



山东大学  
SHANDONG UNIVERSITY



## 2022 山大数论日（12月10日）

### 会议日程

时间	报告人	题目	学校
09:20-09:30	开幕式主持：刘建亚（山东大学）		
上午主持：吕广世（山东大学）			
09:30-10:30	贾朝华	丢番图方程与圆法	中国科学院
10:50-11:50	秦厚荣	CM情形的Lang-Trotter猜想	南京大学
下午主持：赵立璐（山东大学）			
14:00-15:00	徐 飞	通过爆破研究具有奇点的代数簇的Brauer-Manin障碍的强逼近	首都师范大学
15:20-16:20	张文鹏	A special three-term exponential sums and its fourth power mean	西北大学
16:30-17:30	宗传明	从高斯的格理论到后量子密码	天津大学

地点：腾讯会议ID：358 9878 8585





山东大学  
SHANDONG UNIVERSITY



2022 山大数论日

## 丢番图方程与圆法

报告人：贾朝华（中国科学院）

**摘要：**圆法是数论的重要方法之一，它在数论问题中有着广泛的应用。报告人将从一些丢番图方程的解法出发，逐步过渡到圆法，使得听众对于圆法的产生有一个比较自然的认识过程。本报告主要针对本科高年级和研究生低年级的同学。

**报告人简介：**贾朝华，中国科学院数学与系统科学研究院研究员，国家杰出青年基金获得者。1987年毕业于北京大学，获得理学博士学位。在素变量的丢番图逼近、几乎所有的相邻素数差、小区间上的三素数定理、小区间上哥德巴赫数的例外集合等重要的数论问题上，取得了一系列重要的进展。曾获得印度Hardy-Ramanujan协会杰出奖，中国科学院自然科学二等奖。





山东大学  
SHANDONG UNIVERSITY



山东大学数学学院  
1930 School of Mathematics Shandong University

数据科学研究院  
Data Science Institute Shandong University

2022 山大数论日

## CM情形的Lang-Trotter猜想

报告人：秦厚荣（南京大学）

**摘要：**假设 $E$ 是定义在有理数域 $\mathbb{Q}$ 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 $x \rightarrow \infty$ ，时

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

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。

**报告人简介：**秦厚荣，南京大学教授，博士生导师，长江学者，国家杰出青年基金获得者。研究方向主要是代数数论和代数K理论。在同余数这一历史悠久问题上的研究上取得了重要成果；在数域的Tame核、Tate核方面做出了原创性工作，引发了大量后续工作；解决了田野，Browkin等人的多个猜想；在著名的椭圆曲线Anomalous素数的Mazur猜想以及Lang-Trotter猜想的研究中取得了突破。研究成果发表于*J. Reine Angew. Math.*, *Proc. Lond. Math. Soc.*, *Math. Ann.*等国际著名期刊。





山东大学  
SHANDONG UNIVERSITY



2022 山大数论日

# 通过爆破(blowing up)研究具有奇点的代数簇 的Brauer-Manin障碍的强逼近

报告人: 徐飞 (首都师范大学)

**摘要:** 建立代数簇Brauer-Manin障碍的强逼近是研究代数簇整点是否存在的一个重要途径。由于隐函数定理和上同调的计算, 通常研究的代数簇是光滑的。而实际数论问题中, 例如解析数论中研究整点问题的方程可能不是光滑的, 甚至光滑部分的Brauer群在相差常数意义下不是有限的。本报告讲解如何通过爆破(blowing up)做奇点解消, 来研究带奇点代数簇Brauer-Manin障碍的强逼近, 并推广已知关于整点存在性的结果。这是和宋恒的合作研究。

**报告人简介:** 徐飞, 首都师范大学特聘教授, 从事算术代数几何研究。在*Duke J. Math.*; *Memoirs of AMS*; *J. Math. Pures Appl.*; *Compositio Math.*; *Adv. Math.*; *J. reine und angew. Math.*; *Math. Ann.*; *Proc. Lond. Math. Soc.*; *Trans. Amer. Math. Soc.* 等学术刊物发表论文四十余篇。获国家自然科学基金杰出青年基金项目和教育部分自然科学一等奖。





山东大学  
SHANDONG UNIVERSITY



2022 山大数论日

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

报告人：张文鹏（西北大学）

**摘要:** In this talk, we used 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.

**报告人简介:** 张文鹏，西北大学数学系二级教授，博士生导师。曾获国家自然科学基金项目资助8次，获陕西省自然科学基金项目资助4次，获陕西省科学技术奖二等奖4次，三等奖2次，获教育部科技进步奖二等奖1次，入选2022年斯坦福大学全球前2%顶尖科学家榜单，国家人事部“百千万人才工程”，入选陕西省“三五人才工程”第一层。被评为陕西省首届科技新星，陕西省优秀留学回国人员，陕西省有突出贡献中青年专家，陕西省有突出贡献专家，指导学生硕士论文获中国数学会钟家庆数学奖1次，指导学生博士论文获全国优秀博士学位论文提名奖1次，指导学生博士论文获陕西省优秀博士学位论文4次。





山东大学  
SHANDONG UNIVERSITY



2022 山大数论日

## 从高斯的格理论到后量子密码

报告人：宗传明（天津大学）

**摘要:** 1611年开普勒提出了如下猜想：在三维空间，球堆积的最大密度是 $\pi/\sqrt{18}$ 。1840年前后，高斯提出了格(lattice)的概念并解决了格堆球的开普勒猜想。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。

**报告人简介:** 宗传明, 国家万人计划领军人才, 国家杰出青年基金获得者, 长江学者特聘教授。曾荣获美国数学会Levi L. Conant奖、国家自然科学基金二等奖、中国数学会陈省身数学奖、维也纳科学技术大学Prechtl奖章、教育部自然科学一等奖等十余项学术荣誉, 曾应邀在世界密码协会亚洲年会Asiacrypto2012, 中国数学会年会等二十余次中外学术会议做大会报告, 曾两次应约在*Bull. Amer. Math. Soc.*发表综述文章。现任*Science China Mathematics*副主编。

