

Speaker: Prof. C. S. Rajan (TIFR, Mumbai)

Title: On a converse to the Diophantus-Brahmagupta identity and unique factorization.

Abstract:

An instance of the Diophantus-Brahmagupta identity is that the product of two numbers each of which is a sum of two squares is again a sum of two squares. More generally,

$$(x^2+ny^2)(u^2+nv^2) = (xu +nyv)^2+n(xv-yu)^2$$

It was observed by Fermat that if a number is written as a sum of two coprime squares (a primitive representation), then their factors can also be written as a sum of two squares. However this property fails for the form x^2+5y^2 : the number $21=1^2+5\cdot 4^2$, but its factors 3 and 7 cannot be written in the form x^2+5y^2 . We will discuss the failure of this property, the beginnings of abstract group theory, and how it is linked to the failure of unique factorization in quadratic number fields (time permitting).