Speakers, Titles and Abstracts

1. N. Saradha (TIFR, Mumbai)

Title: A passage through Diophantine equations

Abstract: Starting with Pythagoras, we shall survey some of the important Diophantine Equations which have attracted the attention of several mathematicians.

2. S.D. Adhikari (HRI, Allahabad)

Title: Two early Ramsey-type theorems and some early generalizations.

Abstract: The origin of much of the recent developments in Additive Combinatorics can be traced back to some of the early Ramsey-type theorems in Combinatorial Number Theory. Here we take up two of those Ramsey-type theorems and some of the early generalizations.

3. Somjit Datta (Bhaskaracharya Pratisthan, Pune)

Title: Jacobian Elliptic Functions, Theta Functions and Identities of the Rogers-Ramanujan Type

Abstract: In this lecture, an outline of the basic theory of the Jacobian Elliptic Functions and the Theta Functions will be set forth. The importance and implications of the modular transformations of the Theta Functions and the Theta-Zeta correspondence will be briefly discussed. Thereafter the relationship between elliptic curves and modular forms will be demonstrated in the context of the Jacobian theory. A brief account of the celebrated Rogers-Ramanujan identities and other identities related to them will be given.

The chief aim of the lecture will be to show how the Theta Functions and the Jacobian Elliptic Functions have played a crucial role in the evolution of several areas of number theory, algebra and analysis.
4. Shamik Ghosh (Jadavpur University, Kolkata)

Title: Counting number of unordered factorizations of a natural number

Abstract: In this note we describe a new method of counting the number of unordered factorizations of a natural number by means of a generating function and a recurrence relation arising from it, which improves an earlier result in this direction.

5. Kaneenika Sinha (IISER, Kolkata)

Title: Equidistribution in number theory

Abstract: The foundations of equidistribution theory were laid by Hermann Weyl in 1916, who was interested in the behavior of certain sequences consisting of irrational numbers. The ideas in Weyl’s paper have had a big impact on number theory. We will discuss some of those ideas and applications. If time permits, we will also discuss equidistribution questions related to Fourier coefficients of modular cusp forms.

6. Shanta Laishram (ISI, Delhi)

Title: Grimm’s Conjecture and Smooth Numbers

Abstract: Let $g(n)$ be the largest positive integer $k$ such that there are distinct primes $p_i$ for $1 \leq i \leq k$ so that $p_i | n + i$. This function is related to a celebrated conjecture of C.A. Grimm which is considered very difficult. In this talk, we establish upper and lower bounds for $g(n)$ by relating its study to the distribution of smooth numbers. Standard conjectures concerning smooth numbers in short intervals imply $g(n) = O(n^\epsilon)$ for any $\epsilon > 0$. We also prove unconditionally that $g(n) = O(n^\alpha)$ with $0.45 < \alpha < 0.46$. The study of $g(n)$ has some interesting implications for gaps between consecutive primes. This is a joint work with R. Murty.
7. Gautami Bhowmik (Univ.Lille, France)

Title: Methods in Additive Combinatorics.

Abstract: We shall discuss algebraic, analytic and combinatorial methods used in zero-sum problems. In particular we shall mention a new method, that of lattice polyhedra, which has interesting applications.

8. R. Thangadurai (HRI, Allahabad)

Title: Distribution of residues modulo p

Abstract: Let $p$ be an odd prime. In this talk, we give a survey about the various residues (quadratic residue, quadratic non-residue, primitive roots, quadratic non-residue but not primitive roots) how distributed among the elements of modulo $p$.

9. C.S. Rajan (TIFR, Mumbai)

Title: An introduction to algebraic number theory: Quadratic forms, quadratic reciprocity and elliptic curves.

Abstract: The arithmetic theory of quadratic forms will be discussed. If time permits, we will give a brief introduction to the arithmetic of elliptic curves.

10. Subhamoy Maitra (ISI, Kolkata)

Title: Side Channel Attack to Actual Cryptanalysis: Breaking CRT-RSA with Low Weight Decryption Exponents

Abstract: Towards the cold boot attack (a kind of side channel attack), the problems of reconstructing RSA parameters when (i) certain bits are unknown (Heninger and Shacham, Crypto 2009) and (ii) the bits are available but with some error probability (Henecka, May and Meurer, Crypto 2010) have been considered very recently. In this paper we exploit the error correction heuristic proposed by Henecka et al. to show that CRT-RSA schemes having low Hamming weight decryption
exponents are insecure given all encryption exponents (e.g., $e = 2^{16} + 1$).
In particular, we show that the CRT-RSA schemes presented by Lim and Lee (SAC 1996) and Galbraith, Heneghan and McKee (ACISP 2005) with low weight decryption exponents can be broken in a few minutes in certain cases. Further, the scheme of Maitra and Sarkar (CT-RSA 2010), where the decryption exponents are not of low weight but they have large low weight factors, can also be cryptanalysed. We also identify a few modifications of the error correction strategy that provides significantly improved experimental outcome towards the cold boot attack.

11. **Avijit Das** (IIT, Kharagpur)

 **Title:** Recent developments in elliptic-curve cryptography

 **Abstract:** In this talk, a computationally oriented exposition is given to bilinear pairing functions. Miller’s algorithm for the computation of Weil pairing is introduced. The talk ends with some applications of pairing in building cryptographic protocols based upon the bilinear Diffie-Hellman problem.

12. **Satadal Ganguly** (ISI, Kolkata)

 **Title:** Gaps between non-zero Fourier coefficients of cusp forms of level one.

 **Abstract:** We shall discuss the following question of Serre: How large can the length of a string of consecutive zero Fourier coefficients of a modular form be? Using certain congruences for Hecke eigenvalues due to Hatada, it will be shown that there are always non-zero Fourier coefficients in intervals of the type $[X, X + O(X^{1/4})]$ for all $X$ sufficiently large. This is a joint work with Dr. Somya Das.

13. **Ritabrata Munshi** (TIFR, Mumbai)

 **Title:** The circle method

 **Abstract:** In an article with Hardy, Ramanujan introduced the circle method as a powerful tool to study the partition function. Hardy and
Littlewood further developed the method in a series of papers, to study the rational solutions of polynomial equations. Over the years the circle method has proved itself to be indispensable in the analytic theory of numbers. In this expository talk I will briefly explain the method and give some interesting applications.

14. **Anirban Mukhopadhyay (IMSc, Chennai)**

**Title:** Primes and exceptional characters

**Abstract:** Riemann zeta function does not have any real zero. But existence of such a zero for Dirichlet L-functions can not be ruled by present techniques and this presents difficulty in various situations. Surprisingly these unwanted zeros can be used to our advantages in some questions and have produced very strong results. This lecture would be an exposition of some of these unexpected phenomena.