Book of Abstracts
XXV Brazilian Algebra Meeting

State University Campinas, December 3 - 7, 2018

Session: Number Theory

Room L003, Anexo 2 - IMECC

	December 3rd	**December 4th**	**December 5th**
14h00 - 14h50:	Godinho	Lelis	Santos
15h00 - 15h50:	Ribas	Miranda	Silva
16h00 - 16h30:	Coffee Break	Coffee Break	Coffee Break
16h30 - 17h20:	Chaves	Dmitry	Masuda
17h30 - 18h00:	Carvalho	Silva	Veras

Zero-sum sequences on some finite abelian groups

Lucimeire Carvalho (Instituto Federal de Goiás - Brazil)

Abstract:
Let G be a finite abelian group. The Erdos-Ginzburg-Ziv constant $s(G)$ of G is defined as the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S|$ has a zero-sum subsequence T of length $|T| = exp(G)$. In this work we present some results about the EGZ constant in some finite abelian groups.

Exponential Diophantine Equations and Linear Recurrence Sequences

Ana Paula Chaves (Universidade Federal de Goiás - Brazil)

Abstract:
Let $(F_n)_{n\geq 0}$ be the famous Fibonacci sequence, given by $F_{n+2} = F_{n+1} + F_n$, for $n \geq 0$, where $F_0 = 0$ and $F_1 = 1$ are given. There are several interesting identities involving this sequence such as $F_n^2 + F_{n+1}^2 = F_{2n+1}$, for all $n \geq 0$. In a paper of 2011, Luca and Oyono proved that if $F_n^s + F_{n+1}^s$ is a Fibonacci number for $n \geq 3$, then $s = 1$ or 2. In this presentation, we are going to explore the most recent generalizations of Luca and Oyono's result, in particular, that if $(G_m)_m$ is a linear recurrence sequence (under weak assumptions) and $G_n^s + \cdots + G_{n+k}^s \in (G_m)_m$, for infinitely many positive integers n, then s is bounded by an effectively computable constant depending only on k and the parameters of G_m, and also if $(F_m^{(k)})_m$ is the k-generalized Fibonacci sequence, then $(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(k)}$ holds only for trivial cases.

Anderson t-motives: analogs of abelian varieties in finite characteristics

Logachev Dmitry (Universidade Federal do Amazonas - Brazil)

Abstract:
Anderson t-motives are modules over some non-commutative rings. It turns out that their properties are similar to the properties of abelian varieties, more exactly, of abelian varieties with multiplication by imaginary quadratic fields. There are analogs of Tate modules, lattices etc. for them, and their moduli spaces are analogs of Shimura varieties. Nevertheless, this analogy is far to be complete. For example, we do not know whether there exists or not a 1 -1 correspondence between Anderson t-motives and lattices, except some simple cases. The lecture will contain a survey of the theory and some recent results.

Further, it turns out that these varieties are related to a problem of finding of the analytic rank of twists of Carlitz modules (the simplest types of Drinfeld modules), i.e. the order of 0 of their L-function at some point. Generalization of this theory to the case of other Drinfeld modules is a subject of future research.

On Norton's Conjecture

Hemar Godinho (Universidade de Brasilia - Brazil)

Abstract:
The conjecture of Norton is related to the minimum number of variables to ensure p-adic solutions for diagonal forms. In this talk we are going to present examples and counter-

examples for this conjecture.

On a problem of Erdos and Mahler concerning continued fractions

Jean Lelis (Universidade de Brasília - Brazil)

Abstract:
In 1939, Erdos and Mahler, Some arithmetical properties of the convergents of a continued fraction, J. Lond. Math. Soc. 1939, studied some arithmetical properties of the convergents of a continued fraction. In particular, they raised a conjecture related to continued fractions and Liouville numbers. In this paper, we shall apply the theory of linear forms in logarithms to obtain a result in the direction of this problem.

Maximal entries of elements in certain matrix monoids

Ariane Masuda (New York City College of Technology, CUNY- USA)

Abstract:
Let $L_u = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$ and $R_v = \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix}$ be matrices in $SL_2(\mathbb{Z})$ with $u, v \geq 1$. Since the monoid generated by L_u and R_v is free, we can associate a depth to each element based on its product representation. We consider the problem of finding a depth n matrix containing the maximal entry for each $n \geq 1$. Bromberg, Shpilrain, and Vdovina solved this problem when $u = v = 2$ and $u = v = 3$. In this talk we discuss how we extended their results for any $u, v \geq 1$, and in the process we recovered the Fibonacci and some Lucas sequences. This is joint work with Sandie Han, Satyanand Singh, and Johann Thiel.

Uma abordagem multiplicativa para partições de inteiros

José Plinio Santos (Universidade Estadual de Campinas - Brazil)

Abstract:
In this work we define a new set of integer partition, based on a lattice path in $\mathbb{Z}_2$ connecting the line $x + y = n$ to the origin, which is determined by the two-line matrix representation given for different sets of partitions of n. The new partitions have only distinct odd parts with some particular restrictions. This process of getting new partitions, which has been called the Path Procedure, is applied to unrestricted partitions, partitions counted by the 1st and 2nd Rogers-Ramanujan Identities, and those generated by the Mock Theta Function $T_1(q)$.

On Davenport constant in some non-abelian groups and their inverse problems

Sávio Ribas (IFMG - Campus Ouro Preto - Brazil)

Abstract:
Let G be a finite group written multiplicatively. The small Davenport constant of G is the smallest positive integer $d(G)$ such that every sequence of G with $d(G)$ elements has a non-empty subsequence with product 1 in some order. During the talk, we will present the small Davenport constant of some non-abelian groups g and the explicit characterizations of all sequences S of G such that $|S| = d(G) - 1$ and S is free of product-1 subsequences (these kind of characterizations are called "inverse problems"). We will also relate some inverse problems with Davenport constants with weights.

This is a joint work with Fabio Brochero Martinez.

Sobre Funções Inteiras Transcendentes que Levam Racionais em Racionais

Elaine Silva (Universidade de Brasília - Brazil)

Abstract:
Em 1844, Liouville exibiu os primeiros exemplos de números transcendentes, hoje conhecidos como números de Liouville. Em 1906, Maillet provou que a imagem de um número de Liouville por uma função racional (com coeficientes racionais) não constante é um número de Liouville. Em 1984, Mahler perguntou sobre a existência de funções inteiras transcendentes com essa propriedade. Em 2014, Marques e Moreira, apresentaram um resultado que implica uma resposta afirmativa à essa questão, desde que existam funções inteiras transcendentes, tais que $f(\mathbb{Q}) \subseteq \mathbb{Q}$ e $\text{den}\,(f\,(p/q)) \leq F(q)$, para algum polinômio $F(z) \in \mathbb{Z}[z]$ fixado e para todo q suficientemente grande. A existência desse tipo de função ainda é um problema em aberto. Nesta palestra, mostraremos que não existem funções desse tipo com coeficientes racionais (em sua série de potências) e $\text{den}\,(f\,(p/q))$ polinomial em q, para todo q suficientemente grande. Esse resultado foi provado em parceria com Marques.

Congruences related to an eighth order mock theta function of Gordon and McIntosh

Robson da Silva (Universidade Federal de São Paulo - Brazil)

Abstract:
In this talk, we will discuss arithmetic properties of a partition function related to an

eighth order mock theta function of Gordon and McIntosh. Via elementary generating function manipulations, a complete characterization of the parity of this function is presented, from which infinitely many Ramanujan-like congruences modulo 2 are obtained. In addition, many congruences modulo certain numbers of the form $2^\alpha 3^\beta 5$ are presented.

This is a joint work with E. H. M. Brietzke and J. A. Sellers.

Solubility of additive form of degree 10

Daiane Veras (Universidade de Brasília - Brazil)

Abstract:
For $k \in \mathbb{N}$ and p a prime number, define $\Gamma^*(k,p)$ to be the smallest positive integer $n \in \mathbb{N}$ such that any diagonal form $f(x_1,\ldots,x_s) = a_1x_1^k + \cdots + a_sx_s^k$, with integer coefficients, has a nontrivial zero over $\mathbb{Q}_p$ whenever $s \geq n$. Define also

$$\Gamma^*(k) = \max_{p\ prime} \Gamma^*(k,p).$$

In 1963, Davenport and Lewis proved that $\Gamma^*(k) \leq k^2+1$ and $\Gamma^*(p-1,p) = k^2+1$. For specific values of k and the prime p, if $k \neq p-1$, then the number $\Gamma^*(k,p)$ may be less than k^2+1. In fact, in 1966 Dodson published an improved bound, that $\Gamma^*(k) \leq \frac{49}{64}k^2+1$ if $k+1$ is composite.

For specific values of k, a number of exact values of $\Gamma^*(k)$ have been computed. Lewis showed that $\Gamma^*(3) = 7$. The combined work of Gray and Chowla together shows that $\Gamma^*(5) = 16$. Bierstedt appears to have been the first to show that $\Gamma^*(7) = 22$ and $\Gamma^*(11) = 45$. These values were independently discovered by Norton, who also gave the value $\Gamma^*(9) = 37$. The values of $\Gamma^*(7)$ and $\Gamma^*(9)$ were also discovered independently by Dodson. Bovey showed that $\Gamma^*(8) = 39$, and recently Knapp has determined the exact values of $\Gamma^*(k)$ for all remaining $k \leq 32$ with $k \neq p-1$. In unpublished work, some undergraduate students of Knapp have pushed this bound to $k \leq 39$, and have also found the value of $\Gamma^*(45)$.

Most of these results were obtained by fixing the prime p and finding an upper bound for $\Gamma^*(k,p)$, by the relation above. Even in case where $k+1 = p$ is prime, the bound k^2+1 is obtained showing a diagonal form of degree k in k^2 variables with integers coefficients that does not have a nontrivial zero in the p-adic fields, for these specific p, and showing that $\Gamma^*(k,q) \leq \Gamma^*(k,p)$ for all prime $q \neq p$, but the exact values of the $\Gamma^*(k,q)$ is unknown.

Most of these results were obtained by choosing a specific prime p, finding the exact value of $\Gamma^*(k,p)$, and then showing that $\Gamma^*(k,q) \leq \Gamma^*(k,p)$ for all primes $q \neq p$. Then this shows that $\Gamma^*(k) = \Gamma^*(k,p)$. When this method is used, the exact values of the $\Gamma^*(k,q)$ are unknown.

Consider an additive form of degree 10. Is well known that $\Gamma^*(10) = \Gamma^*(10,11) = 101$. In this talk we show the exact values of $\Gamma^*(10,p)$ for all $p \neq 11$. Let

$$\mathcal{P} = \{41, 61, 71, 101, 131, 151, 181, 191, 211, 251, 271, 281, 311, 331, 431, 491, 911\}.$$

So, we get:

$\Gamma^*(10,p) = 23$ and 41, if $p = 2$, and 31, respectively ;

$\Gamma^*(10,p) = 31$, if $p \in \mathcal{P}$;

$\Gamma^*(10,p) = 21$, for $p = 5$ and the other primes.

This results were obtained with the collaboration of the Professor Paulo Henrique Rodrigues from UFG.

Posters Number Theory

Construções de reticulados algébricos via corpos de números de grau primo

Antonio Aparecido de Andrade (São Paulo State University at São José do Rio Preto ? Brazil)

Abstract:

Um corpo de números $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, ou seja, o corpo $\mathbb{K}$ pode ser visto como um espaço vetorial de dimensão finita sobre $\mathbb{Q}$. Um corpo de números é chamado abeliano (cíclico) se seu grupo de Galois é abeliano (cíclico). Pelo Teorema de Kronecker-Weber, segue que existe um inteiro positivo $n \in \mathbb{N}$ tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima da unidade. Deste modo, existe um inteiro positivo n mínimo, chamado condutor, que satisfaça tal condição. Assim, o estudo de corpos abelianos é equivalente ao estudo de subcorpos de corpos abelianos. Neste trabalho trabalhamos com corpo de números de grau um número primo p e analisamos os possíveis condutores.

Consideramos $\mathbb{K}$ um corpo de números abeliano de grau p, com p um primo ímpar. Neste caso, $\mathbb{K}$ é um corpo de números totalmente real e $\mathbb{Q} \subseteq \mathbb{K}$ é uma extensão cíclica, uma vez que p é um primo ímpar. Além disso, os possíveis condutores do corpo $\mathbb{K}$ são da forma $\prod_{i=1}^{s} p_i$ ou $p^2 \prod_{i=1}^{s} p_i$, onde p_i é um primo e $p_i \equiv 1(mod\ p)$ para $i = 1, 2, \cdots, s$, e assim, consideramos $\mathbb{L} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. Explicitamos o elemento primitivo e uma base integral de uma extensão abeliana de grau p e condutor n, e além disso, construímos também reticulados algébricos sobre essas extensões abelianas. Veremos que se n é o condutor de $\mathbb{K}$, onde $n = \prod_{i=1}^{s} p_i$ ou $n = p^2 \prod_{i=1}^{s} p_i$, com $p_i \equiv 1(mod\ p)$ para $i = 1, 2, \cdots, s$, então $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = Tr_{\mathbb{L}:\mathbb{K}}(\zeta_n)$, e mostramos quantas extensões Galoisianas de grau p possuem condutor n. Além disso, apresentamos a caracterização do anel de inteiros algébricos do corpo $\mathbb{K}$. Finalmente, explicitamos a forma traço integral $Tr_{\mathbb{L}:\mathbb{K}}(x^2)$, onde $x \in \mathcal{O}_{\mathbb{K}}$ e obtemos algumas de suas propriedades, entre as quais determinamos o mínimo não nulo assumido em uma classe de $\mathbb{Z}$-módulos do anel de inteiros algébricos $\mathbb{O}_{\mathbb{K}}$ e apresentamos exemplos de reticulados algébricos obtidos através do homomorfismo canônico com densidade de centro ótima via esses corpos.

O Teorema de Mordell

Jaime Edmundo Apaza Rodriguez (Unesp-Ilha Solteiro- Brazil)

Abstract:
Neste trabalho apresentamos uma discussão sobre um clássico resultado da Teoria das Curvas Elípticas, o Teorema de Mordell-Weil. Este resultado foi provado por Mordell, em 1922, para curvas elípticas sobre $\mathbb{Q}$ e foi generalizado por Weil em 1928. Nesse trabalho, Weil mostrou que o resultado vale, não apenas para curvas elípticas sobre corpos de números (isto é, extensões finitas do corpo $\mathbb{Q}$), senão também para variedades abelianas (estruturas análogas, de dimensões superiores, às curvas elípticas).

On congruences involving some Fibonomial coefficients

Gersica Freitas (Universidade Federal Rural de Pernanbuco - Brazil)

Abstract:
On congruences involving some Fibonomial coefficients

Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence. For $1 \leq k \leq m$, the Fibonomial coefficient is defined as $\binom{m}{k} = \frac{F_{m-k+1}\cdots F_{m-1}F_m}{F_1\cdots F_k}$. In 2013, Marques, Sellers and Trojovsky proved that if p is a prime number such that $p \equiv \pm 1 \pmod 5$, then $\binom{p \nmid p^{a+1}}{p^a}$ for all integers $a \geq 1$. In this paper, we study some congruences involving $\binom{p^{a+1}}{p^a}$. In particular, we improve the previous result by proving that if $p \equiv \pm 1 \pmod 5$, then $\binom{p^{a+1}}{p^a} \equiv 1 \pmod p$, for all $a \geq 0$.

On the sum of the powers of consecutive k-Bonacci numbers which are 1-Bonacci numbers

Alessandra Kreutz (Universidade de Brasília - Brazil)

Abstract:
Let $(F_n)n \geq 0$ be the Fibonacci sequence given by $F_{m+2} = F_{m+1} + F_m, form \geq 0$, where $F_0 = 0$ and $F_1 = 1$. A well-known generalization of the Fibonacci sequence is the k-generalized Fibonacci sequence $(F^(k)_n)_n$ which is dened by the initial values $0; 0; ...; 0; 1$ (k terms) and such that each term afterwards is the sum of the k preceding terms. In 2014, Chaves and Marques solved the Diophantine equation $(F^(k)_n)^2 + (F^(k)_{n+1})^2 = F^(k)_m$, in integers $m; n$ and $k \geq 2$. In 2018, Freitas and Marques generalized this result by proving that the Diophantine equation $(F^(k)_n)^2 + (F^(k)_{n+1})^2 = F^(l)_m$ has no solution in positive integers $n; m; k$ and l with $2 \leq k < landn > 1$. We intend generalize this equation showing that $(F^(k)_n)^s + (F^(k)_{n+1})^s = F^(l)_m$ has no solution in positive integers $n; m; k$ and l with $2 \leq k < l, n > 1$ and $s > 2$.