*Sous le co-parrainage de*

***Mr le Ministre de l'Enseignement Supérieur***
***et de la Recherche Scientifique***

***et,***

***De Mr le Ministre de la Défense***

*Sous la Présidence de*

***Mme la Présidente de l'Université Félix Houphouet BOIGNY***

Organisée par le :

Laboratoire de Mathématiques fondamentales de l'UFRMI
(Section Algèbre)

## Cérémonie d'Ouverture de la

# Journée Internationale d'Arithmétique-Abidjan 2014,

## Thème : Cryptographie et Applications

*Abidjan, le jeudi 24 juillet 2014*
*UFRMI Université Félix Houphouet BOIGNY*

**8h50 à 9h10 :** Accueil et mise en place des invités et des participants.

**9h10 à 9h20 :** Allocution du Président du Comité d'organisation : Dr. TANOE François .

**9h20 à 9h30 :** Allocution de Monsieur le Directeur du Laboratoire de Mathématiques Fondamentales : Pr. Edmond FEDIDA.

**9h30 à 9h40 :** Allocution de Monsieur le Doyen de l'UFRMI : Pr. ADJE Assohoun

**9h40 à 9h50 :** Allocution du porte parole des missionnaires visitant : Pr Alain TOGBE.

**9h50 à 10h00 :** Allocution de SEM. Salam EL CHEIKH, Invité d'Honneur, Consul Honoraire du CABO VERDE en Côte d'ivoire

**10h00 à 10h10 :** Allocution, de Madame la Présidente de l'Université Félix Houphouet Boigny : Pr. Bakayoko-Ly Ramata (ou de son représentant).

**10h10 à 10h20 :** Allocutions, suivies de l'ouverture de la **Journée Internationale d'Arithmétique-Abidjan 2014**, par le Ministre de l'Enseignement Supérieur et de la Recherche Scientifique et par le Ministre de la Défense (ou de leurs représentants).

| Cérémonie d'Ouverture de la **Journée Internationale d'Arithmétique ABIDJAN 2014**, de 8h50 à 10h20 | | | |
|---|---|---|---|
| **Horaire** | **Conférenciers – Titres** | **Résumés / Abstracts** | **Modérateurs** |
| **10h20 à 10h55** | **Introduction à la Cryptographie**<br>*Professeur Michel Waldschmidt (France)*<br>*Institut de Mathématiques de Jussieu*<br>Email : miw@math.jussieu.fr | Apres un rapide survol de l'histoire de la cryptographie, nous présenterons le crypto système RSA sous une forme très simplifiée, faisant intervenir des nombres de trois chiffres (restes de la division par 1000). Nous terminerons par quelques compléments sur les nombres premiers. | *Professeur* FEDIDA Edmond |
| **10h55 à 11h30** | **Numération et concepts mathématiques en pays Baoulés.**<br>*Kouamé Bah Saint Bénédic. Chercheur (Côte d'Ivoire)*<br>Email : bahkouame@hotmail.fr | Le projet « BAHouli » (approche scientifique du Baoulé) met en jeu deux systèmes de comptage du peuple Baoulé originaire de la Côte d'Ivoire, et qui sont:<br>1) le système de comptage ordinaire ou la numération ordinaire Baoulé qui est décimal: kun(1), nnyɔn(2), nsan(3), nnan(4), nnu(5), nsiɛn(6),nso(7), mɔcuɛ(8), nglwan(9), blu(10), blu ni kun (10 et 1 soit 11),…. Le zéro n'est pas utilisé dans la numération, mais sa notion existe, il se dit : "fi" ou "ngbɛn".<br>2) le second système est celui des devises (la monnaie) qui pourrait être liés aux comptoirs anglais du Ghana (ponu ↩ pound?), et qui après avoir évolué dans le temps, se résume aujourd'hui en 3 unités monétaires: le "bablu" dont l'unité équivaut 5F CFA, le "pɔnu" (25F) et le "kotokun"(unité de 1000F). On serait ici plutôt proche d'une base 25, ce qui expliquerait nos pièces de monnaies de 25, 50, 100, 250 500 francs et un billet de 2500 (qui n'est plus utilisé aujourd'hui). Le projet « BAHouli » a étudié également certains concepts mathématiques de base (opérations, géométrie) en langue baoulé, ainsi que des méthodologies de décompte. | *Professeur* ADOU Jérôme |
| Pause café | | | |
| **11h45 à 12h20** | **On congruent numbers and related topics**<br>*Professeur Claude Levesque (Canada)*<br>*Département de mathématiques et de statistique,*<br>*Université Laval Québec*<br>Email : Claude.Levesque@mat.ulaval.ca | A positive natural number n is called a congruent number if n is the area of a right triangle with rational sides. In other words, n is congruent if n = ab/2, with a; b; c rational numbers verifying $a^2+b^2=c^2$. It turns out that n is congruent if the elliptic curve $E : Y^2 = X^3 - n^2X$ over $\mathbb{Q}$ has at least one rational solution (x; y) with nonzero rational numbers x; y. We will give other equivalent conditions for having the property that n is a congruent number. We will also take this opportunity for introducing elliptic curves and give some of their properties. | *Docteur* TANOE François |
| **12h20 à 12h55** | **Linear secret sharing schemes and algebraic curves**<br>*Professeur Jorge Jimenez Urroz (Espagne)*<br>*Department of Applied Mathematics IV*<br>*Polytechnic University of Catalonia,Barcelona*<br>Email: jjimenez@ma4.upc.edu | A linear secret sharing scheme is a way of sharing a secret, among a set of participants with different hierarchy. We will introduce the concept, talk about the Shamir threshold scheme, and then generalize it to elliptic and hyperelliptic curves (the last part depending on time.) | *Professeur* Kangni Kinvi |
| Pause Déjeuner | | | |
| **14H30 à 15H05** | **Test de primalité et applications**<br>*Gnagne Sézare –Doctorant.*<br>*Laboratoire de Mathématiques Fondamentales*<br>*UFRMI Univesité Félix Houyphouet BOIGNY, Abidjan*<br>Email : gabesezare@ymail.com | La cryptographie qui est définie comme une habilitation à rendre une information inaccessible à une personne étrangère, est l'une des composantes de la cryptologie, dont la deuxième composante est la cryptanalyse. Cette dernière est définie comme une habilitation à une personne étrangère à prendre connaissance de l'information. Nous nous intéressons au problème de la génération sécuritaire des clés de cryptage des systèmes cryptographiques. En particulier les systèmes symétriques (substitutions mono alphabétiques et poly alphabétiques) dit (RSA, El Gamal, Diffie-Hellman). basés sur l'usage des nombres premiers dans la génération des clés. Nous terminons par l'étude de tests dits de primalités, de types classiques, tels que ceux de Lucas-Lehmer, Fermat et de Miller-Rabin. | *Professeur* Alain TOGBE |

| Horaire | Conférenciers – Titres | Résumés / Abstracts | Modérateurs |
|---|---|---|---|
| **15H05 à 15h40** | **Sur les m-tuplets Diophantiens**<br>*Professeur Alain Togbe (Etats Unis)*<br>*Purdue University North Central, USA*<br>Email : atogbe@pnc.edu | Un ensemble de m nombres entiers positifs distincts $\{a_1, \ldots, a_m\}$ est appelé un m-tuplet diophantien si $a_i \times a_j + 1$ est un carré parfait pour tout i; j; i ≠ j. En général, soit n un nombre entier, un ensemble de m nombres entiers positifs $\{a_1, \ldots, a_m\}$ est appelé un m-tuplet diophantien avec la propriété D(n) ou un D(n)-m-tuplet si $a_i \times a_j + n$ est un carré parfait pour tout i; j; i ≠ j. Diophante étudié des ensembles de nombres rationnels positifs avec la même propriété; notamment il a trouvé l'ensemble des quatre nombres rationnels positifs : $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. Cependant, le premier quadruplet diophantien à été trouvé par Fermat: { 3; 8; 120}. De plus, Baker et Davenport ont prouvé que { 3; 8; 120} ne peut pas être étendu à un quintuplet diophantien. Le problème d'extension de $P_n$-ensembles est d'un grand intérêt. Dans cet exposé, nous allons donner un aperçu très rapide de quelques résultats obtenus. Ensuite, nous allons discuter des conjectures sur les m-tuplets diophantiens et les progrès récents pour les résoudre. | *Professeur* ADJE Assohoun |
| **15h40 à 16h15** | **Introduction to Elliptic Cryptosystems**<br>*Professeur Francesco Pappalardi (Italie)*<br>*Dipartimento di Matematica e Fisica*<br>*Università degli Studi Roma*<br>Email: pappa@mat.uniroma3.it | Nous allons introduire la notion de groupe de points rationnels d'une courbe elliptique définie sur un corps fini et nous allons passer en revue leurs propriétés de base. Nous allons aussi classifier toutes les courbes elliptiques possibles sur les corps de 2 et de 3 éléments. Ensuite, nous allons illustrer les problèmes algorithmiques fondamentaux en rapport avec la théorie et des solutions possibles. Nous allons terminer avec d'autres exemples et records liées aux courbes elliptiques. | *Professeur* KOUAKOU Mathias |
| Pause café | | | |
| **16h30 à 17h05** | **Integer's basis for Triquadratic Fields and monogenecity's problem**<br>*KOUAKOU Vincent – Doctorant (Côte d'Ivoire)*<br>*Laboratoire de Mathématiques Fondamentales*<br>*UFRMI Univesité Félix Houyphouet BOIGNY, Abidjan*<br>Email : kouakouassivincent@gmail.com | Let $K_n = \mathbb{Q}(\alpha_{2^0}, \alpha_{2^1}, \ldots, \alpha_{2^{n-1}})$ be the compositum of the n quadratic fields: $(\mathbb{Q}(\alpha_{2^k}))_{0 \le k \le n-1}$ : $K_n$ is so called n-quadratic number field: In our work we study the monogenecity problem for for $K_3 = \mathbb{Q}(\sqrt{dm}, \sqrt{dn}, \sqrt{d'm'n'\ell})$ ; That is the integers 'base of the integers' ring $\mathbb{Z}_{K_3}$ of $K_3$ is of the type { 1, 1, $\theta^1, \theta^1 \ldots, \theta^7$ } for some $\theta \in \mathbb{Z}_{K_3}$ . Using D. CHATELAIN.s methods, we give an integers basis of $\mathbb{Z}_{K_3}$ in the following complete cases:( $dm, dn, d'm'n'\ell$) ≡ (1; 1; 1) ; (1; 1; 2) ; (1; 1; 3) and (1; 2; 3) mod4, with : ( $dm, dn$) = $d$; ( $dmn, \ell$) = 1; ( $dm, d'm'n'$) = $d'm'$ and ( $dn, d'm'n'$) = $d'n'$. From those basis we are able, by only Diophantine approach, to set, in all cases, the monogenecity equation: $\theta \in \mathbb{Z}_{K_3}$ and $\Delta(\theta) = \prod_{i \neq j}((\sigma_i(\theta) - \sigma_j(\theta))^2 = D_{K_3/\mathbb{Q}}$ ,where $\sigma_i \in$ Gal ($K_3/\mathbb{Q}$) and $D_{K_3/\mathbb{Q}}$ is the discriminant of $K_3$over $\mathbb{Q}$ | *Professeur* NINDJIN Fulgence |
| **17h05 à 17h40** | **Cubic Resolvent and criterions of Monogenesis in Biquadratic Fields**<br>*Dr TANOE François (Côte d'Ivoire)*<br>*Laboratoire de Mathématiques Fondamentales*<br>*UFRMI Univesité Félix Houyphouet BOIGNY, Abidjan*<br>Email : aziz_marie@yahoo.fr | A biquadratic fields K = $\mathbb{Q}(\sqrt{dm}, \sqrt{dn})$ is said to be monogenic i.e. that $\mathbb{Z}_K = <1, 1, \theta_1, \theta_2, \theta_3>$ as a free $\mathbb{Z}$-module of rank 4, if and only if, the Diophantine equation: $(u^2 + v^2)2^{-\delta}d - u^2v^2 2^{\delta}m = s$, (where s = ±1 and $\delta$ = 0 or 1) . In this paper we demonstrate necessary and sufficient conditions of monogenesis, among which the following one: K is monogenic of parameters (u, v), if and only if ∃ a primitive element $\alpha$ of K with irreducible polynomial: $X^4 + pX^2 + qX + r$, such that its ps-cubic resolvent: $X^3 + 2pX^2 + (p^2 - 4r)X - q^2$ , admit 3 integers non square roots, of the type: $\theta_1 = (u^2 + v^2)^2 dm$ , $\theta_2 = (u^2 - v^2)^2 dn$ , $\theta_3 = (2^{\delta}uv)^2 mn$, and such that: discr(R($\alpha$,X)) = $\frac{2^{2+\delta}}{(2^{\delta}uv)(u^2 \mp)(u^2 - v^2)} \theta_1 \theta_2 \theta_3$. (We'll distinguish the case: (u, v) ≠ (±1,_ ±1); (±1, 0); (0, ±1); $u \wedge v = 1$, and its converse). | *Professeur* Claude LEVESQUE |
| Cérémonie de Clôture de la **Journée Internationale d'Arithmétique - ABIDJAN 2014**, de 17h40 à 18h50 | | | |