valeur de l'entier a il peut donc prouver la contrefaçon.

(iv) Soient x_1 et x_2 deux messages distincts avec :

$$s(x_1) = (y_1, z_1) \text{ et } s(x_2) = (y_2, z_2)$$

matriciellement dans $\mathbb{F}_p$ on a :

$$\begin{pmatrix} 1 & 0 & x_1 & 0 \\ 0 & 1 & 0 & x_1 \\ 1 & 0 & x_2 & 0 \\ 0 & 1 & 0 & x_2 \end{pmatrix} \begin{pmatrix} u \\ v \\ u' \\ v' \end{pmatrix} = \begin{pmatrix} y_1 \\ z_1 \\ y_2 \\ z_2 \end{pmatrix}$$

et comme le déterminant de la matrice de ce système vaut $(x_1 - x_2)^2$, on dispose alors d'un système de Cramer ; ainsi on peut facilement déterminer le complément (secret) de la clé K du protocole de signature dès lors que l'on connaît deux messages signés ; par conséquent il faut changer le complément de clé après chaque signature ; on dit alors que le procédé de signature est *à clé jetable.*

Remarque : Si $m = 2p + 1$, le groupe G engendré par α est le groupe des résidus quadratiques du corps $\mathbb{F}_m$ puisque si x appartient à G on a : $x^{\frac{m-1}{2}} = 1 \pmod m$.

Bilan : Ce procédé de signature est aussi difficile à casser que le logarithme discret.

8.3 Un protocole de signature interactif avec l'expéditeur et le destinataire basé sur le logarithme discret

Un protocole de signature est dit *interactif* si la vérification de la signature est le fruit d'un "jeu" de question-réponse de la part du couple expéditeur-destinataire.

a. La clé du procédé de signature

La clé K est définie par : $K = (m, p, \alpha, \beta, a)$ où : m et p sont deux nombres premiers tels que $m = 2p+1$; α est une racine primitive p-ième de l'unité modulo m c'est-à-dire un résidu quadratique (autre que 1) dans $\mathbb{F}_m^*$, a un entier $a \in \{1, 2, \ldots, p-1\}$ et $\beta = \alpha^a \pmod m$.

m, p, α, β sont publics ; a n'est pas dévoilé ; on suppose que le problème du logarithme discret est difficile dans $\mathbb{F}_m^*$.

b. La signature

E et E' sont, ici, le groupe engendré par α *ie* le groupe G des résidus quadratiques de $\mathbb{F}_m^*$.

Soit $x \in G$; on pose alors : $s(x) = y = x^a \pmod m$.

c. La fonction de vérification interactive

Le destinataire choisit k et k' arbitraires dans $\{1, 2, \ldots, p-1\}$ et calcule : $z = y^k \beta^{k'} = x^{ak} \alpha^{ak'} = (x^k \alpha^{k'})^a$; ceci étant fait il fait parvenir au signataire (expéditeur) l'entier z défini modulo m ; étant le seul à connaître a, il désigne par b l'inverse de a modulo p et calcule : $z^b = t$ qu'il renvoie au destinataire ; ainsi :

$$\sigma(x, y) = 1 \text{ si } z^b = t = x^k \alpha^{k'} \pmod m$$
$$\sigma(x, y) = 0 \text{ sinon}$$

La question se trouve dans l'envoi de z et la réponse à cette question est retrouvée par le signataire lorsqu'il retourne l'entier $t = z^b$; le destinataire du couple (x, y) peut donc identifier l'expéditeur.

Remarque : On peut construire un protocole identique en supposant seulement que p premier divise l'entier $m - 1$.

8.4 Mise en forme pratique - Fonctions de hachage

a.

Comme nous l'avons indiqué précédemment, la signature d'un message doit "coller" à celui-ci ; néanmoins si le message est trop long il n'est pas souhaitable (à cause du temps de calcul et de la taille de la signature) de le signer en l'état.

Ce problème technique est résolu par la notion de *fonction de hachage* dont le but est de remplacer tout message par une empreinte numérique binaire "le caractérisant" et de longueur n fixée à l'avance ; en pratique on a toujours $n \leq 512$.

b. Définitions

Etant donné un ensemble E et un entier naturel n, on appelle *fonction de hachage* d'empreinte numérique binaire de longueur n toute application :

$$h : E \longrightarrow \mathbb{F}_2^n$$

très rapide à calculer, telle qu'il est "calculatoirement difficile" de déterminer, $x \in E$ étant donné, un $x' \in E$, x' distinct de x, tel que : $h(x) = h(x')$ et telle que si y est une empreinte numérique, il est "calculatoirement difficile" de trouver un x de E vérifiant $h(x) = y$ (h est alors dite à "sens unique" ("one-way function")).

Etude d'un exemple Soient m et p deux nombres premiers tels que : $m = 2p + 1$, p possédant k bits. Désignons par α et α' deux générateurs du groupe $(\mathbb{F}_m^*, \times)$. Prenons pour E l'ensemble $\mathbb{F}_p \times \mathbb{F}_p$, c'est-à-dire en fait deux suites de k bits et pour $(\bar{x}, \bar{y}) \in \mathbb{F}_p \times \mathbb{F}_p$ soit z l'entier compris entre 0 et $m-1$ tel que :

$$\alpha^x \alpha'^y = z \pmod{m}$$

si $z = \sum_{i=0}^{k} c_i 2^i$ on posera $h(\bar{x}, \bar{y}) = (c_0, c_1, \ldots, c_k) \in \mathbb{F}_2^{k+1}$ et un calcul élémentaire laissé aux soins du lecteur montre qu'il est aussi difficile de trouver $(\bar{x}, \bar{y}) \neq (\bar{x}', \bar{y}')$ tels que $h(\bar{x}, \bar{y}) = h(\bar{x}', \bar{y}')$ que de déterminer le logarithme discret en base α du nombre α'.

c. Mise en forme pratique

Soit E un ensemble de messages tous numérisés en binaire avec au plus m bits.

Soit n' un entier donné (en général $128 \leq n' \leq 512$) ; on supposera que m est un multiple de l'entier n' (sinon on s'y ramène...). Soit alors $x \in E$ du type : $x = c_1 c_2 \ldots c_k$ représenté par une concaténation de k jeux de n' bits c_i avec $c_i \in \mathbb{F}_2^{n'}$.

L'empreinte numérique binaire $h(x)$ du message x est alors déterminée de la manière suivante :

(i) Soit $v_0 \in \mathbb{F}_2^n$ un vecteur d'initialisation et f_i une famille d'applications de $\mathbb{F}_2^n \times \mathbb{F}_2^{n'}$ dans $\mathbb{F}_2^n$ $(i = 1, 2, \ldots, k)$

(ii) Soit $v_1, v_2, \ldots, v_k$ la suite des éléments de $\mathbb{F}_2^n$ définie par :

$$v_i = f_i(v_{i-1}, c_i) \quad i = 1, 2, \ldots, k$$

(par exemple si e_i est une fonction d'encodage de $\mathbb{F}_2^{n'}$ sur $\mathbb{F}_2^n$ on peut prendre : $f_i(x, y) = e_i(x) + y$...)

(iii) On pose alors : $h(x) = v_k$ qui est le résultat final du hachage, et *c'est le haché* $v_k = h(x)$ *qui est signé par l'expéditeur* du message par le biais de son procédé de signature.

Il existe des fonctions de hachage standard qui sont très rapides à exécuter et, de ce fait, très commodes pour signer de longs messages ; les plus connues sont :

- MD5 : (Message digest 5) créée par Rivest qui fournit une empreinte numérique de 128 bits à partir d'un message divisé en blocs de 512 bits ($n' = 512, n = 128$).
- RIPEMD (160-128-256-320) fournissent une empreinte de 128, *resp.* 160.... bits.
- SHA 256 (Secure hash algorithm) fournit une empreinte de 256 bits à partir d'un bloc de 512 bits.
- SHA 512 avec une empreinte de 512 bits à partir de blocs de même taille.
- SNEFRU 128 ou 256 bits.
- WHIRLPOOL avec une empreinte de 512 bits.

En général avant l'opération de hachage (*ie* de compression numérique) on ajoute une chaîne de caractères au message ; ce procédé est connu sous le nom *d'opération de "salage"* ; il permet de renforcer la sécurité de ce protocole. On peut aussi utiliser

les fonctions de hachage lors des "interrogations" informatiques faisant intervenir ces fameux "mots de passe" comme cela a été suggéré au chapitre **7**, en **7.1.b.** ; la fonction f utilisée est alors une fonction de hachage (la plus sûre possible) très rapide à exécuter ; afin d'avoir le maximum de sécurité, on concatène le mot de passe à une chaîne de caractères, avant le hachage ; seul le résultat du hachage est stocké et, pour identifier un utilisateur, l'ordinateur compare l'empreinte de l'information originale qui est stockée avec l'empreinte associée au mot de passe fourni.

Conclusion : Le but de l'algorithme de hachage cryptographique est que la création de l'empreinte (ou condensé) soit la plus rapide possible et que le décryptage soit le plus fastidieux possible ; il faut aussi que la longueur de l'empreinte soit telle qu'une "collision", c'est-à-dire l'obtention de deux messages x et x' distincts ayant la même empreinte soit la plus rare possible ; or on peut montrer qu'avec une empreinte binaire de longueur n, il faut "en moyenne" effectuer $(1,17)2^{n/2}$ hachés pour obtenir une collision ; cela impose $n \geq 128$ et pour plus de sécurité il vaut mieux avoir $n \geq 160$.

Utilisées pour "coder" les mots de passe, les fonctions de hachage nécessitent, pour plus de sécurité, qu'on ajoute au mot de passe avant le hachage, certaines informations seules connues de l'utilisateur (par exemple l'identifiant), le tout étant haché après remplissage et concaténation ; l'ordinateur comparant ensuite les hachés (technique de salage).

En pratique l'empreinte (*ie* le condensé, ou le haché...) est fournie en écriture hexadécimale afin de limiter la longueur de la chaîne de caractères et de faciliter la comparaison des empreintes.

Actuellement toutes les fonctions de hachage fournissant une empreinte binaire de longueur 128 bits sont réputées peu sûres et on attend, semble-t-il pour l'année 2011, un standard de hachage résistant à la cryptanalyse ; la norme actuelle, pour les empreintes binaires, est au moins de 160 bits.

d. Exemple de fonction de hachage pouvant conduire à la factorisation d'un entier RSA

Soient p et q deux entiers premiers distincts du même ordre de grandeur avec : $p = 2p' + 1$ et $q = 2q' + 1$ où p' et q' sont aussi premiers.

p et q sont supposés secrets, mais leur produit $n = pq$ est public.

Le lemme chinois permet d'écrire $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{F}_p \times \mathbb{F}_q$ et si G_n est le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, G_n possède $\varphi(n) = (p-1)(q-1)$ *ie* $4p'q'$ éléments ; dans $(\mathbb{F}_p^*, \times)$ l'ordre maximum d'un élément est égal à $2p'$; il s'ensuit de manière évidente que l'ordre maximum d'un élément de G_n est le ppcm de $2p'$ et $2q'$, *ie* est égal à $2p'q'$; de plus si $\bar{a}$ dans $\mathbb{F}_p^*$ génère le groupe $(\mathbb{F}_p^*, \times)$ et si $\bar{\bar{b}}$ dans $\mathbb{F}_q^*$ génère $(\mathbb{F}_q^*, \times)$, l'élément $(\bar{a}, \bar{\bar{b}})$ de $\mathbb{F}_p \times \mathbb{F}_q$ est d'ordre $2p'q'$.

Bilan : il existe dans G_n des éléments d'ordre maximum égal à $2p'q'$. D'ailleurs si $\alpha \in G_n$, et si r est l'ordre de α, r divise $4p'q'$, donc :

$$r \in \{1, 2, 4, p', q', 2p', 2q', 4p', 4q', 2p'q'\}$$

Supposons connaître un élément α de G_n d'ordre $2p'q'$; soit alors h la fonction : $\begin{cases} E = \{1, 2, \ldots, n^2\} \to G_n \\ x \to \alpha^x \end{cases}$.

Dans E la relation binaire $x \sim x'$ *si et seulement si* $h(x) = h(x')$ est une relation d'équivalence et l'ensemble quotient $E/\sim$ est en bijection avec l'image $h(E)$; comme le cardinal de G_n n'excède pas n, et que celui de E vaut n^2, il y a de multiples triples collisions pour h dans E, c'est-à-dire qu'il existe x, x', x'' deux à deux distincts dans E avec :

$$h(x) = h(x') = h(x'')$$

Supposons donc disposer d'une triple collision avec :

$$1 \leq x < x' < x'' \leq n^2$$

et telle qu'il existe un entier k "pas trop grand" vérifiant :

$$1 \leq x' - x \leq kn$$
$$1 \leq x'' - x' \leq kn$$

(En d'autres termes on suppose avoir trouvé une triple collision à termes "assez voisins"). On peut donc écrire :

$$\alpha^{x'-x} = \alpha^{x''-x'} = 1 \pmod{n}$$

et ainsi :

$$\begin{aligned} x' - x &= 2p'q'u \\ & \qquad \text{avec } u, v \text{ dans } \mathbb{N}^2 \\ x'' - x' &= 2p'q'v \end{aligned}$$

Soit M le pgcd des entiers $x' - x$ et $x'' - x'$; on a :

$$M = (x' - x) \wedge (x'' - x') = 2p'q'(u \wedge v)$$

or :

$$2p'q'u \leq kn \text{ et } 2p'q' \geq \frac{2pq}{5} = 2\frac{n}{5}$$

car p et q sont supposés assez grands pour que l'on ait $p'q' \geq \frac{pq}{5}$. Il en résulte alors : $\frac{2n}{5}u \leq 2p'q'u \leq kn$, ce qui entraîne : $u \leq \frac{5}{2}k$ et de ce fait si $\delta = u \wedge v$, $1 \leq \delta \leq \frac{5}{2}k$; puis en calculant tous les éventuels M/d avec : $d \leq \frac{5}{2}k$, d divisant M et en calculant $\alpha^{M/d}$, on obtient rapidement l'entier $2p'q'$ *ie* l'ordre dans G_n de α ; il s'ensuit que l'entier $\varphi(n) = 4p'q' = (p-1)(q-1)$ est connu ; comme n est lui aussi connu on peut donc en déduire p et q puisque, par exemple, il suffit de trouver les racines de l'équation :

$$X^2 - (n - \varphi(n) + 1)X + n = 0$$

qui ne sont autres que les entiers p et q.

Bilan : Dans certains cas une fonction de hachage peut permettre de réaliser une attaque du cryptosystème RSA de clé $K = (n, p, q, a, b)$.

Etude d'un exemple : On prend $n = 162\ 049$ et on sait que $\alpha = \bar{2}$ est un élément de G_n d'ordre maximum, bien sûr non précisé. Supposons que l'on dispose de la triple collision :

$$h(2\ 015\ 450) = h(2\ 821\ 630) = h(4\ 353\ 372)$$

ainsi : $x = 2\ 015\ 450$, $x' = 2\ 821\ 630$, $x'' = 4\ 353\ 372$, $x' - x = 806\ 180$ et $x'' - x' = 1\ 531\ 742$; un calcul laissé aux soins du lecteur montre que :

$$(x' - x) \wedge (x'' - x') = 80\ 618$$

car : $\begin{cases} x' - x = 10 \times (80\ 618) \\ x'' - x' = 19 \times (80\ 618) \end{cases}$.

Ici, on constate que $k = 10$ convient. D'où *via* les notations précédentes :

$$M = 80\ 618 = 2p'q'(u \wedge v) \text{ et } u \leq 25 \text{ donc : } u \wedge v \leq 25$$

Si on suppose que p et q sont "grands" : $\varphi(n) = (p-1)(q-1)$ est "très voisin" de pq en lui étant inférieur ; or $2p'q' = \frac{1}{2}\varphi(n)$; par conséquent plus $u \wedge v$ est "petit" plus $\varphi(n)$ est "grand" ; il est donc "légitime" de commencer avec les plus petites valeurs positives pour $u \wedge v$; c'est pourquoi supposons $u \wedge v = 1$; alors on obtient : $\frac{1}{2}\varphi(n) = 80\ 168$ *ie* $\varphi(n) = 161\ 236$ et alors l'équation du second degré associée est :

$$X^2 - 814X + 162\ 049 = 0$$

son discriminant vaut $14\ 400 = (120)^2$ ce qui fournit pour racines : $X_1 = 467$ et $X_2 = 347$ qui sont bien des nombres premiers fournissant le résultat escompté.

L'exposant du groupe G_n est ici égal à 80 618.

8.5 Protocoles d'identification numériques n'utilisant pas de mot de passe

a. Instance du problème

Dans bien des cas l'utilisation d'un moyen informatique d'accès à une connexion à distance, à un guichet automatique d'une banque, à une chaîne cryptée *etc.*. nécessite de prouver son identité.

L'objet d'un protocole – ou procédé – d'identification est de permettre à un intervenant de se faire connaître afin qu'il puisse utiliser le réseau informatique de communication dont il dispose ; cela doit pouvoir s'effectuer sans que personne puisse, même en écoutant le canal de communication, se substituer à l'intervenant et utiliser les échanges d'information.

Dans ce paragraphe les procédés d'identification exposés sont des "allers-retours" de questions et de réponses entre l'identificateur et l'identifiable comme la suite l'explique en s'affranchissant de la notion de mot de passe.

b. Exemples pratiques de procédés d'identification

b.1. Protocole de Schnorr

Le protocole d'identification présenté ci-dessous porte le nom de protocole d'identification de Schnorr. Il est élaboré de la façon suivante et par l'intermédiaire d'un organisme officiel, faisant autorité, noté H par la suite.

Désignons par A l'utilisateur d'un réseau informatique où il devra être identifié.

1° étape : réalisation d'un certificat d'identité

(i) H dispose d'un grand nombre premier p d'au moins 512 bits tel que, dans $\mathbb{F}_p$, le problème du logarithme discret est difficile et d'un "grand" nombre premier q, q divisant $p-1$; H désigne par α un élément d'ordre q dans $\mathbb{F}_p$ *ie* une racine primitive q-ième de 1 modulo p, et on suppose de plus qu'il possède un protocole de signature s_H de $\mathbb{F}_p \times \mathbb{F}_p$ dans $\mathbb{F}_p$ la fonction de vérification associée est notée σ_H ; éventuellement, H possède une fonction de hachage h si cela est nécessaire, réputée sûre.

p, q, α, h et σ_H sont publics ; s_H est secret ; enfin H attribue à A un élément $x \in \mathbb{F}_p$ décrivant l'identité de A (exemple, le numéro de sécurité sociale).

(ii) A choisit un entier a, avec $a \in \{1, 2, \ldots, q\}$ (a est un "PIN") et calcule : $y = \alpha^a \pmod p$ et le fait parvenir à H qui constitue alors $z \in \mathbb{F}_p$ où : $z = s_H(x, y)$; le triplet : (x, y, z) est envoyé à Alice et constitue le certificat d'identité de A validé par H.

2° étape : procédé d'identification de A par B sous la houlette de H

Il est constitué par les étapes suivantes :

(i) A choisit $k \in \{1, 2, \ldots, q\}$ et calcule $t = \alpha^k \pmod p$

(ii) A transmet (x, y, z) et t à B

(iii) B vérifie que le triplet (x, y, z) est valable en calculant $\sigma_H(x, y)$

(iv) B choisit : k' arbitraire et le transmet à A (k' entier)

(v) A calcule : $u = k - ak' \pmod q$ et transmet u à B

(vi) B calcule $\alpha^u y^{k'}$ et reconnaît A *si et seulement si* :

$$\alpha^u y^{k'} = t$$

b.2. Une variante de ce protocole : le protocole d'Okamoto

Il s'élabore toujours sous l'autorité de H ; les entiers p, q et les fonctions σ_H et s_H ont la même signification que dans le protocole de Schnorr.

H publie α et α', deux éléments distincts de $\mathbb{F}_p^*$ d'ordre q tels que $\log_\alpha \alpha'$ est difficile à trouver.

1° étape : Le certificat

(i) A nouveau, x désigne un élément de $\mathbb{F}_p$ établi par H, identifiant A (exemple : numéro de sécurité sociale)

(ii) A choisit deux PINs a et a' dans $\{1, 2, \ldots, q\}$ et calcule modulo p : $y = \alpha^a \alpha'^{a'}$ qui est envoyé à H ; H signe le couple (x, y) par $z = s_H(x, y)$ et délivre le certificat (d'identité) : $(x, y, z) \in \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$ à A.

2° étape : Identification de A par B

(i) A choisit $k, k' \in \{1, 2, \ldots, q\}$ et calcule $t = \alpha^k \alpha'^{k'}$ modulo p

(ii) A transmet (x, y, z) et t à B

(iii) B vérifie que $z = s_H(x, y)$ en calculant $\sigma_H(x, y)$ et choisit k'' dans $\{1, 2, \ldots, q\}$ pour le transmettre à A

(iv) A calcule simultanément :

$$u_1 = k - ak'' \pmod{q}$$
$$u_2 = k' - a'k'' \pmod{q}$$

et fournit le couple (u_1, u_2) à B

(v) B calcule $\alpha^{u_1} \alpha'^{u_2} y^{k''}$ modulo p et reconnaît A *si et seulement si* :

$$\alpha^{u_1} \alpha'^{u_2} y^{k''} = t \pmod{p}$$

Ici la nouveauté par rapport au procédé précédent et que l'identifiable possède deux PINs a et a' ; cependant le procédé de Schnorr est plus rapide que celui d'Okamoto.

c. Procédé d'identification basé sur le RSA

Il est toujours validé par une autorité H qui choisit deux entiers p et q secrets, premiers distincts, du même ordre, et forme le produit :

$$n = pq$$

H dispose toujours d'un protocole de signature s_H de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, et d'une fonction de vérification σ_H ainsi que (si nécessaire) d'une fonction de hachage et publie un grand nombre premier $r \notin \{p, q\}$.

r, n, σ_H sont publics, ainsi que la fonction de hachage.

1° étape : Le certificat d'identité

(i) x est un entier de $\{1, 2, \ldots, n\}$ attaché à l'identité de A et connu de H et même choisi par H.

(ii) A choisit un PIN a de $\{1, 2, \ldots, n\}$ tel que $\bar{a} \in G_n$ où G_n est le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ et calcule :

$$y = (\bar{a}^{-1})^r \pmod{n}$$

qu'elle transmet à H.

(iii) H valide et effectue la signature :

$$z = \sigma_H(x, y)$$

et fournit à A le triplet (x, y, z) qui constitue le certificat d'identité de A.

2° étape : Identification de A par B
Elle s'effectue selon le protocole suivant :

(i) A choisit k arbitraire dans $\{0, 1, 2, \ldots, n-1\}$, et calcule :

$$t = k^r \pmod{n}$$

(ii) A transmet (x, y, z) et t à B qui vérifie que l'on a bien $z = s_H(x, y)$ et choisit $k' \in \{0, 1, \ldots, r-1\}$ arbitraire et l'envoie à A.

(iii) A calcule :

$$u = ka^{k'} \pmod{n}$$

et l'envoie à B.

(iv) B calcule :

$$y^{k'} u^r$$

et accepte l'identité de A *si et seulement si* :

$$u^r y^{k'} = t \pmod{n}$$

Conclusion : Dans chacun des protocoles d'identification, l'autorité de référence fournit un certificat d'identité à l'intervenant A qui, à chaque demande d'identification, doit le fournir et ensuite, par un aller-retour de questions et de réponses, confirmer son identité.

8.6 Exemples numériques concernant les protocoles de Schno et d'Okamoto

a. Le protocole d'identification de Schnorr

On prend $p = 467$ et $q = 233$; comme q est un nombre premier, si m est un entier, $\bar{m}' = \bar{m}^2$ est un résidu quadratique modulo 467 ; ainsi si $\bar{m}' \neq \bar{0}$, $\bar{m}'^{233} = \bar{1} \pmod{467}$; comme 233 est un nombre premier, si $\bar{m}' \neq \bar{1}$, $\bar{m}'$ est d'ordre $q = 233$; ainsi tout résidu quadratique autre que $\bar{1}$ est d'ordre $q = 233$ modulo 467 ; on prendra donc le plus simple *ie* : $\bar{\alpha} = \bar{4}$; ensuite le "pin" a est pris égal à 6 ; A choisit donc $y = \bar{4}^6 \pmod{467}$.

Ainsi A obtient :

$$\bar{y} = \bar{4}^6 = \bar{\alpha}^a = 360 \pmod{467}$$

afin de continuer A choisit pour fixer les idées, $k = 100$, alors il obtient :

$$t = 4^{100} \pmod{467} = 229$$

Le choix arbitraire de B est $k' = 10$ ce qui fournit $u = 40$ et :

$$\alpha^u = 4^{40} = 123 \pmod{467},\ y^{k'} = 360^{10} = 74 \pmod{467}$$

D'où :

$$\alpha^u y^{k'} = 123 \times 74 = 9102 = 229 \pmod{467}$$

et ainsi l'identification de A par B est légitime.

b. Le protocole d'Okamoto

On reprend $p = 467$ et $q = 233$; les deux éléments α et α' publiés par H sont définis par :

$$\alpha = \overline{4} \text{ et } \alpha' = \overline{159} \pmod{467}$$

Les deux "PINs" a et a' choisis par A et tenus cachés sont :

$$a = 6 \text{ et } a' = 100$$

dans ces conditions c'est le produit :

$$y = \alpha^a \alpha'^{a'} = \overline{4}^6 \cdot \overline{159}^{100} = 360 \times 262 = 453 \pmod{467}$$

est celui qui est communiqué à H pour la délivrance du certificat.

Ensuite les entiers k et k' choisis au hasard par A sont pris tels que :

$$k = 100,\ \ k' = 101$$

Alors :

$$\alpha^k = 4^{100} = 229 \pmod{467}$$

et :

$$\alpha'^{k'} = 159^{101} = 363 \pmod{467}$$

et alors :

$$t = 229 \times 363 = 1 \pmod{467}$$

Supposons que B choisisse $k'' = 181$ et le transmette à A ; ce dernier calcule alors modulo 233 :

$$u_1 = 100 - 6 \times 181 = 179 \pmod{233}$$
$$u_2 = 101 - 100 \times 181 = 175 \pmod{233}$$

Pour identifier A, B doit calculer :

$$\alpha^{u_1} \alpha'^{u_2} y^{k''} \pmod{467}$$

et reconnaîtra A s'il trouve la valeur de t *ie* 1 modulo 467.

Or :

$$\begin{aligned}\alpha^{u_1} &= 4^{179} = 434 \pmod{467}\\ \alpha'^{u_2} &= 159^{175} = 223 \pmod{467}\\ y^{k''} &= 453^{181} = 4^{154} \times 159^{159} = 62 \pmod{467}\end{aligned}$$

et on vérifie que :

$$434 \times 223 \times 62 = 6\ 000\ 484 = 1 \pmod{467}$$

Par conséquent B est rassuré et a pu identifier A.

Conclusion : Comme nous l'avons écrit au début de ce dernier chapitre, les protocoles de signature et d'identification numériques utilisent exclusivement l'élégance et l'efficacité de l'arithmétique modulaire dans l'anneau $\mathbb{Z}$; c'est encore une fois une des raisons justifiant le titre de cet ouvrage.

Mon privilège à moi, c'est vous !

Pierre MEUNIER à ses élèves

Annexe A

Cryptographie et surface de Frobénius

Le T.I.P.E. d'un élève reçu à l'ENS Lyon consacré à la cryptologie en liaison avec le thème national imposé intitulé : "Surfaces"

Note du copiste : La présentation est celle qu'a utilisée l'élève en question, il est donc normal que les notations diffèrent quelque peu de celles employées dans le reste du livre.

A.1 Introduction :

L'objectif de tout cryptosystème El Gamal est double : être rapide au codage comme au décodage mais surtout être difficile à casser, c'est à dire résister aux algorithmes de Shanks et de Pohlig.

Ici, l'on étudie les propriétés d'un cryptosystème El-Gamal utilisé avec les éléments d'un groupe G : la surface de Frobenius. Entre autre, après quelques définitions, nous allons encadrer le cardinal de G, voire le déterminer entièrement sous certaines conditions, et nous prouverons que dans ce cas, G est cyclique. Enfin, nous verrons rapidement le principe du cryptosystème El-Gamal ainsi que deux algorithmes pour le casser : les algorithmes de Shanks et de Pohlig.

Tout d'abord je souhaite remercier monsieur Pierre Meunier, professeur de mathématiques en classe de MP* au lycée Joffre à Montpellier, créateur du cryptosystème présenté ici.

Dans toute la suite la notation #A correspond au cardinal de A

A.2 Un peu de théorie

A.2.1 Premières définitions

a. Préliminaires :

- On considère dans toute la suite deux nombres n et p tel que n est supérieur à 2 et p soit premier ; on considère aussi le corps noté $\mathbb{K} = \mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (corps premier de Frobénius).
- On définit la matrice de Frobenius que l'on note F, $F \in Mn(\mathbb{K})$,

$$F = \begin{pmatrix} 0 & 1 & 0 & 0 & ... & 0 \\ 0 & 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & ... & 1 \\ 1 & 0 & 0 & 0 & ... & 0 \end{pmatrix}$$

  On remarque que le polynôme minimal de F, noté μ_F est $X^n - 1$ (F est la matrice compagnon de ce polynôme).
- On note $\mathbb{K}[F]$ la $\mathbb{K}$ algèbre commutative engendrée par F.
  Or selon le cours $\mathbb{K}[F]$ est isomorphe à $\frac{\mathbb{K}[X]}{\mu_F \mathbb{K}[X]}$ donc ici $\mathbb{K}[F]$ est isomorphe à $\frac{\mathbb{K}[X]}{(X^n-1)\mathbb{K}[X]}$

b. Définition

- Définition : On note A l'application de $\mathbb{K}[F] \to \mathbb{K}^n$ telle que :
  $x_0 I_n + x_1 F + ... + x_{n-1} F^{n-1} \mapsto (x_0, x_1, ..., x_{n-1})$
  et on définit sur $\mathbb{K}^n$ la loi de composition interne suivante
  $\star : ((x_0, x_1, ..., x_{n-1}), (y_0, y_1, ..., y_{n-1})) \mapsto (z_0, z_1, ..., z_{n-1})$
  où pour tout k de 0 à $n-1$, $z_k = \sum_{i+j=k \ mod \ n} x_i y_j$
- Propriétés :
  - $\boxed{(\mathbb{K}^n, \star, +, .) \text{ est une algèbre commutative}}$
  - en effet, l'application A est un morphisme de $\mathbb{K}$ algèbre de $(\mathbb{K}[F], \times, +, .)$ dans $(\mathbb{K}^n, \star, +, .)$
- Preuve : A est bien évidemment une application linéaire. Montrons que A est un morphisme de $(\mathbb{K}[F], \times)$ dans $(\mathbb{K}^n, \star)$:
  $A((x_0 I_n + x_1 F + ... + x_{n-1} F^{n-1}) \times (y_0 I_n + y_1 F + ... + y_{n-1} F^{n-1})) = A(\sum_{1 \le i,j \le n} x_i y_j F^{i+j})$
  $= A(\sum_{k=0}^{n-1} \sum_{i+j=k \ mod \ n} x_i y_j F^k) = A(\sum_{k=0}^{n-1} F^k \sum_{i+j=k \ mod \ n} x_i y_j) = (x_0, x_1, ..., x_{n-1}) \star (y_0, ..., y_{n-1})$

- Remarque : de plus, (1,0,...,0) est le neutre pour $\star$, et on rappelle que tout élément de $\mathbb{K}[F]$ inversible est inversible dans $\mathbb{K}[F]$. En conséquence tout élément de $\mathbb{K}^n$ qui est l'image d'un élément inversible est inversible dans $\mathbb{K}^n$ pour $\star$.
- Conclusion : Dans toute la suite on identifie les éléments de $\mathbb{K}[F]$ et ceux de $\mathbb{K}^n$.

c. Surface de Frobénius

- Définition :
  On note G l'ensemble des éléments x de $\mathbb{K}[F]$ tel que det(x)=1
  On note aussi G l'ensemble A(G) , G est dit surface de Frobénius.
- Remarque : (G,$\star$) est un groupe commutatif.

A.2.2 Encadrement du cardinal de G

L'objectif de cette partie est de démontrer la proposition suivante :

- Proposition :
  - si n est premier avec $p-1$ alors $\#G \leq p^{n-1}$
  - De plus si $n \notin p\mathbb{Z}$ alors $\#G \leq p^{n-1}-1$

a. Deux lemmes pour la preuve

- Commençons par démontrer le résultat suivant : si $n \wedge (p-1) = 1$ alors l'application $\lambda \in \mathbb{K} \mapsto \lambda^n \in \mathbb{K}$ est une bijection.
  Montrons que cette application est injective, ce qui suffira à prouver la bijectivité.
  Si $\lambda^n = \mu^n$, soit $\lambda = 0$ alors $\mu = 0$. Sinon, selon le théorème de Lagrange $\lambda^{p-1} = \mu^{p-1}$ donc si d est l'ordre de $\lambda\mu^{-1}$ alors d divise n et d divise $p-1$ donc d=1 et donc $\lambda = \mu$.

- Démontrons désormais l'égalité suivante :

$$\#\mathbb{K}^n = \#\omega_0 + (p-1)\#G$$

  où ω_0 est l'ensemble des éléments de $\mathbb{K}^n$ de déterminant nul.

  En effet, soit $\lambda \neq 0$ on note $\omega_\lambda = \{x \in \mathbb{K}^n / det(x) = \lambda\}$.
  Si μ est l'unique élément de $\mathbb{K}$ tel que $\mu^n = \lambda$
  Alors les applications $x \in G \mapsto \mu x \in \omega_\lambda$ et $x \in \omega_\lambda \mapsto \mu^{-1}x \in G$ sont toutes deux injectives donc bijectives.
  De plus $\mathbb{K}^n = \coprod_{\lambda \in \mathbb{K}} \omega_\lambda$, et donc $\#\mathbb{K}^n = \sum_{\lambda \in \mathbb{K}} \#\omega_\lambda$. D'où la conclusion.

b. Etude du cardinal de ω_0 :

Démontrons l'inégalité suivante : $\#\omega_0 \geq p^{n-1}$
pour cela, montrons que ω_0 contient l'hyperplan H d'équation $x_0 + ... + x_{n-1} = 0$

Les $n-1$ vecteurs $\begin{pmatrix}1\\-1\\0\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\0\\\vdots\\0\end{pmatrix}, ..., \begin{pmatrix}0\\0\\\vdots\\0\\1\\-1\end{pmatrix}$ forment une base de H. Or le vecteur $\begin{pmatrix}1\\1\\1\\\vdots\\1\\1\end{pmatrix}$ est libre avec les vecteurs ci-dessus ; ils forment donc une base de $\mathbb{K}^n$. Si P est la matrice de passage de la base canonique dans cette base alors :

$$P^{-1}FP = \begin{pmatrix}1 & 0 & 0 & ... & ... & ... & 0\\0 & -1 & 1 & 0 & & & \vdots\\\vdots & \vdots & 0 & 1 & & & \vdots\\\vdots & \vdots & \vdots & & & & \vdots\\\vdots & \vdots & \vdots & & & 1 & 0\\\vdots & \vdots & 0 & ... & ... & 0 & 1\\0 & -1 & 0 & ... & ... & ... & 0\end{pmatrix} = \begin{pmatrix}1 & 0 & ... & 0\\0 & & & \\\vdots & & B & \\0 & & & \end{pmatrix}$$

où $B = \begin{pmatrix}-1 & 1 & 0 & ... & ... & 0\\-1 & 0 & 1 & 0 & & \vdots\\\vdots & \vdots & & & & \vdots\\\vdots & \vdots & & & 1 & 0\\\vdots & 0 & ... & ... & 0 & 1\\-1 & 0 & ... & ... & ... & 0\end{pmatrix}$

En conséquence,

$$x_0I_n+x_1F+...+x_{n-1}F^{n-1} \sim \begin{pmatrix}x_0+...+x_{n-1} & 0 & ... & ... & ... & ... & 0\\0 & & & & & & \\\vdots & & x_0I_{n-1}+ & x_1B & +... & + & x_{n-1}B^{n-1}\\0 & & & & & & \end{pmatrix}$$

donc $det(x_0I_n + x_1F + ... + x_{n-1}F^{n-1}) = (x_0 + ... + x_{n-1})det(x_0I_{n-1} + x_1B + ... + x_{n-1}B^{n-1})$

donc H $\subset \omega_0$ donc $\#\omega_0 \geq p^{n-1} \Rightarrow \#G \leq p^{n-1}$

Si en plus $n \notin p\mathbb{Z}$: alors les $p-1$ matrices $\lambda(I_n + F + ... + F^{n-1})$ pour λ dans $\mathbb{K}^*$ sont dans ω_0 mais pas dans H. Donc $\#\omega_0 \geq p^{n-1} + p - 1 \Rightarrow \#G \leq p^{n-1} - 1$

A.2.3 Cas particulier où G est cyclique

L'objectif de cette partie est de démontrer le résultat suivant :

Si p et n sont premiers tel que p modulo n soit un générateur de $(\mathbb{F}_n^*, \times)$ alors G est de cardinal $p^{n-1} - 1$ et, de plus, G est cyclique.

a. Préliminaires :

On utilise le résultat suivant (preuve en annexe) : Si $\mathbb{K}$ est un corps de cardinal q et si n est un nombre premier avec q alors la classe de q modulo nappartient à $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ et si r est l'ordre de $\bar{q}$ alors tous les facteurs premiers de K_n, le n-ième polynôme cyclotomique, sont simples et de degré r.

On sait que si (A,+,.) est un anneau commutatif et si I est un idéal de A alors $\frac{A}{I}$ est un corps $\Leftrightarrow$ I est un idéal maximal de A. De plus, si $A = \mathbb{K}[X]$ et I un idéal de A alors $I = P\mathbb{K}[X]$ et I est maximal $\Leftrightarrow$ P est irréductible.

Conclusion : Si n est premier et si la classe de p est un générateur de $(\mathbb{F}_n^*, \times)$ alors $\frac{\mathbb{K}[X]}{K_n(X)\mathbb{K}[X]} = \frac{\mathbb{K}[X]}{(1+X+...+X^{n-1})\mathbb{K}[X]}$ est un corps.

b. Preuve que #G=$p^{n-1} - 1$, et que G est cyclique

On remarque que $\mu_B(X) = 1 + X + ... + X^{n-1}$ car B est la matrice compagnon de ce polynôme. Donc selon les remarques du a), $\mathbb{K}[B]$ est un corps car $\mathbb{K}[B]$ est isomorphe à $\frac{\mathbb{K}[X]}{K_n(X)\mathbb{K}[X]}$.

De plus si $\mathbb{K}$ est un corps fini alors $(\mathbb{K}^*, \times)$ est cyclique (preuve en annexe) or ici $\mathbb{K}[B]$ est fini, et possède p^{n-1} éléments ; donc $\#\mathbb{K}[B]^* = p^{n-1} - 1$. Soit donc $M \in \mathbb{K}[B]^*$ tel que M soit générateur de $(\mathbb{K}[B]^*, \times)$, $M = \sum_{k=0}^{n-2} a_k B^k$. Pour tout k de 0 à $n-2$ on pose $x_k = a_k + x_{n-1}$

Et alors :

$$x_0 I_n + x_1 F + ... + x_{n-1} F^{n-1} \sim \begin{pmatrix} x_0 + ... + x_{n-1} & 0 & ... & ... & 0 \\ 0 & & & & \\ \vdots & & \sum_{k=0}^{n-2} (x_k - x_{n-1}) B^k & & \\ 0 & & & & \end{pmatrix}$$

donc $det(x_0 I_n + x_1 F + ... + x_{n-1} F^{n-1}) = (a_0 + ... + a_{n-2} + n.x_{n-1}) det(M)$

On choisit $x_{n-1} = \frac{1}{n}(\frac{1}{det(M)} - (a_0 + ... + a_{n-2}))$ pour que :
$x_0 I_n + x_1 F + ... + x_{n-1} F^{n-1} \in G$

De plus $(x_0 I_n + x_1 F + ... + x_{n-1} F^{n-1})^k = I_n \Rightarrow M^k = I_{n-1}$, donc k est un multiple de $p^{n-1} - 1$ donc $\#G = p^{n-1} - 1$ et G est cyclique.

A.3 Cryptosystème El-Gamal sur $\mathbb{K}^n$

De façon générale, un cryptosystème est un quintuplet (K,E,E',e,d) où K est la clé du cryptosystème, E l'ensemble des textes à coder, et E' l'image de E par e ; e est la fonction de codage, d la fonction de décodage avec pour tout x de E, d(e(x))=x.

De plus, dans les cryptosystèmes à clé publique une partie de la clé K est publique, pour que n'importe qui puisse utiliser la fonction e, donc coder des messages, mais pas la fonction d.

Définition du cryptosystème étudié :

Ici la clé K=(G,α,β,a) où α est un générateur de G et $\beta = \alpha^a$ seuls α et β sont publics, E=$\mathbb{K}^n$ et E' =$\mathbb{K}^n$×G, e : x↦ $(\beta^k \star x, \alpha^k)$ où k est un entier choisi au hasard, d :(x,y)↦ $x \star y^{-a}$

Montrons que le cryptosystème est bien défini, c'est-à -dire que pour tout $x \in E$, $d(e(x)) = x$: en effet $d(e(x)) = \beta^k \star x \star (\alpha^k)^{-a} = x \star \beta^k \star (\alpha^a)^{-k} = x$

L'avantage de ce cryptosystème est que le chiffrement est aléatoire, il dépend d'un entier k choisi au hasard pour chaque élément, contrairement au RSA. De plus, on peut coder tous les éléments de $\mathbb{K}^n$, pas seulement les éléments de G, ce qui facilite la programmation.

A.4 Casser le cryptosystème

L'objectif est de calculer a à partir de α et β avec la meilleure complexité possible.

A.4.1 Algorithme de Shanks

- Soit m= #G, on pose q=$\lceil \sqrt{m} \rceil$ (partie entière par excès), on note $a = qj + i$ où i et j sont compris entre 0 et $q - 1$. Donc $\alpha^{qj} = \beta\alpha^{-i}$.
- Pour calculer a, on calcule les q éléments α^{qj} pour j variant de 0 à $q - 1$ en les plaçant dans un tableau, puis on calcule de même les q éléments $\beta\alpha^i$ pour i variant de 0 à $q - 1$ en les plaçant dans un second tableau.
- Pour finir on cherche i et j dans les deux tableaux tel que $\alpha^{qj} = \beta\alpha^{-i}$ et alors on a $a = qj + i$.
- On remarque que la complexité de cet algorithme est O($\sqrt{m}$).

A.4.2 Algorithme de Pohlig

- Soit m= #G, $m = p_1^{d_1} p_2^{d^2} \cdots p_k^{d_k}$, (décomposition en facteurs premiers de m).

Cet algorithme est en deux étapes ; premièrement pour tout i de 1 à k on calcule a modulo $p_i^{d_i}$, ensuite on conclut en utilisant l'algorithme des restes chinois. Dans la suite nous allons décrire seulement la première étape.

– Soit p un facteur premier de m et d sa multiplicité,
a est égal à $x_0 + x_1 p + ... + x_{d-1}p^{d-1}$ modulo p^d où chaque x_i est compris entre 0 et $p-1$.
De plus on remarque que
$\alpha^{\frac{x_0 m}{p}} = \alpha^{\frac{mx_0}{p} + \frac{pm(x_1+...+x_{d-1}p^{d-2})}{p}} = \alpha^{\frac{m(x_0+x_1p+...+x_{d-1}p^{d-1})}{p}} = \alpha^{\frac{ma}{p}} = \beta^{\frac{m}{p}}$
Ensuite on remarque que

$$\begin{aligned}\alpha^{\frac{x_1 m}{p}} &= \alpha^{\frac{mx_1}{p} + \frac{pm(x_2+...+x_{d-1}p^{d-3})}{p}} + \frac{mx_0}{p^2} \alpha^{\frac{-mx_0}{p^2}} \\ &= \alpha^{\frac{m(x_0+x_1p+...+x_{d-1}p^{d-1})}{p^2}} \alpha^{\frac{-mx_0}{p^2}} = \beta^{\frac{m}{p^2}} \alpha^{\frac{-mx_0}{p^2}}\end{aligned}$$

De même pour tout i de 2 à $d-1$,

$$\begin{aligned}\alpha^{\frac{x_i m}{p}} &= \alpha^{\frac{mx_i}{p} + \frac{pm(x_{i+1}+...+x_{d-1}p^{d-2-i})}{p}} + \frac{m(x_0+x_1p+...+x_{i-1}p^{i-1})}{p^{i+1}} - \frac{m(x_0+x_1p+...+x_{i-1}p^{i-1})}{p^{i+1}} \\ &= \alpha^{\frac{m(x_0+x_1p+...+x_{d-1}p^{d-1})}{p^{i+1}}} \alpha^{\frac{-m(x_0+x_1p+...+x_{i-1}p^{i-1})}{p^{i+1}}} \\ &= \beta^{\frac{m}{p^{i+1}}} \alpha^{\frac{-m(x_0+x_1p+...+x_{i-1}p^{i-1})}{p^{i+1}}}\end{aligned}$$

– Conséquence : on calcule les $\alpha^{\frac{jm}{p}}$ pour j de 0 à $p-1$ jusqu'à l'obtention de $\beta^{\frac{m}{p}}$ et $x_0 = j$; puis on calcule de façon itérative les x_i de 0 à $d-1$, en utilisant les formules ci-dessus.
– Pour finir, on remarque que la complexité de cet algorithme est $O((d_1p_1 + ... + d_kp_k)n^3)$

A.5 Conclusion

En conclusion, pour pouvoir résister à la fois à l'algorithme de Shanks et de Pohlig le nombre d'éléments du groupe engendré par α doit être "grand" et avoir un facteur premier qui est lui même "grand". Le cas où G est cyclique est où α est générateur de G est donc optimal. L'intérêt de ce cryptosystème est qu'il code des n-uplets de la longueur voulue, et avec un large choix (en fait une infinité selon le théorème de Dirichlet) de nombres p permettant que le groupe G soit cyclique, et donc que le logarithme discret soit le plus difficile possible à trouver (avec n=19 et p=257 les algorithmes de Shanks et de Pohlig n'ont toujours pas abouti après 2h sur mon portable, alors que le codage et

le décodage d'une ligne de texte prend environ une seconde). De plus l'isomorphisme entre $\mathbb{K}^n$ et $\mathbb{K}[F]$ permet l'utilisation de méthodes d'algèbre linéaire tant pour la théorie que pour la programmation (voir les annexes 6 et 7).

A.6 Annexe : programmes en Caml

A.6.1 Programmes utiles dans la suite

On programme la multiplication de A(x) par A(y) :

```
let mul a b p =
let n=vect_length a in let v = make_vect n 0 in
for i=0 to n-1
do
  for j=i+1 to n-1
  do
    v.(i) <- (v.(i)+a.(i+n-j)*b.(j)) mod p
  done;
  for j=0 to i
  do
    v.(i) <- (v.(i)+a.(j)*b.(i-j)) mod p
  done
done;
v;;
```

L'exponentiation rapide dans G :

```
let rec puissance x m p =
let n=vect_length x in
if m=0 then let a=make_vect n 0 in a.(0)<-1;a;
        else if m=1 then x
                    else if m mod 2 = 0 then let y=puissance x (m quo 2) p in mul
y y p
                                        else let y=puissance x ((m-1) quo 2) p in
                                             mul (mul y y p ) x p;;
```

Calcul de l'inverse d'un nombre modulo p via la méthode de l'algorithme d'Euclide :

```
let inverse x p=
if x mod p=0 then 0 else
let u=ref 0 and v=ref 1 and t=ref x and r=ref p and s=ref 0 and q=ref 0 and w=
ref 0 in
while !t>0
do
  s := !r mod !t; q := !r quo !t;
```

```
    w :=( !u-( !q)*( !v)+p*p) mod p ; u := !v ;
    v := !w ; r := !t ; t := !s ;
  done ;
  !u ; ;
```

Calcul du polynôme caractéristique par la méthode de Fadeev :

```
  let caractéristique x p=
  let n=vect_length x in let l=make_vect (n+1) 1 and q=copy_vect x in let m=ref
q in
  for i=1 to n
  do
    l.(i) <- ( -(inverse i p )*n*( !m.(0)) + p*p*n ) mod p ;
    !m.(0)<- ( !m.(0)-(inverse i p )*n*( !m.(0)) + p*p*n) mod p ;
    m := mul !m x p ;
  done ;
  l ; ;t
```

Calcul de l'inverse d'un élément de G :

```
  let inv x p =
  let n=vect_length x in let id= make_vect n 0 in id.(0)<-1 ;
  let m=caractéristique x p and l=make_vect n 0 and v=make_vect n id in
  let a= p - ( inverse m.(n) p ) in
  for i=1 to (n - 1)
  do
    v.(i)<-mul v.(i-1) x p
  done ;
  for i=0 to n - 1
  do
    for j=0 to n - 1
    do
      l.(i)<- ( l.(i)+a*m.(n-j-1)*(v.(j)).(i) ) mod p
    done ;
  done ;
  l ; ;
```

A.6.2 Cryptosystème d'El-Gamal

Fonction auxiliaire de codage, code un tableau d'éléments de G :

```
  let codage_aux l p alpha bêta =
  let q=vect_length l and n=vect_length l.(0) in let c=make_vect q (l.(0),l.(0)) in
  for i=0 to (q-1)
  do
```

```
  let k=random__int ( int_of_float (2.**(float_of_int n))) in
  let x=puissance alpha k p and y=mul l.(i) ( puissance bêta k p ) p in
  c.(i)<-(x,y)
done;
c;;
```

Fonction codage, code une chaine de caractères :

```
let codage c p alpha bêta =
let n=vect_length alpha in let q = string_length c in
let r = q quo n and s = q mod n in let v = make_matrix (r+1) n 0 in
for i=0 to r-1
do
  for j=0 to n-1
  do
    v.(i).(j) <- int_of_char c.[n*i+j]
  done;
done;
for i=0 to s-1
do
  v.(r).(i) <- int_of_char c.[n*r+i]
done;
codage_aux v p alpha bêta;
```

Fonction auxiliaire de décodage, décode un tableau d'éléments de G :

```
let décodage_aux c p a =
let q=vect_length c in let d=make_vect q ( fst c.(0) ) in
for i=0 to (q-1)
do
  let x=fst c.(i) and y=snd c.(i) in
  let z= inv (puissance x a p) p in d.(i)<- mul y z p
done; d;;
```

Fonction de décodage, renvoie une chaine de caractères :

```
let décodage c p a=
let n=vect_length ( fst c.(0) ) in
let d = décodage_aux c p a and s = ref n-1 and bool=ref true in
let q = vect_length d in
while !s>0 & !bool
do
  if d.(q-1).(!s)=0 then bool := false
                    else decr s
done;
let t = make_string ((q-1)*n+(!s)) 'a' in
```

```
for i=0 to q-2
do
  for j=0 to n-1
  do
    t.[i*n+j]<- char_of_int (d.(i)).(j)
  done;
done;
for j=0 to !s-1
do
  t.[(q-1)*n+j]<- char_of_int (d.(q-1)).(j)
done; t;;
```

Remarque : par élément, la complexité est pour le codage comme pour le décodage $O(n^2.\log(p)^2)$.

A.6.3 Algorithme de Shanks

```
let shanks alpha beta p =
let n=vect_length alpha in let g=(float_of_int p)**(float_of_int n-.1.)-.1. in
let q=int_of_float (sqrt g) in let c=make_matrix q n 0 in c.(0)<-beta;
let d=make_matrix q n 0 in d.(0).(0)<-1;
let i=ref 0 and j=ref 0 and bool=ref true in let a=inv (puissance alpha q p) p in
while !i<=q-1 & !bool
do
 j :=0;
 if !i>0 then c.(!i)<- mul a c.(!i-1) p;
 while !j<=q-1 & !bool
 do
   if !i=0 & !j>0 then d.(!j)<- mul alpha d.(!j-1) p;
   if c.(!i)=d.(!j) then bool :=false
                    else incr j;
 done;
 incr i;
done;
q*(!i-1)+(!j);;
```

A.7 Annexe : programmes en Maple :

A.7.1 programmes utiles dans la suite :

On programme la multiplication de A(x) par A(y) :

```
mult :=proc(a,b)
local l,i,j,c :
```

```
l :=[seq(0,i=1..n)] :
for i from 0 to n-1
do
   c :=0 :
   for j from i+1 to n-1
   do
      c := ( c+a[i+n-j+1]*b[j+1] ) mod p
   od :
   for j from 0 to i
   do
      c := ( c+a[j+1]*b[i-j+1] ) mod p
   od :
   l[i+1] :=c :
od :
l; end proc;
```

L'exponentiation rapide :

```
puissance := proc(x, m)
local y, z;
if m = 1 then z := x
          else if m mod 2 = 0 then y := puissance(x, 1/2*m); z := mult(y, y)
                              else y := puissance(x, 1/2*m - 1/2);
                                   z := mult(mult(y, y), x); end if; end if;
z; end proc;
```

Calcul de l'inverse d'un nombre modulo p via la méthode de l'algorithme d'Euclide :

```
inver :=proc(x)
local u,v,t,r,s,q,w :
u :=0 :v :=1 :t :=x :r :=p :
while t>0
do
   s :=irem(r,t) : q :=iquo(r,t) : w :=u-q*v mod p :
   u :=v : v :=w : r :=t : t :=s :
od :
u; end proc;
```

Calcul du polynôme caractéristique par la méthode de Fadeev :

```
caract := proc(x)
local l, m, y, i;
l := [1] ;m := x;
for i to n
do
```

```
  l := [op(l), (-inver(i)*n*m[1]) mod p] ;
  m[1] := (m[1] - inver(i)*n*m[1]) mod p ;
  m := mult(x, m)
od ;
l ; end proc ;
```

Calcul de l'inverse d'un élément de G :

```
inv := proc(x)
local a, b, l, m, i, q, j ;
a := caract(x) ; b := (-inver(a[n + 1])) mod p ; l := [[1, seq(0, i = 1 .. n - 1)]] ;
for i to n - 1
do
  l := [op(l), puissance(x, i)]
od ;
m := [] ;
for i to n do
  q := b*sum(a[j]*l[n - j + 1][i], j = 1 .. n) mod p ;
  m := [op(m), q]
od ;
m ; end proc ;
```

A.7.2 Cryptosystème d'El-Gamal :

Fonction auxiliaire de codage, code une liste d'éléments de G :

```
codage :=proc(l)
local k,v,y,z,u,c,i,x :
u :=nops(l) :
c :=[] :
for i from 1 to u
do
  x :=l[i] : k :=rand(1..p^(n-1)-1)() :
  z :=puissance(alpha,k) : v :=puissance(beta,k) : y :=mult(v,x) :
  c :=[op(c),[z,y]] :
od :
c ; end proc ;
```

Fonction codage, code une chaine de caractères :

```
codagefinal := proc (t)
local c, d, q, i, a ;
c := convert(t,'bytes') ; d := [] ; q := nops(c) ;
for i from 0 to iquo(q,n)-1
do
  d := [op(d), [seq(c[n*i+j],j = 1 .. n)]]
```

```
od ;
a := mod(q,n) ;
d := [op(d), [seq(c[iquo(q,n)*n+j],j = 1 .. a), seq(0,j = a+1 .. n)]] ;
codage(d) ; end proc ;
```

Fonction auxiliaire de décodage, décode une liste d'éléments de G :

```
décodage := proc (l)
local i, w, y, z, u, v, x, d ;
w := nops(l) ; d := [] ;
for i to w
do
  z := l[i][1] ; y := l[i][2] ;
  u := puissance(z,a) ;
  v := inv(u) ;
  x := mult(v,y) ;
  d := [op(d), x]
od ;
d ; end proc ;
```

Fonction de décodage, décode une chaine de caractères :

```
décodagefinal :=proc(c)
local d,e,q,i :
d := décodage(c) :e :=[d[1][1]] :q :=n*nops(d)-1 :
for i from 1 to q
do
  e :=[op(e), (d[ iquo(i,n)+1 ])[(i mod n)+1]]
od :
convert(e,'bytes') : end proc ;
```

Remarque, complexité : par élément, la complexité est pour le codage comme pour le décodage $O(n^2.\log(p)^2)$.

A.7.3 Etude du groupe G

programme qui teste si un élément de $\mathbb{K}^n$ est dans G :

```
frobénius :=proc(a)
local i :
evalb( caract(a)[n+1] = (-1)^n mod p ) ; end proc ;
```

On calcule l'élément de $\mathbb{K}^n$ suivant dans l'ordre lexicographique :

```
suivant :=proc(x)
local b,i,a :
b :=true ;i :=1 :a :=x :
while b and i<=n
```

```
do
  if x[n-i+1]=p-1 then a[n-i+1] :=0 : i :=i+1
                  else b :=false : a[n-i+1] :=x[n-i+1]+1 mod p : fi :
od ;
a : end proc ;
```

Liste des diviseurs maximaux (ie les $\frac{\#G}{p}$ où p premier divise #G) de #G :

```
listediviseur :=proc()
local i,g,h,j,k,l,m :
g :=p^(n-1) − 1 :
h :=ifactors(g)[2] : j :=nops(h) : l :=[ ] :
for i from 1 to j
do
  l :=[op(l), g/h[i][1]]
od ;
l : end proc ;
```

On teste si un élément de G est générateur :

```
estgénérateur :=proc(x,f)
local a,b,c,i :
c :=x : i :=1 :
while c<>[1,seq(0,i=1..n-1)] and i<= nops(f)
do
  c :=puissance(x,f[i]) :
  i := i+1 :
od :
evalb(i=nops(f)+1) ; end proc ;
```

Programme qui renvoie le plus petit élément générateur supérieur à un élément :

```
recherchefrobénius := proc (x)
local c, d, e, f ;
d := suivant(x) ; c := [ ] ; e := true ; f := listediviseur() ;
while d <> x and e
do
  if frobénius(d) then if estgénérateur(d,f) then e := false
                                             else d := suivant(d) : fi :
                  else d := suivant(d) : fi :
od ;
d ; end proc ;
```

Remarque : On obtient d'autres générateurs en mettant le générateur trouvé par le programme ci-dessus à le puissance q où q est un nombre premier avec $p^{n-1} - 1$.

A.7.4 Algorithme de Pohlig :

```
pohlig :=proc()
local m,l,g,i,bool_bis,h,b,r,j,c,bool,d,k,q :
m :=p^(n-1)-1 ; l :=ifactors(m)[2] ; g :=[] ;
for i from 1 to nops(l)
do
  bool_bis :=true :
  h :=[] :
  b :=puissance(alpha,m/l[i][1]) :
  r :=[[1,seq(0,i=1..n-1)]] :
  while bool_bis
  do
    j :=0 :
     c :=puissance(mult(beta,puissance(inv(alpha),add(h[j]*l[i][1]^(j-1),j=1..nops(h)) )
),m/l[i][1]^(nops(h)+1)) :
    bool :=true :
    while bool
    do
      if j=nops(r) then d :=mult(b,r[j]) :
                        r :=[op(r),d] :
                  else d :=r[j+1] : fi :
      if d=c then bool :=false :
             else j :=j+1 : fi :
    od :
    h :=[op(h),j] :
    if nops(h)=l[i][2] then bool_bis :=false : fi :
  od :
  g :=[op(g),h] :
od :
h :=[seq(0,i=1..nops(g))] :
for i from 1 to nops(g)
do
  h[i] :=add(g[i][j]*l[i][1]^(j-1),j=1..nops(g[i])) mod l[i][1]^l[i][2]
od :
k :=0 :
for i from 1 to nops(h)
do
  b :=mul(l[j][1]^l[j][2],j=1..nops(l))/l[i][1]^l[i][2] :
  q :=inver(b,l[i][1]^l[i][2]) :
  k :=k+b*q*h[i] :
```

od :
k mod m ; end proc ;

A.8 Annexe : Résultats pratiques :

La correspondance entre les caractères orthographiques et les entiers est fournie par le code ASCII (comme indiqué dans les programmes en Caml ou en Maple grâce au choix de $p = 257$).

A.8.1 Cas n=3, p=257 :

n :=3 ; p :=257 ; dans ce cas #G= 66048
alpha :=[37, 62, 20] ;
a := 33370 ;
beta := [179, 20, 243] ;

On code la citation suivante : "Et lorsqu'on vient à voir vos célestes appas, un cœur se laisse prendre et ne raisonne pas." (Molière : Tartuffe)

Voici un codage possible de cette citation : [[[173, 61, 241], [109, 236, 225]], [[139, 206, 47], [111, 34, 64]], [[218, 81, 104], [185, 137, 119]], [[155, 200, 21], [222, 12, 64]], [[223, 21, 227], [141, 196, 236]], [[134, 78, 145], [133, 253, 94]], [[53, 186, 11], [31, 238, 157]], [[139, 91, 180], [131, 72, 35]], [[52, 243, 97], [90, 11, 111]], [[100, 79, 207], [60, 203, 58]], [[65, 243, 241], [155, 70, 207]], [[52, 191, 138], [242, 211, 143]], [[23, 89, 192], [121, 8, 150]], [[74, 60, 230], [159, 196, 117]], [[112, 130, 247], [94, 188, 48]], [[5, 11, 37], [36, 222, 152]], [[215, 41, 59], [223, 57, 190]], [[226, 150, 46], [54, 17, 60]], [[255, 44, 165], [33, 230, 193]], [[28, 27, 0], [164, 60, 40]], [[133, 25, 45], [104, 115, 144]], [[35, 51, 88], [58, 96, 6]], [[38, 169, 71], [236, 126, 18]], [[19, 38, 32], [8, 220, 42]], [[128, 162, 253], [176, 228, 133]], [[103, 118, 107], [124, 239, 9]], [[28, 33, 17], [127, 205, 155]], [[200, 107, 103], [191, 210, 38]], [[144, 59, 210], [120, 164, 30]], [[24, 200, 101], [126, 72, 61]], [[202, 11, 80], [221, 68, 24]]] ;

A.8.2 Cas n=7, p=257 :

n :=7 ; p :=257 ; dans ce cas #G= 288136807515648
alpha := [232, 154, 146, 107, 37, 41, 210] ;
a := 162386677410711 ;
beta := [1, 129, 36, 122, 15, 227, 194] ;

On code la citation suivante : "Mon beau voyage encore est si loin de sa fin ! Je pars, et des ormeaux qui bordent le chemin j'ai passé les premiers à peine." (André Chénier)

Voici un codage possible de cette citation : [[[214, 156, 139, 249, 177, 69, 173], [19, 116, 240, 38, 85, 43, 77]], [[238, 113, 18, 28, 213, 126, 156], [147, 197, 242, 150, 69, 6, 165]], [[59, 140, 44, 53, 37, 11, 185], [79, 128, 173, 50, 16, 68, 127]], [[236, 45, 227, 226, 161, 34, 171], [160, 222, 216, 193, 171, 190, 116]], [[17, 237, 183, 97, 90, 39, 18], [209,

126, 67, 103, 106, 184, 226]], [[143, 55, 76, 224, 245, 49, 91], [173, 5, 247, 192, 45, 44, 146]], [[144, 103, 44, 139, 142, 118, 115], [114, 199, 206, 0, 104, 25, 201]], [[16, 239, 173, 77, 187, 187, 233], [206, 239, 159, 102, 24, 85, 81]], [[228, 42, 183, 112, 161, 37, 218], [76, 199, 4, 37, 242, 81, 157]], [[143, 252, 73, 108, 23, 149, 109], [163, 114, 196, 65, 52, 188, 156]], [[43, 125, 91, 48, 48, 192, 39], [187, 66, 101, 214, 20, 78, 43]], [[51, 248, 16, 183, 199, 225, 233], [254, 180, 98, 244, 194, 72, 235]], [[9, 142, 240, 34, 43, 204, 184], [33, 171, 155, 14, 166, 12, 108]], [[219, 14, 212, 69, 54, 33, 38], [148, 146, 12, 244, 200, 43, 242]], [[218, 86, 4, 13, 141, 69, 20], [100, 224, 232, 218, 65, 200, 134]], [[133, 134, 38, 130, 66, 66, 45], [205, 191, 220, 164, 240, 193, 204]], [[155, 18, 238, 108, 122, 253, 88], [139, 247, 12, 251, 108, 141, 120]], [[248, 66, 218, 58, 99, 100, 96], [40, 140, 248, 12, 149, 51, 209]]] ;

A.8.3 Cas n=19, p=257 :

n :=19 ; p :=257 ;

dans ce cas #G= 2392193026117453804855151154629552472490444 8 $\approx 2,3.10^{43}$

alpha := [86, 214, 234, 30, 10, 95, 47, 57, 230, 119, 120, 149, 2, 230, 3, 146, 145, 4, 190] ;

a := 65411049156393798004868354115572143929453 56 ;

beta := [69, 84, 52, 151, 15, 215, 227, 130, 42, 200, 46, 27, 186, 64, 241, 153, 108, 25, 102] ;

On code la citation suivante : "Jeunes, gais, satisfaits, sans soins, sans prévoyance, quel besoin avions-nous d'une telle abondance" (Voltaire)

Voici un codage possible de cette citation : [[[13, 113, 130, 76, 106, 116, 50, 137, 153, 53, 86, 210, 143, 186, 19, 168, 22, 167, 184], [86, 74, 98, 58, 241, 191, 62, 56, 72, 2, 226, 154, 108, 69, 215, 141, 121, 158, 63]], [[224, 58, 241, 88, 91, 37, 48, 147, 80, 185, 63, 127, 122, 229, 6, 103, 11, 126, 95], [36, 113, 92, 233, 224, 91, 221, 124, 71, 24, 154, 219, 214, 82, 139, 32, 216, 227, 184]], [[4, 143, 200, 139, 89, 55, 34, 124, 144, 37, 211, 15, 107, 192, 179, 200, 249, 134, 225], [129, 138, 32, 4, 174, 217, 149, 199, 123, 88, 242, 245, 103, 66, 42, 183, 44, 161, 64]], [[202, 235, 126, 103, 170, 0, 144, 144, 173, 67, 86, 209, 117, 39, 193, 225, 214, 147, 6], [10, 88, 82, 40, 27, 248, 149, 240, 124, 149, 19, 148, 60, 77, 234, 66, 36, 77, 38]], [[56, 113, 41, 114, 188, 158, 250, 93, 6, 38, 114, 194, 70, 40, 111, 17, 157, 207, 34], [149, 135, 177, 228, 189, 41, 1, 232, 142, 215, 151, 219, 79, 96, 201, 215, 154, 125, 73]], [[184, 162, 35, 246, 159, 43, 70, 192, 67, 176, 104, 93, 120, 201, 131, 169, 246, 143, 127], [12, 241, 144, 230, 196, 48, 119, 29, 0, 242, 122, 62, 91, 242, 37, 60, 31, 231, 24]]] ;

A.8.4 Cas n=37, p=257 :

n :=37 ; p :=257 ;

dans ce cas $\#G \approx 6.10^{86}$, et le plus grand facteur premier de #G fait 25 chiffres.

alpha := [160, 244, 210, 53, 231, 237, 80, 164, 224, 177, 115, 10, 241, 205, 234, 194, 173, 150, 127, 106, 76, 167, 111, 16, 67, 177, 164, 85, 181, 214, 33, 127, 233, 199, 227, 46, 69] ;

a :=3411580715404269422484344762067542365684237770723074252413876184569
597992359
88915989289 ;
beta := [80, 121, 34, 54, 98, 174, 29, 145, 200, 139, 150, 116, 171, 230, 165, 34, 35, 116, 192, 135, 145, 230, 59, 118, 55, 240, 129, 145, 175, 182, 70, 126, 86, 34, 4, 249, 212] ;

On code la citation suivante : "Un poète doit laisser des traces de son passage, non des preuves. Seules les traces font rêver." (René Char)

Voici un codage possible de cette citation : [[[30, 250, 104, 107, 83, 138, 240, 200, 122, 198, 97, 49, 156, 72, 161, 129, 130, 93, 12, 60, 102, 31, 200, 212, 137, 224, 233, 186, 124, 157, 238, 137, 98, 171, 147, 54, 14], [89, 211, 224, 145, 234, 229, 149, 9, 203, 231, 201, 54, 24, 0, 183, 101, 46, 129, 170, 191, 150, 3, 131, 239, 124, 82, 145, 246, 72, 233, 171, 230, 255, 18, 207, 42, 68]], [[37, 207, 144, 188, 110, 181, 165, 18, 146, 58, 6, 36, 110, 206, 187, 106, 155, 65, 37, 112, 79, 102, 37, 150, 157, 121, 187, 161, 39, 186, 145, 141, 5, 237, 72, 204, 38], [211, 230, 56, 126, 112, 64, 170, 217, 203, 145, 245, 42, 117, 62, 192, 218, 137, 43, 230, 161, 251, 21, 202, 129, 69, 170, 102, 142, 184, 185, 173, 8, 123, 173, 162, 73, 250]], [[90, 48, 201, 238, 66, 82, 180, 56, 164, 64, 111, 70, 70, 38, 169, 45, 186, 28, 63, 171, 92, 138, 38, 56, 100, 134, 28, 25, 34, 155, 87, 182, 81, 89, 133, 152, 202], [169, 192, 81, 67, 105, 67, 53, 5, 188, 29, 36, 69, 123, 70, 252, 160, 128, 181, 140, 6, 142, 71, 25, 61, 58, 235, 191, 159, 212, 235, 210, 167, 70, 176, 95, 100, 217]]]

A.9 Annexe : Deux propositions utilisées sans démonstration :

A.9.1 Preuve que $\mathbb{K}^*$ est cyclique :

Soit $\mathbb{K}$ un corps, G un sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$, alors G est cyclique.

- On rappelle la formule de Mobius : $\sum_{d/n} \phi(d) = n$
- Montrons la proposition suivante : si n=#G pour tout d divisant n , #{x∈G, x d'ordre d}=ϕ(d).
  Si c'est le cas, en particulier {x∈G, x d'ordre n} est non vide, G est donc cyclique.
- soit d un diviseur de n , soit {x∈G, x d'ordre d} est l'ensemble vide. Sinon il existe b∈ G, d'ordre d, {1,b,...,b^{d-1}} est le groupe engendré par b qui contient ϕ(d) éléments d'ordre d.
  De plus, si a∈ G et a est d'ordre d alors a est un élément du groupe engendré par b car le polynôme $X^d - 1$ a au plus d racines, or tous les éléments du groupe à d éléments engendré par b sont racines de ce polynôme. Donc soit #{x∈G, x d'ordre d}=0, sinon #{x∈G, x d'ordre d}=ϕ(d).
  Or n=#G=$\sum_{d/n} \#\{x \in G,\ x\ d'ordre\ d\} \leq \sum_{d/n} \phi(d) = n$ d'où la conclusion.

A.9.2 Preuve de l'irréductibilité des polynômes cyclotomiques :

Démontrons que si $\mathbb{K}$ est un corps de cardinal q et si n est un nombre premier avec q alors la classe de q modulo n est un élément inversible de $((\frac{\mathbb{Z}}{n\mathbb{Z}})^*, \times)$ et si l'on note r l'ordre de $\bar{q}$ alors tous les facteurs premiers de K_n, le n-ième polynôme cyclotomique, sont simples et de degré r.

- Rappel avant la preuve : si $\mathbb{K}$ est un corps fini alors le cardinal de $\mathbb{K}$ est p^m où p est la caractéristique de $\mathbb{K}$, un nombre premier.
- Preuve de la proposition : tout d'abord, montrons que tous les facteurs premiers de K_n dans $\mathbb{K}[X]$ sont simples.
  En effet par l'absurde si K_n s'écrit $K_n = P^2Q$ alors $X^n - 1 = \prod_{d/n,\ d\leq n} K_d = P^2R$
  donc, en dérivant $nX^{n-1} = P(2P'R + PR')$ et en conséquence :
  $n = X(nX^{n-1}) - n(X^n - 1) = XP(2RP' + PR') - nP^2R = P[X(2RP' + PR') - nPR]$
  Or n est différent de $0_{\mathbb{K}}$ car si c'est le cas alors $n \in p\mathbb{Z}$ ce qui est impossible car $n \wedge p = 1$
  Donc l' égalité ci-dessus est impossible si deg(P)> 1
  Donc tous les facteurs premiers de K_n sont simples.
- Ensuite : Soit P un facteur premier de K_n, $P \in \mathbb{K}[X]$. Notons s son degré, de plus on note r l'ordre de $\overline{q}$ dans $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$. Montrons que r=s :
  L'idéal $P\mathbb{K}[X]$ est maximal dans $\mathbb{K}[X]$ donc $\frac{\mathbb{K}[X]}{P\mathbb{K}[X]}$ est un corps à q^s élément qui contient le corps $\mathbb{K}$ ($q = \#\mathbb{K}[X]$).
  Donc pour tout élément a non nul de $\frac{\mathbb{K}[X]}{P\mathbb{K}[X]}$, $a^{q^s-1} = 1$
  Or $P = 0 \Rightarrow K_n = 0 \Rightarrow X^n = 1$. Si l'ordre de X dans $\frac{\mathbb{K}[X]}{P\mathbb{K}[X]}$ est $d < n$ alors $X^d - 1 = 0 \Rightarrow \prod_{k/d,\ k\leq d} K_k = 0 \Rightarrow$ il existe $k \leq d$ tel que $K_k = 0$. Mais k/d et $d/n \Rightarrow k/n$
  De plus $K_k = 0 \Rightarrow P/K_k$ donc P^2 divise $X^n - 1$ ce qui est impossible.
  Donc $X^{q^s-1} = 1 \Rightarrow q^s - 1 = 0\ mod\ n \Rightarrow q^s = 1\ mod\ n \Rightarrow s = 0\ mod\ r$, donc $r \leq s$
- Pour finir : r est l'ordre de $\bar{q}$ dans $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ donc $q^r = 1\ mod\ n \Rightarrow q^r - 1$ est un multiple de n.
  Donc, pour tout i, $(X^i)^{q^r} = X^i$
  De plus pour tous polynômes P et Q de $\mathbb{K}[X]$ $(P + Q)^{q^r} = P^{q^r} + Q^{q^r}$. Car la caractéristique de $\mathbb{K}$, p, divise tous les $\binom{q^r}{k}$ sauf pour $k = 0$ et $k = q^r$
  Donc pour tout $P \in \frac{\mathbb{K}[X]}{P\mathbb{K}[X]}$, $P^{q^r} = P$. Donc le polynôme $X^{q^r} - X$ admet comme racine tous les éléments de $\frac{\mathbb{K}[X]}{P\mathbb{K}[X]}$ donc $q^s \leq q^r \Rightarrow s \leq r$. Donc r=s.

– En conséquence : Si $\bar{q}$ est un générateur de $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ alors tous les facteurs premiers de K_n sont de degré $\phi(n)$ et si en plus n est premier alors l'ordre de $\bar{q}$ est $n-1$ donc tous les facteurs premiers de K_n sont de degré $n-1$ or $n-1$ est le degré de K_n qui est donc irréductible.

Postface

La cryptographie, c'est l'art de transmettre des informations de telle manière qu'elles ne soient compréhensibles que du récipiendaire légitime des données. Autrefois de très nombreux systèmes (dits à *clef symétrique*) ont été inventés en ce sens (chiffre de César, carré de Vigenère, chiffre des francs-maçons, chiffre VIC, et même le code Morse !).

Aujourd'hui, dans un monde où l'informatique règne en maître, la cryptographie est utilisée en permanence : cartes de crédits, sites internet, téléphones portables... Partout autour de nous se cachent des codes. Bien évidemment, les systèmes actuels sont bien plus complexes que ceux d'autrefois, complexité rendue possible grâce au développement de l'informatique et à l'accroissement perpétuel de la puissance de calcul des ordinateurs. La cryptologie repose désormais sur des mathématiques subtiles et ardues, inaccessibles au profane, mais fascinantes pour celui qui a la chance d'avoir quelques bases en arithmétique, et la volonté de se plonger dans cet univers fascinant des anneaux, des corps et des nombres premiers.

Dans cet ouvrage, Pierre Meunier, professeur en classes préparatoires à Montpellier depuis de nombreuses années, veut nous montrer et nous faire apprécier les mathématiques utilisées en cryptographie. Ce travail extraordinaire, il l'a entrepris essentiellement pour ses élèves, et en tant qu'ancien étudiant de M. Meunier, je puis affirmer que ce fut, sans conteste, le domaine des mathématiques qui m'a marqué le plus lors de mon passage au lycée Joffre.

Si le lecteur s'en donne la peine, je suis certain qu'il trouvera autant de plaisir à parcourir ces pages que j'en ai eu à taper ces lignes. Je vous souhaite bon courage, et surtout bonne lecture !

Samuel Franco, moine copiste

Vous pouvez faire part de vos remarques,
critiques, suggestions
aux auteurs à cette adresse :

auteurs@cepadues.com

Achevé d'imprimer en France
en décembre 2010 chez Messages SAS
111, rue Nicolas-Vauquelin • 31100 Toulouse
Tél. : 05 61 41 24 14 • Fax : 05 61 19 00 43
imprimerie@messages.fr