IMS September Meeting 2007 Seminar

Title: 'Gauss' method for the determination of the minimal polynomial of the Gaussian period

Speaker: C. Mac an Bhaird

Date: Mon 3rd September 2007 at 12:30PM

Location: ENG226

Abstract: ¡P¿ It is commonly believed that Gauss' method for the determination of Cyclotomic Numbers, and thus the determination of the minimal polynomial of Gaussian Periods, is unwieldy for the general case. See for example, the remarks of Andr233; Weil in ¡I¿Numbers of Solutions of Equations in Finite Fields¡/I¿, Bull. A.M.S., v.55, 1949, pp. 497-508. The prevailing wisdom now seems to be that the determination of the minimal polynomial of the Gaussian Periods, using Jacobi Sums etc., should be done first and then the Cyclotomic numbers be determined as a consequence. In fact, this was suggested by Weil in the paper above. It appears that Gauss' original method has now been abandoned.

¡P¿ We have shown that Gauss' method leads to a series of functional equations. We then obtain necessary and sufficient conditions for these functional equations to have integer solutions. This leads to a finite Diophantine system - the number of equations is independent of the prime. We have shown that this purely Diophantine system has precisely ¡em¿x03C6;(l)¡/em¿ solutions which correspond to the Cyclotomic numbers of order ¡em¿l¡/em¿ . This is, in fact, the first purely Diophantine characterisation of the cyclotomic numbers and the coefficients of the minimal polynomial of the Gaussian

periods and the problem is solved for all orders. The bulk of the work involves proving that the Galois group of a related polynomial acts cyclically on its roots and therefore the polynomial is irreducible. It is then not too difficult to show that the polynomial is in fact the minimal polynomial of the Gaussian Periods. In view of Weil's belief, as alluded to above, it is of interest that Jacobi sums appear nowhere in our argument and furthermore, that the determination of the Cyclotomic numbers can be taken as a starting point for the determination of the Gaussian periods. This of course was Gauss' motivation for his work on Cyclotomic numbers of orders 3 and 4.

¡P¿ There are other descriptions of the general Cyclotomic numbers which involved Diophantine systems, but these descriptions all employ a rejection criterion and so cannot be considered to be purely Diophantine. A purely Diophantine description has the advantage that if one obtains alternative formulae for the cyclotomic numbers, the result can be proved by simply verifying that these formulae satisfy the system of equations.