STATEMENT OF PURPOSE

ARUL SHANKAR, DATE OF BIRTH NOVEMBER 2, 1986, APPLYING TO THE DEPARTMENT OF MATHEMATICS

I am applying for admission to the Ph.D program in Mathematics because I wish to pursue a career in research and teaching. My primary field of interest is Number Theory and I hope to make significant contributions to it. I am applying to Princeton University because I believe that the Mathematics Department at Princeton is the best in the world, especially in my area of interest. I would enjoy studying under A.Wiles, M.Bhargava and other leading experts.

My interest in Mathematics was first kindled when in an attempt to understand the RSA algorithm I read the first few chapters from *A Course in Number Theory and Cryptography* by N. Koblitz. Two years later in 2002, I was selected to attend the IMOTC (the annual summer camp where the Indian team for the IMO is selected) as also in 2003 and 2004. I learnt a lot in these camps, and in the process, my interest in Mathematics grew substantially. At the end of high school I decided to enroll in the BSc Honours programme at the Chennai Mathematical Institute (CMI) because it provided me with the opportunity of learning mathematics from people actively engaged in research. I would then also have the chance to learn from the faculty of the Institute of Mathematical Sciences (IMSc).

In my second year at CMI, I took two optional courses in Number Theory under Professor R.Balasubramanian at IMSc viz. *Algebraic Number Theory*, and *Elliptic Curves and Modular Forms*. In the course on Algebraic Number Theory, we proved the Prime Number Theorem and Dirichlet's theorem on primes in arithmetic progressions among other things. We were studying L functions in the other course and I was astounded by the fact that they encode such basic arithmetic properties. I also understood that there were many close connections between the two subjects. For instance, the question: "When is the ring of integers of an imaginary quadratic field a unique factorization domain" is best solved using the theory of Elliptic Curves.

In the course Elliptic Curves and Modular Forms, I was fascinated by Mordell's proofs of the first two Ramanujan τ conjectures. As Hecke's reinterpretation of the proofs led to the concept of Hecke Operators, I studied them from *Elliptic Curves* by A. Knapp and *A Course in Arithmetic* by J.P. Serre. As a continuation of the course, I am reading further from Knapp's book, and have studied eight chapters of it so far. I plan to finish reading through it this December. I particularly want to read the proof of the fact that the Taniyama -Weil Conjecture implies Fermat's Last Theorem.

One of the things which I found particularly beautiful in the course Elliptic Curves and Modular Forms was the use of complex analysis. I enjoyed the Complex Analysis course I took in my fourth semester taught by Prof. S. Nayak very much and I have studied the book *Theory of Complex Functions* by R. Remmert. I plan to take an advanced course on Complex Analysis offered by Prof. R.Sridharan next semester.

Last semester I took a course on *Abelian Varieties* offered by Prof. S. Ramanan. Here we studied Elliptic Curves using the language of Algebraic Geometry. I understood connections between modular forms, and cohomology and line bundles.

Because of the important role that Representation Theory plays in Number Theory, I took two optional courses in it. As part of the course offered by Prof. S. Kannan, I read through the first two parts of *Linear Representations of Finite Groups by J.P Serre.* In the other course offered by Prof. A. Prasad, we studied modular representations. We finally proved the Brauer Nesbitt theorem which gives information about the Cartan matrix of $F[G]$. The course also involved a project of independent work in which I investigated modular representations of finite abelian groups over finite fields and calculated the radical of its group ring. That allowed me to describe all its irreducible representations. I also made some headway in describing the indecomposible representations.

I am also taking an independent study course with Prof. C.S. Seshadri on *Automorphic Functions* which will continue into the next semester. In this course, I am reading the lecture notes of a course he delivered in 1969 at Harvard.

I understand that there are deep connections between the theory of modular forms and the inverse Galois problem. I also understood that some problems which are simple over Q are not simple over other number fields. As Class Field Theory addresses these matters, I plan to study it from Serre's book next semester.

Prof. Balasubramanian mentioned that the Taniyama -Weil conjecture was a special case of the *Langland's Programme*, which involved relating L functions which arise from Algebraic Geometry to L functions in Number Theory. This December onwards I plan to take a reading course under him and try to understand more of this program.

As top of my class, I will visit the Ecole Normale Superior, Paris, for an internship next summer. There, I plan to study further in Class Field Theory.

I am very interested in applications of Number Theory, especially of those to Cryptography. Last summer (2006), I attended a summer school organized by Microsoft Research. The school included lectures by A. Shamir and other experts. One of the things that particularly interested me was the application of the Riemann Roch theorem and the Tate and Weil pairings in Elliptic Curve Cryptography.

I am also interested in problems of Complexity Theory that arise from Number Theory. In a course on Algorithms that I took in my third semester, we studied the famous algorithm given by M.Agarwal which solved the primality testing problem in polynomial time.

I believe that Princeton University has outstanding departments not just in Mathematics but also in many other areas such as Literature and Music. Given the chance to study at Princeton, I would take courses in these disciplines. I would especially welcome the opportunity to take a course under Prof. Toni Morrison some of whose books I have read and admire.