



Advanced Training in Mathematics Schools

Supported by *National Board for Higher Mathematics*

Co-ordinating Institute: Bhaskaracharya Institute in Mathematics (BIM), Pune

Workshop on Elliptic Curves and Cryptology

Venue: *The Institute of Mathematical Sciences, Chennai*

21 July - 2 August, 2008

Conveners: *R. Balasubramanian and D. S. Ramana*

Brief description of ATM Schools

Advanced Training in Mathematics (ATM) Schools are a joint effort of more than fifty active researchers across the country with support from the National Board for Higher Mathematics. The programmes are conducted in reputed mathematics departments in Summer and Winter each year. In these Schools, the emphasis will be on problems solving and on highlighting inter-relations of basic subjects in mathematics. The schools are offered mainly for Ph.D. students and lecturers.

Workshop on Elliptic Curves and Cryptology

The purpose of the programme is to introduce its participants to Cryptography with elements of the theory of Elliptic Curves and Analytic Number Theory that are used in this subject.

This is to be done by means of one course on cryptography followed by two courses on two landmark papers in the subject: H.Lenstra Factoring Integers with Elliptic Curves, *Annals of Mathematics*, 1987 and R. Schoof, Elliptic Curves over ordinary Finite fields and computation of square roots mod p , *Math. Comp.*, 1985.

The courses based on these papers are to be preceded by two background courses covering the material from Elliptic Curves and Analytic Number Theory.

Financial Support

Selected participants will be paid III-AC return train fare from their place of work/home town to the venue by shortest route and provided with a accommodation and local hospitality.

Eligibility for participation

The workshop will admit 25 students in their first and second years of Ph.D. programme, Postdoctoral fellows and some college teachers.

How to Apply

The syllabus, application form and other information about the programme is available on the website:

<http://www.math.iitb.ac.in/atm> or
<http://www.bprim.org>

Applications may also be made on plain paper, giving the following information:

Name, Date of Birth, Age, Gender, Institute/Department, Areas of interest, Address for correspondence, email address, City, State, Pincode, Academic Record: B.Sc./M.Sc./ with names of the Institutes. These should be attested by Head/Principal of the institute. The completed application form should reach by **Monday 12th May, 2008** to:

Prof. R. Balasubramanian
Director,
The Institute of Mathematical Sciences,
C.I.T. Campus, Taramani,
Chennai 600 113.
Email: balu@imsc.res.in, suri@hri.res.in
Tel: 044-2254 3100, 2254 1856,
Fax: 044-2254 1586

List of selected candidates will be posted on the website of The Institute of Mathematical Sciences (www.imsc.res.in) on **Tuesday 20th May, 2008**.

Resource Persons

R. Thangadurai, D.S. Ramana,	H.R.I., Allahabad
Kapil Paranjape, D.S. Nagraj,	I.M.Sc, Chennai.
R. Balasubramanian	I.M.Sc., Chennai.

Unity of Mathematics Lectures

Palash Sarkar	Veni Madhavan
---------------	---------------