Université Mohammed-V Agdal
Faculté des Sciences de Rabat
Département d'Informatique
Av Ibn battouta, B.P 10 14 Rabat

Email : ouahidi@fsr.ac.ma
Tél : 037 77 54 71

# Théorie des Nombres Appliquée à la Cryptographie

Ce fasicule [1] regroupe une série d'exerices sur la théorie des nombres appliquée à la cryptographie mathématique. Ils s'adressent aux étudiants de master Mathématiques et Informatique.

[1] ©Pr Bouabid EL Ouahidi, email :ouahidi@fsr.ac.ma

# Série 1

1°) Montrer que $pgcd(a,m)=1 \Longleftrightarrow a$ est invesrible modulo $m$

2°) Soit l'équation : $ax \equiv b mod\ m$ monter qu'elle a :

$$\begin{cases} d=pgcd(a,m) & solutions\ si\ d|b \\ 0 & solutions\ si\ d \not| b \end{cases}$$

3°) Soit $p$ premier impair, $t \in \mathbb{N}^*$, $e \geq 1$, montrer que l'équation en $x$ : $x^t \equiv 1\ mod\ p^e$ admet $pgcd(t,\varphi(p^e))$ solutions.

Montrer que l'équation en $x$ : $x^t \equiv -1\ mod\ p^e$ admet $pgcd(t,\varphi(p^e))$ solutions si $pgcd(t,\varphi(p^e))\ |\frac{\varphi(p^e)}{2}$ et 0 solutions sinon.

4°) Soit les trois équations suivantes :

$$\begin{cases} f(x) \equiv 0\ mod\ m*n & (1) \\ f(x) \equiv 0\ mod\ m & (2) \\ f(x) \equiv 0\ mod\ n & (3) \end{cases}$$

Soit $n_1,\ n_2,\ n_3$ le nombre de solutions respectivement de (1), (2) et de (3). Montrer que : $n_1 = n_2 * n_3$.

5°) Résoudre le système suivant :

$$\begin{cases} x \equiv 2\ mod\ 3 \\ x \equiv 4\ mod\ 5 \\ x \equiv 6\ mod\ 7 \end{cases}$$

6°) Quels sont les nombres premiers $p$ pour lesquels $-2$ est un carré modulo $p$, même question en remplaçant $-2$ par 3.

7°) Soit $n=2^{2^k}+1$ Montrer que $n$ est premier si 5 est un non résidu modulo $n$.
Montrer que : $n$ est premier $\Longleftrightarrow 5^{\frac{n-1}{2}} \equiv -1 mod\ n$.

8°) Soit $p$ un nombre premier, $p \equiv -1\ mod\ 4$ soit l'équation en x : $y \equiv x^2\ mod\ p$
a) Montrer que $y^{\frac{p+1}{4}}\ mod\ p$ est solution ?
b) Trouver $x$ lorsque $p=103$ et $y=28$ ?

8°) Le but de ce qui suit est de chercher $z$ tel que : $z^2 \equiv 28\ mod\ 309$.
a) Montrer que si $t \equiv 1\ mod\ 3$ et $t \equiv 50\ mod\ 103$ alors $t^2 \equiv 28\ mod\ 309$
b) Trouver tous les $t$ tels que : $t \equiv 50\ mod\ 103$ (il y en a trois).
c) En déduire $z$ tel que : $z^2 \equiv 28\ mod\ 309$.

# Série 2

1) Montrer que dans l'algortithme de calcul de la relation de bezout $am+bn = pgcd(m,n)$ les coefficients $a$ et $b$ vérifient $|a| \leq n$ et $|b| \leq |m|$.

2) Calculer l'inverse de 5 dans $\mathbb{Z}/17\mathbb{Z}$.

3) Quels sont les générateurs de $\mathbb{Z}/n\mathbb{Z}$ ? Quels sont les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (c'est à dire les bijections de $\mathbb{Z}/n\mathbb{Z}$ dans lui même vérifiant $f(a+b) = f(a) + f(b)$).

4) Montrer que tout sous-groupe d'un groupe cyclique est cyclique ? Calculer le nombre de sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
5) Quels sont les générateurs de $(\mathbb{Z}/13\mathbb{Z})^*$ ?

6) Soit $p$ un nombre premier donné. Écrire un algortithme qui recherche un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.

7) Résoudre les congurences simultanées :

$$\begin{cases} x & \equiv & 1 \ mod\ 2 \\ x & \equiv & 2 \ mod\ 3 \\ x & \equiv & 4 \ mod\ 5 \\ x & \equiv & 6 \ mod\ 7 \\ x & \equiv & 18 \ mod\ 29 \\ x & \equiv & 31 \ mod\ 53 \end{cases}$$

8) Soit $n \geq 1$, montrer que la fraction $\frac{1}{n}$ a un développement décimal périodique de période $r$ et que $r$ est l'ordre de 10 dans le groupe $(\mathbb{Z}/13\mathbb{Z})^*$. (On suppose que $2 \not| n$ et $5 \not| n$). De façon générale étudier le développement dècimal de $\frac{1}{n}$ .

9) Montrer que si $x^2 \equiv a \ mod\ p^\alpha$ alors
Si $y \equiv 2^{-1}(x + \frac{a}{x}) \ mod\ p^{2\alpha}$ on a $y^2 \equiv a \ mod\ p^{2\alpha}$
(Si l'on connaît un résidu quadratique de $a$ module $p^\alpha$, on peut connaître son résidu quadratique modulo $p^{2\alpha}$.

# Série 3

1) Résoudre les congruences :

$$\begin{cases} x^7 & \equiv & 15\ [29] \\ x^7 & \equiv & 12\ [29] \end{cases}$$

2) Démontrer le théorème de Wilson :

$$(p-1)!\ \equiv\ -1\ [p] \Longleftrightarrow p \text{ est premier}$$

3) Résoudre l'équation : $y^2\ =\ x^3\ +\ 2x\ +3$ dans $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/35\mathbb{Z}$.

4) Le nombre de faux témoins pour $n$, c'est à dire le nombre de $a$, $1 \leq a \leq n-1$, vérifiant $a^{n-1}\ = \equiv\ [n]$ est égal à : $\prod_{p|n} pgcd(p-1, n-1)$
Application : $n = 561, \quad n = 341$.

5) Quels sont les nombres premiers p pour lesquels $-2$ est un facteur carré $[p]$ ? Même question pour 3.

6) Écrire un algorithme calculant le symbole de Jacobi $(\frac{n}{m})$.

7) Pour $n$ fixé, construre un tableau $\mathbb{Q}(1)$, ..., $\mathbb{Q}(a)$, ..., $\mathbb{Q}(n)$, tel que $\mathbb{Q}(a) = 1$ si $a$ est un carré $[n$ et $\mathbb{Q}(a) = -1$ sinon.
Puis calculer le nombre de carrés $[n]$, que l'on appelle $q(n)$. Montre que $q(n)$ est une fonction multiplicative $((m,n) = 1\ \Rightarrow\ q(mn) = q(m)q(n)$ et que :

$$q(p^\alpha) = \frac{p^{\alpha+1}}{2(p+1)} + 1 \ si\ p \neq 2 \ \ et \quad q(2^\alpha) = \frac{2^\alpha}{6} + 2.$$

Calculer q(110880).

# Série 4

1) Soit $p \equiv 2\ [3]$. Montre que $x \mapsto x^3$ est un automorphisme de $(\mathbb{Z}/p\mathbb{Z})^*$. Calculer le nombre de solutions de $y^2 = x^3 + a$ dans $\mathbb{Z}/p\mathbb{Z}$.

2) Soit $n = 2^{2^k} + 1$ Montrer que is $n$ est premier ; 5 est un non résidu quadratique pour $n$. Montrer que :

$$n \quad est \quad premier \iff 5^{\frac{n-1}{2}} \equiv -1\ [n]$$

3) On suppose que $n = 2^{2^k} + 1$ a un diviseur premier $p$. Montrer que l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$ est $2^{k+1}$. En déduire, lorsque $k \geq 2$ que 2 est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$. Soit $y$ tel que $y^2 = 2$. Quel est l'ordre de $y$. En déduire que $p \equiv 1\ [2^{k+2}]$. Application $k = 5$ : quels sont les $p$ possibles.

4) Montrer que $n = 2^{2^k} + 1$ est psp-2, est pspf-2.
Soit $p$ un nombre premier, montrer que $n = 2^p - 1$ est psp-2, pspf-2.

5) Soit $n \equiv 5\ [8]$. Montrer que $n \ \ est \ \ pspe - 2 \ \Rightarrow \ n \ est \ pspf - 2$

Soit $n \equiv 5\ [12]$. Montrer que $n \ \ est \ \ pspe - 3 \ \Rightarrow \ n \ est \ pspf - 3$

6) Montrer que $6m + 1$, $12m + 1$, $18m + 1$ sont des premiers, leur produit est un nombre de Carmichael.

7) Montrer que $n$ est un nombre de Carmichael est équivant à : $\forall\ a \in \mathbb{Z}, \ \ a^n \equiv a\ [n]$ .

8) Soit $n = 1729$. Calculer $a^{\frac{n-1}{2}}\ [n]$ lorsque $(a, n) = 1$.

# Série 5

1) Calculer $mod(111, 555)$, $mod(\frac{10^{21}-1}{9}, 5\frac{10^{14}-1}{9})$.

2) Soit $n = 2^s t + 1$ avec $t$ impair. On suppose qu'il existe $b$ tel que $b^{\frac{n-1}{2}} \equiv -1\ [n]$. Montrer que si $p$ est diviseur premier de $n$ alors $p = 2^s d + 1$, où $d \in \mathbb{N}$. Montrer que si $a$ est tel que $a^{\frac{n-1}{2}} \in \{\pm 1\}\ [n]$ alors forcément $a^{\frac{n-1}{2}} \equiv (\frac{a}{n})\ [n]$.
On observera que si

$$n = \prod_{i=1}^{k} p_i \text{ avec } p_i = 2^s d_i + 1 \text{ on a } \sum_{i=1}^{k} d_i \text{ impair}$$

.

3) Soit $n = 1729$. Quel est le nombre de bases de bases $b$, $1 \leq b \leq 1729$ pour lesquelles $n$ est pp-f en base $b$. Même question pour $n = 49939$. $n = 99877$

4) Soit $p$ un nombre premier $\neq 2$. Montrer que la congruence $x^4 \equiv -1[p]$ a une solution si et seulement si $p \equiv 1[8]$.
Montrer q'il existe une infinité de nombres premiers $p \equiv 1[8]$. On raisonnera par l'absurde, en supposant qu'il y en a un nombre fini $p_1, \ldots p_n$ et en considérant $(p_1 p_2 \ldots p_n)^4 + 1$

5) Soit $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, avec $p_i = 2^{s_i} t_i + 1$ avec $s_1 \leq s_2 \leq \ldots \leq s_k$ et $n = 1 + 2^s t$ avec $t$ et $t_i$ impairs. Montrer que le nombre des bases $b$ pour lesquelles $n$ est un ppe en base $b$ vaut : (avec $1 \leq b \leq n-1$)) :

$$\delta \prod_{i=1}^{k} (\frac{n-1}{2}, p_i - 1) \text{ où } \delta \in \{2, \frac{1}{2}, 1\}$$

# Série 6

1) On suppose que $n$ a deux diviseurs premiers $p_1$ et $p_2$ vérifiant $p_1 = 2^{s_1}t_1+1$, $p_2 = 2^{s_2}t_2+1$ $t_1$, $t_2$ impairs, $s_1 \leq s_2$, et qu'il existe $b \leq 2\,log^2(p_2)$ avec $(\frac{b}{p_2}) = -1$. Montrer que $n$ n'est pas un ppf-b.

On suppose maintenant que $s_1 = s_2$, et qu'il existe $b$ tel que $(\frac{b}{p_1}) = +1$ et $(\frac{b}{p_2}) = -1$. Montrer que l'ordre de $b$ dans $(\mathbb{Z}/p_2\mathbb{Z})^*$ est de la forme $2^{s_1}\beta_1$ avec $\beta_1$ impair, et que l'ordre de $b$ dans $(\mathbb{Z}/p_1\mathbb{Z})^*$ est de la forme $2^{s'}\beta_1$ avec $s' \prec s_1$. En déduire que $n$ n'est pas ppf-b. Montrer que ceci justifie le test de primalité de Miller sous l'hypothèse de Reimann généralisée.

2) Écrire un certificat de primalité pour le nombre 127.

3) Montrer que tous sous graphe additif de $\mathbb{R}$ est discret, ou dense dans $\mathbb{R}$. Montrer que l'ensemble $\{a + 2\pi b; a \in \mathbb{Z}, b \in \mathbb{Z}\}$ est un sous groupe de $\mathbb{R}$. On admettra que $\pi$ est irrationnel. Quelles sont les valeurs d'adérence de la suite $(\cos(n))_{n\geq 0}$?

4) Exercice de programmation : Entrer un nombre réel $\theta \succ 0$, et un nombre entier $N$. Pour $0 \leq n \leq N$, construire le tableau $X(n) = \{n\theta\}$ = partie fractionnaire de $n\theta$. Ordonner ce tableau en un tableau ordonné $Y(n)$, $0 \leq n \leq N$ avec $Y(0) \leq Y(1) \leq \ldots \leq Y(N)$. Caclculer les différences $Y(n+1) - Y(n)$. Qu'observe t-on ?

5) Soit $n \geq 2$, $a \geq 1$ et $n|(a^2+1)$. Montrer qu'il existe deux nombres entiers $s$ et $t$ tels que $n = s^2 + t^2$. On choisira pour $s$ le plus grand dénominateur $q_k$ qui soit $\leq \sqrt{n}$, des réduites du nombre $\frac{a}{n}$. On montrera que $|\frac{a}{n} - \frac{p_k}{q_k}| \leq \frac{1}{(q_k([\sqrt{n}]+1)}$. Montrer que tout nombre premier $p \equiv 1[4]$ est la somme de deux racines carrés.

# Série 7

1) Trouver le nombre rationnel de la forme $\frac{a}{b}$ avec $1 \leq b \leq 100$ le plus près possible de $\sqrt{2}$.
2) Soit une fraction continue $[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}$. Montrer que $[a_n, a_{n-1}, \ldots, a_1] = \frac{q_n}{q_{n-1}}$ , et que $[a_n, \ldots, a_1, a_0] = \frac{p_n}{p_{n-1}}$.

3) Soit d un nombre entier sans facteur carré (c'est à dire $p$ premier divise $d \Rightarrow p^2$ ne divise pas $d$). Montrer que, si l'équation $x^2 - dy^2 = 1$ a une racine $(x, y) \in \mathbb{N} \times \mathbb{N}$, alors $\frac{x}{y}$ est une reduite de $\sqrt{d}$ .

4)
a) Soit $a, n, k$ des entires $\geq 0$, $a \neq 0$, on pose :

$$u_{n,k} = \frac{2^n((n+k)!)}{k!(2n+2k)!} \frac{1}{a^{2k}}$$

$$v_n = \sum_{k=0}^{\infty} u_{n,k}, \quad w_n = a\frac{v_n}{u_n}$$

Montrer que $w_n$ vérifie la relation de récurrence $w_n = (2n+1)a + \frac{1}{w_{n+1}}$

En déduire le développeme en fraction continue de $\frac{\cosh(a)}{\sinh(a)}$ et celui de $\frac{e-1}{e+1}$.
b) $b$ et $c$ étant des entiers positifs, $(g_n)_{n\geq 0}$ une suite d'entiers strictement positifs (sauf $g_0$ qui peut être négatif) on pose :

$$\alpha = [g_0, b, c, g_1, b, c, g_2, b, c, \ldots]$$

$$\alpha' = [g_0(bc+1) + b + c, g_1(bc+1) + b + c, \ldots]$$

Soit $\frac{p_n}{q_n}$ et $\frac{p'_n}{q'_n}$ les $n^{imes}$ réduites de $\alpha$ et $\alpha'$

Montrer que $p_{2n+3} = p'_n - bq'_n$ ; $q_{3n+2} = (bc+1)q'_n$.
Calculer $\alpha'$ en fonction $\alpha$. Du développement en fraction continue de $\frac{e-1}{e+1}$, déduire celui $e$.

# Série 8

1) Soit $x$ réel $\geq 1$. Soit $(\frac{p_n}{q_n})_{n\geq 0}$ l'ensemble de ses réduites. Montrer que l'ensemble des réduites de $\frac{1}{x}$ est $\{0\} \cup \{(\frac{p_n}{q_n})_{n\geq 0}\}$.

2) On veut adapter la méthode de S.Lehmann pour montrer que $n$ n'a pas de diviseurs entre $\frac{\sqrt{n}}{10}$ et $\sqrt{n}$. Quel est le coût de cet algorithme ?

3) On pose $P(m,n) = \frac{m(m-1)...(m-n-1)}{m^n}$ pour $1 \leq n \leq m$. En utilisant la formule de sommatoire de d'Euler Mac Laurin, montrer qu'il existe $\theta$ $1 \succ \theta \succ 1$ tel que :

$$log(P(m,n)) = (m-n+\frac{1}{2})log(\frac{m}{m-n}) - n - \frac{\theta n}{12m(m-n)}$$

Application : Calculer $P(365, 23)$

4) Calculer $\int_0^\infty e^{-t}t^n dt$ et en déduire que :

$$\frac{n!}{n^n}\sum_{k=0}^{n}\frac{n^k}{k!} = \int_0^\infty e^{-t}(1+\frac{t}{n})^n dt$$

En utilisant les inégalités : $log(1+u) \geq u - \frac{u^2}{2}$ et $n! \leq n^n e^{-n}\sqrt{2\pi n}\ exp(\frac{1}{12n})$ montrer que :

$$\sum_{k=0}^{n}\frac{n^k}{k!} \geq \frac{1}{2}exp(n-\frac{1}{2n})$$

5) Calculer la queue et le cycle de la suite liée à l'application de $\mathbb{Z}17\mathbb{Z}$ dans lui même définie par $f(x) = x^2 + 1$ [17] et que $x_0 = 3$.

6) Soit $E_m$ un ensemble à $m$ éléments et $x_0 \in E_m$. On suppose que chaque $x_0 \in E_m$ et que chaque $f \in \mathcal{F}(E_m, E_n)$ sont équiprobables. Calculer l'espérance mathématique de la longueur $\lambda$ de la suite $x_{n+1} = f(x_n)$

7) Écrire un programme réalisant la méthode de factorisation suivante : (1) Entrer $N$ ; Faire K=1 ; (2) Choisir $D$ au hasard entre 2 et $\sqrt{N}$ ; (3) Tester si $D$ divise $N$, si oui terminer afficher $K$ ; sinon faire $K = k + 1$ et aller en (2).
Application N=6731. Que pensez-vous de cette méthode ?

# Série 9

Exercice 1 :

a) Soit $w = 2^s t$, $s \in \mathbb{N}$, $t$ impair. On considère la suite $x_0 = 1$, $x_k \equiv 2x_{k-1}[w]$. Montrer que si $e$ est l'ordre de 2 dans $(\mathbb{Z}/t\mathbb{Z})^*$, la queue de la suite $x_k$ est formée de $1, 2, \ldots, 2^{s-1}$ et le cycle de $2^s, \ldots, 2^{s+e-1}$. Montrer que l'épacte vaut $\lceil \frac{s}{e} \rceil e$ .

b) Soit $p$ un nombre premier. $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ définie par $f(x) = x^2$, $a_0 = a$, $a_k = f(a_{k-1}) = a^{2^k}$ $[p]$. Soir $w$ l'ordre de $a$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Calculer la queue, le cycle et l'épacte de la suite $a_k$. Application p=59, a=2.

c) Soit $a \neq 1$, $a \in (\mathbb{Z}/p\mathbb{Z})^*$. On pose $x_0 = a + \frac{1}{a}$, $f(x) = x^2 - 2$ $[p]$, $x_k = f(x_{k-1})$. On a ainsi $x_k = a^{2^k} + a^{-2^k}$. Montrer que si $a + \frac{1}{a} = b + \frac{1}{b}$ $[p]$, on a soit $a = b$, soit $a = \frac{1}{b}$ . Soit $w = 2^s t$, l'ordre de $a$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que $x_0, x_1, \ldots x_s$ sont distincts. Montrer que si l'équation en $w$ : $2^w = -1[t]$ a au moins une racine, le cycle vaut $\frac{1}{e}$, si elle n'en a pas, le cycle vaut $e$. Déterminer la queue, le cycle, l'épacte.

d) Soit $x_0 \in (\mathbb{Z}/p\mathbb{Z})^*$. On suppose qu'il n'existe pas de $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que : $x_0 = a + 1/a$. Soit $\mathbb{F}_{p^2}$ le corps à $p$ éléments. Soit $\alpha \in \mathbb{F}_{p^2}$ tel que $x_0 = \alpha + 1/\alpha$. On a $\alpha^p = 1/\alpha$ soit $\alpha^{p+1} = 1$ dans $\mathbb{F}_{p^2}$. Soit $w$ l'ordre de $\alpha$ dans $\mathbb{F}_{p^2}^*$, $w$ divise $(p+1)$, $w = 2^s t$, $e$ est l'ordre de 2 dans $(\mathbb{Z}/t\mathbb{Z})^*$. Montrer que $\alpha, \alpha^2, \ldots, \alpha^{2^s}$ sont tous distints dans $\mathbb{F}_{p^2}$ et que $\alpha^{2^{s+e}} = \alpha^{2^s}$. Montrer que $x_0, \ldots, x_s$ sont distincts. S'il existe $w$ avec $w \equiv= 1 \ mod \ t$ , le cycle vaut $e/2$, s'il n'existe pas un tel $w$, le cycle vaut $e$. Application numérique : $p = 5$, $x_0 = 1$.

2) Montrer que si $2 \leq a \leq b$, on a :

$$\psi(x, b) = \psi(x, a) + \sum_{a < p \leq b} \psi(\frac{x}{p}, p)$$

Application numérique : $b = x$, $a = x^\alpha$ $(\frac{1}{2} \leq \alpha < 1)$.
On montrera que si $y \geq x$, $\psi(x, y) = [x]$. On donne la formule :

$$\sum_{p \leq x} \frac{1}{p} = loglogx + c + O(\frac{1}{logx})$$

# Série 10

1) Faire la liste liste des formes quadratiques binaires, primitives, réduites de discriminant $\triangle = -163$ (1 classe), $-167$ (11 classes), $-75$ (2 classes), $-455$ (20 classes), $-959$ (36 classes).

2) Soit $\mathbb{Z}+i\mathbb{Z}$ le quadrillage du plan complexe (entiers de Gauss). Trouver une base de ce réseau. $\vec{w_1}$, $\vec{w_2}$ telle que la longueur des vecteurs de base soit $\geq 100$. Quelle est la forme quadratique associée ? A quelle forme réduite est elle équivalente ?

3) Soit $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$. Soit $ax^2+bxy+cy^2$ une forme réduite. On la transforme par : $\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} X \\ Y \end{pmatrix}$ en une forme quadratique $AX^2 + BXY + CY^2$. On appliquera à cette dernière forme l'algorithme de réduction. On pose :

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Montrer qu'il existe une suite finie $n_1, n_2, \ldots, n_k \in \mathbb{Z}$ telle que :
$M = \pm IT^{n_1}ST^{n_2}S \ldots ST^{n_{k-1}}ST^{n_k}$.

4) Soit $N = 91$. On considère les congruences mod $N$ :
$95 \equiv 5$; $90 \equiv -1$; $88 \equiv -3$; $81 \equiv -10$; $75 \equiv -16$.

Soit $g$ un générateur de de $(\mathbb{Z}/p\mathbb{Z})^*$ avec $p$ divisant $N$, et $-1 = g^{x_1}$, $2 = g^{x_2}$, $3 = g^{x_3}$, $5 = g^{x_4}$, $11 = g^{x_5}$.
Traduire les congruences ci dessus en équations linéaires en $x_1, \ldots, x_5$. En ajoutant les équations 1, 3 et 5, montyrer que $12x_2 = 0$ et que $(2^6 - 1, N) et (2^6 + 1, N)$ sont des factuesr non triviaux de $N$.

# Série 11

1) Soit $(a,b,c)$ une forme quadratique de discriminant $\triangle < 0$. On suppose que :
- $a \leq \frac{\sqrt{|\triangle|}}{2}$ et $b \leq a$, montrer que la forme est semi réduite.
- $a \leq \sqrt{\frac{|\triangle|}{3}}$ et $b \leq a$, montrer que $|b| \leq c$, et que l'une des deux formes $(a,b,c)$ ou $(c,-b,a)$ est semi réduite.

2) On donne les 5 formes linéaires en $x,y,z,t$ à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ :

$f_1 = x+y+z$, $f_2 = x+z$, $f_3 = y+t$, $f_4 = x+z+t$ et $f_5 = z+t$.

Trouver une relation linéaire de dépendence linéaire.

3) On veut factoriser 5777 par la méthode du cribe quadratique, on pose $f(A) = A^2 + 152A - 1$. Résoudre $f(A) \equiv 0 \mod 7$. Résoudre $f(A) \equiv 0 \mod 49$. Résoudre $f(A) \equiv 0 \mod 2^k$ avec $3 \leq k \leq 8$. Cribler par les puissances de 2 et de 7 les nombres $f(A)$ avec $-12 \leq k \leq 12$. Pour quelles valeurs de $A$ vérifiant $|A| \leq 12$ $f(A)$ se factorise t-il sous le forme $\pm 1.2^{\alpha}7^{\beta}$ ? Factoriser 5777.

4) On pose $\triangle = -224$. Lister les 8 formes quadratiques réduites, primitives de decriminants $\triangle$. On pose $q = (5,4,12)$ et $Q = (4,4,15)$. Calculer $q^2$, $q^3$, $q^4$, $Qq$, $Qq^2$, $Qq^3$, $Q^2$ et en déduire la structure du groupe des formes quadratiques $\mathcal{H}(-224)$.

5) Soit $\triangle = -198596$. calculer

$$n = \prod_{2 \leq p \leq 41} \frac{p}{p - \frac{\triangle}{p}}$$

et en déduire une valeur approchée de $h(\triangle)$. Montrer que $(2,2,\frac{-\triangle+4}{8})$ est ambigue et en déduire que $h(\triangle)$ est pair.

Montre que $F = (3,-2,16550)$ est un générateur du groupe cyclique $\mathcal{H}(\triangle)$.

# Série 12

1) On considère un système RSA : $n = pq$, $e$ l'exposant public de chiffrage. Soit $M$ un message, et $C = M^e \bmod n$ le message chiffré. On construit la suite $C_1 = C^e \bmod n$, $\ldots C_{j+1} = C_j^e \bmod n$.

Montrer qu'il existe un indice $j$ tel que $C_j = C \bmod n$. Que vaut $C_{j-1}$. Montrer que cet indice $j$ divise $\varphi(\varphi(n))$.
Application : $n = 47 * 59$ et $e = 17$, Décrypter le message codé $C = 1504$ .

Montrer que si $\frac{p-1}{2}$ et $\frac{q-1}{2}$ sont premiers, cette méthode de décryptage est peu efficace.

2) Trouver un plynôme $f(x)$ de degré $\leq 3$, à coefficients dans $\mathbb{Z}/11\mathbb{Z}$ tel que $f(1) \equiv 8$, $f(2) \equiv 2$, $f(3) \equiv 4 \bmod 11$ . On pourra utiliser la forme quadratique de Lagrange.

3) On rappelle que tout élément $a \in (\mathbb{Z}/2^k\mathbb{Z})^*$ peut s'écrire sous la forme $(-1)^\alpha 5^\beta$ avec $\alpha \in \{0, 1\}$ et $0 \leq \beta \leq 2^{k-2} - 1$ , et ceci de façon unique lorsque $k \geq 3$.

Trouver *alpha* et $\beta$ lorsque $k = 4$ et $a = 7$. Résoudre les équations $7x^9 \equiv 11 \bmod 32$ et $3^x \equiv 17 \bmod 32$.

Montrer que l'équation $x^2 \equiv a \bmod 2^k$ a ou bien zéro solutions, ou bien exactement 4 solutions.

Université Mohammed-V Agdal
Faculté des Sciences de Rabat
Département de Mathématiques et d'Informatique

Pr Bouabid El Ouahidi, Email : ouahidi@fsr.ac.ma

**Examen**, durée 4 heures : Master SMI

**Porblème n° 1**

Soit $n \in \mathbb{N}^*$, on pose $E_n = (\mathbb{Z}/n\mathbb{Z})^*$, $E_n^2 = \{x^2; x \in E_n\}$.
Lorsque $n$ est impair, on désigne par $(\frac{x}{n})$ le symbole de Jacobi,
et on pose $E_n^+ = \{x \in E_n;\ (\frac{x}{n}) = +1\}$.

1°) Montrer que $E_n^2 \subset E_n^+$

2°) On suppose que $n \equiv 3 \bmod 4$, et que $n$ est pseudo premier en base $a$ (c'est à dire $a^{\frac{n-1}{2}} \equiv (\frac{x}{n}) \bmod n$) pour $a \in E_n$. Montrer que si $(\frac{x}{n}) = +1$, alors $a \in {E_n}^2$, et indiquer un algorithme de calcul de sa racine carrée (mod $n$), déterministe, et polynomial en $log\ n$.

3°) Soit $p$ et $q$ deux nombres premiers $\equiv 3 \bmod 4$. On suppose que $n = pq$. Montrer que l'application $\alpha : E_n^2 \leftarrow E_n^2\ x \rightarrow x^2$ est un isomorphisme de groupe. On notera $\beta$ l'isomorphisme réciproque. Montrer que si $x \in E_n^+$, l'un des deux nombres $x$ ou $-x$ est dans $E_n^2$.

4°) On suppose que l'on connaît $p$ et $q$. Donner un algorithme de calcul de $\beta(a)$, déterminiset , polynomial en $log\ n$.

On suppose que l'on connaît $p$ et $q$, mais que l'on sait calculer $\beta(a)$ pour $a \in E_n^2$, construire in algorithme probabiliste qui factorise $n$.

5°) Soit une boite magique, qui pour l'entrée $x \in E_n^2$ fournit la réponse "oui" si $1 \leq \beta(x) \leq n/2$ et "non" dans le cas contraire. Utiliser cette boite magique pour résoudre le problème de résidualité quadratique : Entrée $x \in E_n^+$, sortie "oui" si $x \in E_n^2$.

6°) On suppose maintenant que $n = pqr$ avec $p = 67$, $q = 103$, $r = 239$. On admettera que $p,\ q,\ r$ son premeirs.

1. Quel est le nombre d'éléments de $E_n, E_n^+, E_n^2$ ?
2. Quel est l'ordre maximum d'un élément de $E_n, E_n^+, E_n^2$ ?
3. Répéter parmi les 6 nombres $p \pm 1,\ q \pm 1, r \pm 1$ ceux qui divisent $n + 1$ ; calculer $(n + 1) \bmod (q + 1)$.

7°) Sot $d \in \mathbb{N}$ un nombre sans facteur carrée et $\sqrt{d}$ sa racine réelle.
Lorsque $(A, B) \in \mathbb{Z}^2$ on dit que :

$A + B\sqrt{d}\ \ equiv 0 \bmod n$, si $A \equiv b \bmod n$ et
$A + B\sqrt{d} \in \mathbb{Z} \bmod n$, si $B \equiv 0 \bmod n$.

Soit P un nombre premier, soit $d$ un carrée modulo $P$ et $(a,b) \in \mathbb{Z}^2$. On suppose que $P$ ne divise pas ni $d$ ni $a^2 - db^2$, montrer que : $(a + b\sqrt{d}\ )^{p-1} \equiv 1 \bmod P$.

8°) Montrer que $(a,b) \in \mathbb{Z}^2$, on a (avec $n = 67.103.239$)
$(n, a^2 - 2b^2) = 1 \Rightarrow (a + \sqrt{2}\ )^{n+1} \in \mathbb{Z} \bmod n$ .

9°) Montrer qu'il n'existe pas de $d$ sans facteur carré, $d \in \mathbb{N}$, tel que $(\frac{d}{q}) = -1$ et pour tout $(ab, b) \in \mathbb{Z}^2$ avec $(n, a^2 - 2b^2) = 1$, $(a + b\sqrt{d}\ )^{n+1} \in \mathbb{Z} \bmod n$.

**Problème n° 2**

Alice veut envoyer à Bob les plans d'une machine de Turing révolutionnaire permettant de faire le produit de 2 nombres unaires . (5 s'écrit 11111).

1°) une Construire une telle machine (non necessairement révolutionnaire).

2°) Alice et Bob sont réliés par l'intermédiaire d'un central. Comment peuvent-ils être mis en relation ? Votre solution devra bien préciser les hypothèses dans les quelles vous vous placez.

3°) Alice écrit en décimal les plans de sa machine ce qui donne un nombre de 2000 digits. Comment peut-elle transmettre ce plan à Bob ? La sécurité commande d'abord qu'Alice et Bob construisent une clé non connue du central.

4°) Alice se ravise et décide de partager son plan entre 3 personnes de telle sorte qu'une personne seule ne puisse construire le plan, mais que 2 personnes réunies puissent le faire. Quel message envoie-t-elle à chacun des ses correspondants.