成都国际数论研讨会
报告题目与摘要

(2022年12月10日至12日，成都)

1. 欧拉猜想及其变种

蔡天新
浙江大学
Email: txcai@zju.edu.cn

Abstract

历史上有些猜想被推翻后，仍在发挥积极作用，例如17世纪的费马素数猜想、18世纪的欧拉猜想。本报告首先回顾欧拉猜想的历史和现状，然后介绍欧拉猜想的一个变种，利用椭圆曲线理论，得到若干解的结论，特别地，我们给出费马大定理$n = 3$时一个新的简洁证明，并提出若干新问题和新猜想。

2. Identities in prime number theory and their applications

蔡迎春
同济大学
Email: yingchuncai@tongji.edu.cn

Abstract

In this talk, I will give a survey of the arithmetic identities such as Vaughan's identity, Heath-Brown's identity, Linnik's identity and so on, and their applications in prime number theory.

3. Divisibility on point counting over finite Witt rings

曹炜
闽南师范大学
Email: caow2286@mnnu.edu.cn

Abstract

Let F_q denote the finite field of q elements with characteristic p. Let Z_q denote the unramified extension of the p-adic integers Z_p with residue field F_q. In a joint work with Prof. Daqing Wan, we study the q-divisibility for the number of solutions of a polynomial system in n variables over the finite Witt ring $Z_q/p^m Z_q$, where the n variables of the polynomials are restricted to run through a combinatorial box lifting F_q^n. We prove a q-divisibility theorem for any box of low algebraic complexity, including the simplest Teichmuller box. This extends the classical Ax-Katz theorem over finite field F_q (the case $m = 1$). Taking $q = p$ to be a prime, our result extends and improves a recent combinatorial theorem of Grynkiewicz. Our different approach is based on the addition operation of Witt vectors and is conceptually much more transparent.

4. Well lacunary series and modular forms of weight one

陈士超
河南大学
Email: schen@henu.edu.cn

Abstract

A series $\sum a(n)q^n$ is lacunary if the set of n for which $a(n) = 0$ has density 1. A well-known theorem of Deligne and Serre states that each modular form of weight one is lacunary. We say a q-series $f = \sum a(n)q^n$ is *well lacunary* if f is lacunary and $a(n)$ assume every integer value infinitely often. In this talk, we shall construct a family of well lacunary series via Hecke eigenform of weight one and binary quadratic forms.

5. 素数与指数型整数列中数之和

陈永高
南京师范大学
Email: ygchen@njnu.edu.cn

Abstract

1849年, de Polignac 猜想每个大于3的奇数均可表示为一个素数与一个2的方幂之和, 不久就发现了反例. 1934年, Romanoff 证明: 有正比例的奇数可表示为一个素数与一个2的方幂之和. 1950 年, van der Corput证明: 有正比例的奇数不可表示为一个素数与一个2的方幂之和. 同年, Erdos 借助同余覆盖系证明: 存在一个由正奇数构成的算术级数, 其中每一项都不可表示为一个素数与一个2的方幂之和. 这引起了一系列后续的研究. 2010年, Lee 证明了有正比例的正整数可表示为一个素数与一个斐波那契数之和. 我们将介绍相关进展. 特别地, 我和王瑞靖最近证明了: 有正比例的正整数可表示为一个素数与一个斐波那契数之和, 并且表法数唯一.

6. Exponential sums on reductive groups

扶磊
清华大学
Email: leifu@mail.tsinghua.edu.cn

Abstract

We introduce exponential sums on reductive groups and sketch the l-adic approch for estimating such sums.

7. On Erdős-Ginzburg-Ziv constant

高维东
天津大学
Email: wdgao1963@aliyun.com

Abstract

In 1961, Erdős, Ginzburg and Ziv proved the following well known result: any multiset of $2n-1$ integers has a subset of cardinality n the sum of whose elements is a multiple of n, which is known as Erdős-Ginzburg-Ziv theorem and has attracted a lot of attention. In this talk, we will present some results and open problems related to this theorem.

8. Least zero of a cubic form

李红泽
上海交通大学
Email: lihz@sjtu.edu.cn

Abstract

An effective search bound is established for the least non-trivial integer zero of an arbitrary cubic form $C \in \mathbb{Z}[X_1, \ldots, X_n]$, provided that $n \geq 14$.

9. Factorizations of polynomials over finite fields and applications

李吉有
上海交通大学
Email: lijiyou@sjtu.edu.cn

Abstract

In this talk, we introduce the basic and advanced problems of factorization of polynomials over finite fields, which arise naturally from coding theory and graph theory. In particular, we present results on the distribution of polynomials with a given number of distinct linear factors in arithmetic progressions for a large range of parameters.

10. Irreducible components of eigencurves

刘若川
北京大学
Email: liuruochuan@bicmr.pku.edu.cn

Abstract

In this talk we will show that the irreducible components of eigencurves are always finite, a corollary of the recent joint work with Nha Xuan Trong, Xiao Liang, Zhao Bin on the ghost conjecture of modular forms.

11. Complete solutions of the simultaneous Pell equations $x^2 - (a^2 - 2)y^2 = 2$ and $x^2 - bz^2 = 1$

罗家贵
西华师范大学
Email: luojg62@aliyun.com

Abstract

In this paper, we consider the simultaneous Pell' equations $x^2-(a^2-2)y^2=2$ and $x^2-bz^2=1$ where a is a positive integer and $b>1$ is squarefree and has at most three prime divisors. We obtain the necessary and sufficient conditions that the above simultaneous Pell equations have positive integer solutions by using only the elementary methods of factorization, congruence, the quadratic residue and fundamental properties of Lucas sequence and the associated Lucas sequence. Moreover, we prove that these simultaneous Pell equations have at most one solution in positive integers. When a solution exists, assuming the positive solutions of the Pell equation $x^2-(a^2-2)y^2=2$ are $x=x_m$ and $y=y_m$ with $m\geq 1$ odd, then the only solution of the system is given by $m=3$ or $m=5$ or $m=7$.

12. Averaged forms of two conjectures of Erdős and Pomerance

吕广世
山东大学
Email: gslv@sdu.edu.cn

Abstract

In this talk, we will introduce our recent progress on two conjectures of Erdős and Pomerance concerning shifted prime numbers and shifted friable integers. Our results imply that two conjectures hold on average.

This is joint work with Yujiao Jiang and Zhiwei Wang.

13. Unboundedness of Tate-Shafarevich groups in cyclic extensions

欧阳毅
中国科学技术大学
Email: yiouyang@ustc.edu.cn

Abstract

Suppose K is a global field, L/K is a cyclic extension and A/K is an abelian variety. In this talk, we prove unboundedness results of the Tate-Shafarevich groups Sha(A/L) under the following conditions: (1) if A is fixed and L varies, which give an affirmative answer to an open problem proposed by Cesnavicius; (2) if L/K is fixed, and either K is a number field and A varies over elliptic

curves，or $[L : K] = 2$-power and A varies over quadratic twists of a principally polarized abelian variety, which generalize results of KMatsuno and M. Yu respectively.

This is a joint work with Jianfeng Xie.

14. 有限群上的受限制和集

潘颢
南京财经大学
Email: haopan79@zoho.com

Abstract

我们将简单介绍关于有限群上的受限制和集的一些结果。

15. CM情形的Lang-Trotter猜想

秦厚荣
南京大学
Email: hrqin@nju.edu.cn

Abstract

假设E是定义在有理数数域$\mathbb{Q}$上的椭圆曲线. 对于素数p, 我们用a_p表示Frobenius自同态的迹. 任意给定整数r, 定义$\pi_{E,r}(x) := \sum_{p\leq x, p\nmid \Delta_E, a_p=r} 1$. Lang-Trotter 猜想断言，当$x \to \infty$时，

$$\pi_{E,r}(x) = C_{E,r} \cdot \frac{\sqrt{x}}{\log x} + o(\frac{\sqrt{x}}{\log x})$$

这里$C_{E,r}$是一个非负常数. 我们将讨论常数$C_{E,r}$的具体值.

16. New results on power residues modulo primes

孙智伟
南京大学
Email: zwsun@nju.edu.cn

Abstract

In this talk we introduce some new results on power residues modulo primes. Let p be an odd prime, and let a be an integer not divisible by p. When m is a positive integer with $p \equiv 1 \pmod{2m}$ and 2 is an mth power residue modulo p, the speaker determines the value of the product $\prod_{k\in R_m(p)}(1+\tan\pi\frac{ak}{p})$, where

$$R_m(p)=\{0<k<p:\ k\in\mathbb{Z} \text{ is an } m\text{th power residue modulo } p\}.$$

In particular, if $p=x^2+64y^2$ with $x,y\in\mathbb{Z}$, then

$$\prod_{k\in R_4(p)}\left(1+\tan\pi\frac{ak}{p}\right)=(-1)^y(-2)^{(p-1)/8}.$$

Let $p>3$ be a prime, and let $(\frac{\cdot}{p})$ be the Legendre symbol. Let $b\in\mathbb{Z}$ and $\varepsilon\in\{\pm1\}$. Joint with Q.-.H. Hou and H. Pan, we prove that

$$\left|\left\{N_p(a,b):\ 1<a<p \text{ and } \left(\frac{a}{p}\right)=\varepsilon\right\}\right|=\frac{3-(\frac{-1}{p})}{2},$$

where $N_p(a,b)$ is the number of positive integers $x<p/2$ with $\{x^2+b\}_p>\{ax^2+b\}_p$, and $\{m\}_p$ with $m\in\mathbb{Z}$ is the least nonnegative residue of m modulo p.

We will also mention some open conjectures.

17. PDA及其组合刻画

唐小虎
西南交通大学
Email: xhutang@home.swjtu.edu.cn

Abstract

最近，Placement-Delivery Array（PDA）被提出用于描述编码缓存方案的放置和发送阶段。本报告中，我们首先介绍PDA及其在视频分发、分布式计算系统等方面的应用，然后我们给出PDA 的一种组合刻画。

18. Divisibility of zeros and Poles for zeta functions

万大庆
美国加州大学欧文分校
Email: dwan@math.uci.edu

Abstract

For an affine variety over the finite field of q elements, the reciprocal zeros and poles of its zeta function are algebraic integers. The q-divisibility of these reciprocal zeros and poles as algebraic integers was studied by Ax-Katz (1971), Deligne (1973), the speaker (2000) and Esnault-Katz (2005). In this introductory talk, we explain new progress which unifies and sharpens all previous results in this direction. This is based on recent joint work with Esnault and with Dingxin Zhang on q-divisibility for Frobenius eigenvalues acting on l-adic cohomology and rigid cohomology.

19. 勒让德猜想与相关问题

吴杰
法国国家科学研究中心（CNRS）
Email:jie.wu@univ-lorraine.fr

Abstract

十八世纪法国数学家勒让德(Adrien-Marie Legendre) 猜想每两个连续平方数之间一定存在素数。虽然此猜想至今还未彻底解决，然而两百多年来，经过人们的不断努力已发展许多有力的工具、建立了非常丰富的理论、并取得了重要的阶段性成果。在本报告中，我们将简单地介绍相关的主要内容。特别地，我们将介绍报告人与哈尔滨工业大学刘弘泉教授的合作工作：关于短区间整数的最大素因子的下界估计。

20. On the linear independence measure of logarithms of rational numbers

吴强
西南大学
Email:qiangwu@swu.edu.cn

Abstract

In this talk, we will present some new results on the linearly independence measure of logarithms of rational numbers.

21. The fourth moment of Dirichlet L-functions at the central value

吴小胜
合肥工业大学
Email:xswu@amss.ac.cn

Abstract

The asymptotic formula of the fourth moment of Dirichlet L-functions at the central value was predicted in a conjecture by J. B. Conrey, D.W. Farmer, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, and the prime moduli case was proved by M. P. Young in his famous paper "The fourth moment of Dirichlet L-functions, Ann. Math., 173, 1 – 50 (2011)". In this talk, we will introduce our recent work, establishing this asymptotic formula for general moduli.

22. Cameron-Liebler line classes, tight sets and strongly regular Cayley graphs)

向青
南方科技大学
Email: xiangq@sustech.edu.cn

Abstract

Cameron-Liebler line classes are sets of lines in $PG(3,q)$ having many interesting combinatorial properties. These line classes were first introduced by Cameron and Liebler in their study of collineation groups of $PG(3,q)$ having the same number of orbits on points and lines of $PG(3,q)$. During the past decade, Cameron-Liebler line classes have received considerable attention from researchers in both finite geometry and algebraic combinatorics. In the original paper by Cameron and Liebler, the authors gave several equivalent conditions for a set of lines of $PG(3,q)$ to be a Cameron-Liebler line class; later Penttila gave a few more of such characterizations. We will use one of these characterizations as the definition of Cameron-Liebler line class. Let $\mathscr{L}$ be a set of lines of $PG(3,q)$ with $|\mathscr{L}| = x(q^2+q+1)$, x a positive integer. We say that $\mathscr{L}$ is a Cameron-Liebler line class with parameter x if every spread of $PG(3,q)$ contains x lines of $\mathscr{L}$. It turned out that Cameron-Liebler line classes are closely related to certain subsets of points (tight sets) of the Klein quadric. We will talk about a recent construction of a new infinite family of Cameron-Liebler line classes with parameter $x = (q+1)2/3$ for $q \equiv 2 \pmod 3$. When q is an odd power of 2, this family of Cameron-Liebler line classes represents the first infinite family of Cameron-Liebler line classes ever constructed in $PG(3,q)$, q even. This talk is based on joint work with Tao Feng, Koji Momihara, Morgan Rodgers and Hanlin Zou.

23. An improvement on Hasse-Weil bound and applications

邢朝平
上海交通大学
Email:xingcp@sjtu.edu.cn

Abstract

In this talk, we show an improvement on Hasse-Weil bound and applications to coding, cryptography and exponential sums. We first introduce our improvement and then show how the result can be applied to various topics. Finally, we provide a very brief idea on the proof.

24. On indefinite k-universal integral quadratic forms over number fields

徐飞
首都师范大学
Email: xufei@math.ac.cn

Abstract

An integral quadratic form is called k-universal if it represents all integral quadratic forms of dimension k. This is a natural extension of classical universal forms to higher dimensional situation. In this talk, we will prove that a number field F admits an integral quadratic form which is locally k-universal but not globally if and only if $k = 1$ or 2 and the class number of F is even. When $k = 1$, there are infinitely many classes of such integral quadratic forms over F. When $k = 2$, there are only finitely many classes of such integral quadratic forms over F.

25. Linearly recurrent sequences and p-regularity

姚家燕
清华大学
Email: jyyao@tsinghua.edu.cn

Abstract

In this talk we show the p-regularity of the p-adic valuation of a p-adic analytic function with exponential perturbations. Then we apply it to study linearly recurrent sequences, and give a necessary and sufficient condition for the p-adic valuation of a linearly recurrent sequence of arbitrary order to be p-regular. Finally we present two families of linearly recurrent sequences of higher orders whose p-adic valuations are p-regular.

26. Permutation polynomials and their compositional inverses

袁平之
华南师范大学
Email: yuanpz@scnu.edu.cn

Abstract

we prove that every PP is an AGW-PP. We also provide a local method to find compositional inverses of all PPs, some new PPs and their compositional inverses are given.

27. A class of quasi-cyclic parity-check subcodes of Goppa codes and extended Goppa codes

岳勤
南京航空航天大学
Email: yueqin@nuaa.edu.cn

Abstract

Let $\mathbb{F}_{q^2}$ be a finite field of order $q^2(=2^{2m})$. In this paper, we find a class of irreducible polynomials $g(x)=x^{q+1}+ax^q+bx+c$ over $\mathbb{F}_{q^2}$ such that we can construct quasi-cyclic parity-check subcodes of Goppa codes and extended Goppa codes with permutation groups $\mathbb{Z}/(q+1)$ and $\mathbb{Z}/(2q+2)$, respectively. Moreover, we support the upper bound of dimensions of these codes.

28. On a sum involving small arithmetic functions

翟文广
中国矿业大学
Email:wgzhai@163.com

Abstract

Suppose $x > 0$ is a large real number and f is any arithmetic function. In recent years, many authors studied the sum $S_f(x) = \sum_{n \leq x} f\left(\left[\frac{x}{n}\right]\right)$ for different f's. If an arithmetic function $f(n)$ satisfies $f(n) \ll n^{\varepsilon}$, then we say f is a *small* arithmetic function. In this talk, I will present some new results about $S_f(x)$ for small arithmetic functions.

29. Twisted generalized Reed-Solomon codes with ℓ twists

张俊
首都师范大学
Email: junz@cnu.edu.cn

Abstract

Twisted generalized Reed-Solomon (TGRS) codes get much attention recently. In this talk, we focus on a class of TGRS codes with general ℓ twists. Conditions to be MDS or self-dual are discussed.

30. A special three-term exponential sums and its fourth power mean

张文鹏
西北大学
Email: wpzhang@nwu.edu.cn

Abstract

In this talk, I use the elementary and analytic methods and the number of the solutions of some congruence equations to study the calculating problem of the fourth power mean of a special three-term exponential sums, and give some interesting identities for them.

31. 几类新型序列编码

周正春
西南交通大学
Email:zzc@swjtu.edu.cn

Abstract

序列编码在通信、雷达和信息安全中具有重要应用，与差集、差族等数学对象具有深刻的联系。本报告主要介绍几类新型序列编码及其应用，并探讨相关的组合问题。

32. 从高斯的格理论到后量子密码

宗传明
天津大学
Email: cmzong@math.pku.edu.cn

Abstract

1831年，高斯提出了格(lattice)的概念。历经Hermite, Minkowski, Siegel, Lovasz等数学家的深入研究,格理论已发展成为数论，代数与几何交叉领域的一个重要数学分支。2021年, Lovasz由于LLL算法荣获Abel奖。2022年, Viazovska由于8维空间和24维空间的堆球成就荣获Fields奖。上世纪末，格理论被意想不到地用于现代密码学，特别是由Shor, Ajtai, Pipher等人进行的抗量子攻击密码体系的研究。2022年7月5日，美国国家标准与技术研究院(NIST) 公布了四项后量子密码标准，其中三项基于格理论。这样，格理论成了未来量子科技时代信息安全的“保护神”。本报告将介绍格理论的历史及其在后量子密码中基础作用。