Mathematical Tour of West Africa

Alain Togbe

July 19 – 25, 2014

1 Introduction

1. Jorge Jimenez Urroz (Universitat Polytecnica de Catalunia, Barcelona, España)
2. Claude Levesque (Université Laval à Québec, Canada)
3. Francesco Pappalardi (Università Roma Tre, Italia)
4. Adriana Salerno (Lewiston, USA)
5. Alain Togbe (Westville, USA)
6. Michel Waldschmidt (Université Pierre et Marie Curie, Paris, France)

2 Program – Lomé - 2014 (July 21, 2014)

1. Professeur Michel Waldschmidt (Paris, France)

   Titre: *La constante d'Euler est-elle un nombre rationnel, un nombre algébrique irrationnel ou bien un nombre transcendant?*

   Résumé: *Déterminer la nature arithmétique de constantes de l'analyse est le plus souvent un problème difficile, très fréquemment on ne connait pas la réponse - c'est le cas pour la constante d'Euler. Néanmoins, on connaît un certain nombre de propriétés de cette constante qui vaut approximativement*

   $$0,577215664901532860606512090082402431042 1.$$

   Nous en décrirons quelques unes.

2. Professeur Francesco Pappalardi (Rome, Italie)

   Titre: *Propriétés des réductions de groupes de nombres rationnels*

   Résumé: *Soit Γ un sous-groupe multiplicatif de $\mathbb{Q}^*$ et soit p un nombre premier pour lequel la valuation $v_p(x) = 0$, pour tout x dans G. Alors le groupe $\Gamma_p = \{x(\mathrm{mod}p) : x \in \Gamma\}$ est un bien-défini sous-groupe de $\mathbb{F}_p^*$. Nous allons examiner les différentes propriétés de Γ_p lorsque p varie et nous proposons divers résultats nouveaux dans analogie avec l'ancienne conjecture de Artin pour les racines primitives.*

   Title: *Properties of reductions of groups of rational numbers*

   Abstract: *Let Γ be a multiplicative subgroup of $\mathbb{Q}^*$ and let p be a prime number for which the valuation $v_p(x) = 0$ for every $x \in \Gamma$. Then the group $\Gamma_p = \{x(\mathrm{mod}p) : x \in \Gamma\}$ is a well–defined subgroup of $\mathbb{F}_p^*$. We will consider various properties of Γ_p as p varies and we will propose various new results in analogy with the old Artin Conjecture for Primitive roots.*

3. Professeur Alain Togbe (Westville, USA)

   Titre: *The P-integer conjecture of Pomerance.*

   Abstract: Let $k > 1$ be an integer. Moreover, let $\varphi(k)$ denote Euler's totient function and $\omega(k)$ the number of distinct prime divisors of k. An integer k is a P-integer if the first $\varphi(k)$ primes coprime to k form a reduced residue system modulo k. In 1980, Pomerance proved the finiteness of the set of P-integers. Moreover, he proposed the following conjecture. Conjecture: If k is a P-integer, then $k \leq 30$. In this talk, we will discuss

the proof of this conjecture. Titre : La conjecture de P-entier de Pomerance. Résumé: Soit $k > 1$ un entier. En outre, soit $\varphi(k)$ la fonction indicatrice d'Euler et $\omega(k)$ le nombre de diviseurs premiers distincts de k. Un entier k est un P-entier si les premiers $\varphi(k)$ entiers relativement premiers entre eux pour k forment un système réduit de résidus modulo k. En 1980, Pomerance a prouvé la finitude de l'ensemble des P-entiers. En outre, il a proposé la conjecture suivante. Conjecture: Si k est un P-entier, alors $k \leq 30$. Dans cet exposé, nous allons discuter du progrès jusqu'à la preuve de cette conjecture.

4. Claude Levesque (Québec, Canada)

Title: *Congruent numbers and related topics*

Abstract: *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*

$$E : Y^2 = X^3 - n^2 X$$

over $\mathbb{Q}$ has at least one rational solution (x, y) with nonzero rational numbers x, y. We will give other equivalent conditions for n to be a congruent number. We will also take this opportunity for introducing elliptic curves and give some of their properties.

Titre: *Sur les nombres congruents et sujets connexes.*

Résumé: *Un nombre entier positif n est dit un nombre congruent si n est l'aire d'un triangle droit avec des côtés rationnels. En d'autres mots, n est congruent si $n = ab/2$, où a, b, c sont des nombres rationnels vérifiant $a^2 + b^2 = c^2$. Il s'avère que n est un nombre congruent si la courbe elliptique sur $\mathbb{Q}$ définie par*

$$E : Y^2 = X^3 - n^2 X$$

possède au moins une solution (x, y) avec des nombres rationnels x, y non nuls. Nous donnerons d'autres conditions équivalentes pour que n soit un nombre congruent. Nous profiterons de l'occasion pour introduire les courbes elliptiques et mentionner certaines de leurs propriétés.

5. Jorge Jimenez Urroz (Barcelone, Espagne)

Title: *Malleability and the factorization of RSA numbers*

Abstract: *Given a number n product of two unknown primes, is it easier to factorize if we allow the attacket to factorize another number (coprime to n) at his will?*

6. Adriana Salerno (Lewiston, USA)

Title: *Effective computations in arithmetic mirror symmetry*

Abstract: *In this talk, I will talk about computational approaches to the problem of arithmetic mirror symmetry. One of the biggest questions facing string theorists is the one of mirror symmetry. In arithmetic mirror symmetry, we approach the conjecture from a number theoretic point of view, namely by computing Zeta functions of mirror pairs. I will define all of these terms and then explain our work through a couple of examples of families of $K3$ surfaces. This is joint work with Xenia de la Ossa, Charles Doran, Tyler Kelly, Stephen Sperber, and Ursula Whitcher.*

3 Program – Abidjan - 2014 (July 24, 2014)

1. Professeur Michel Waldschmidt (Paris, France)

Titre: *Introduction à la cryptographie*

Résumé: *Après un rapide survol de l'histoire de la cryptographie, nous présenterons le cryptosystème RSA sous une forme très simplifiée, faisant intervenir de nombres de trois chiffres (restes de la division par 1000). Nous terminerons par quelques compléments sur les nombres premiers.*

2. Professeur Francesco Pappalardi (Rome, Italie)

Title: *Introduction to Elliptic Cryptosystems*

Abstract: *We will introduce the notion of group of rational points of an elliptic curve defined over a finite field and we will review all the basic properties that they satisfy. We will also classify all the possible elliptic curves over the fields with 2 and 3 elements. Then we will illustrate the fundamental algorithmic problems related with the Theory and possible solutions. We will conclude with some more examples and records related to elliptic curves.*

Titre: *Introduction aux systèmes Cryptoelliptiques*

Résumé: *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 toutes les propriétés de base qu'ils satisfont. Nous allons aussi classifier toutes les possibles courbes elliptiques 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 liés aux courbes elliptiques.*

3. Professeur Alain Togbe (Westville, USA)

Title: *On Diophantine m–tuples*

Abstract: *A set of m distinct positive integers $\{a_1, \ldots, a_m\}$ is called a Diophantine m-tuple if $a_i a_j + 1$ is a perfect square. In general, let n be an integer, a set of m positive integers $\{a_1, \ldots, a_m\}$ is called a Diophantine m-tuple with the property $D(n)$ or a $D(n)$-m-tuple (or a P_n-set of size m), if $a_i a_j + n$ is a perfect square. Diophantus studied sets of positive rational numbers with the same property, particularly he found the set of four positive rational numbers $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$. But the first Diophantine quadruple was found by Fermat. That is the set $\{1, 3, 8, 120\}$. Moreover, Baker and Davenport proved that the set $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. The problem of extendibility of P_n-sets is of a big interest. In this talk, we will give a very quick survey of results obtained. Finally, we will discuss the conjectures on Diophantine m-tuples and the recent progress to solve them.*

Titre: *Sur les m–tuplets diophantiens*

Résumé: *Un ensemble de m les nombres entiers positif distincts $\{a_1, \ldots, a_m\}$ est appelé un m-tuplet diophantien si $a_i a_j + 1$ est un carré parfait. 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 $a_i a_j + n$ est un carré parfait. Diophantus a étudié des ensembles de nombres rationnels positifs avec la même propriété, notamment il a trouvé l'ensemble de quatre nombres rationnel positif $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$. Mais le premier quadruplet diophantien a été trouvé par Fermat. Cela est l'ensemble $\{1, 3, 8, 120\}$. De plus, Baker et Davenport ont prouvé que l'ensemble $\{1, 3, 8, 120\}$ 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 quelques résultats obtenus. Enfin, nous allons discuter des conjectures sur m–tuplets diophantiens et les progrès récents pour les résoudre.*

4. Claude Levesque (Québec, Canada)

Title: *Congruent numbers and related topics*

Abstract: *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*

$$E : Y^2 = X^3 - n^2 X$$

over $\mathbb{Q}$ has at least one rational solution (x, y) with nonzero rational numbers x, y. We will give other equivalent conditions for n to be a congruent number. We will also take this opportunity for introducing elliptic curves and give some of their properties.

Titre: *Sur les nombres congruents et sujets connexes.*

Résumé: *Un nombre entier positif n est dit un nombre congruent si n est l'aire d'un triangle droit avec des côtés rationnels. En d'autres mots, n est congruent si $n = ab/2$, où a, b, c sont des nombres rationnels vérifiant $a^2 + b^2 = c^2$. Il s'avère que n est un nombre congruent si la courbe elliptique sur $\mathbb{Q}$ définie par*

$$E : Y^2 = X^3 - n^2 X$$

possède au moins une solution (x, y) avec des nombres rationnels x, y non nuls. Nous donnerons d'autres conditions équivalentes pour que n soit un nombre congruent. Nous profiterons de l'occasion pour introduire les courbes elliptiques et mentionner certaines de leurs propriétés.

5. Jorge Jimenez Urroz (Barcelone, Espagne)

Title: *Linear secret sharing schemes and algebraic curves*

Abstract: *A linear secret sharing scheme is a way of sharing a secret amount 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.)*