MSPRF PROJECT SUMMARY: ELEMENTARY AND ANALYTIC NUMBER THEORY IN BOTH THE RATIONAL AND POLYNOMIAL SETTINGS

PAUL POLLACK

Number theory is well-known for its abundance of easily-stated problems whose solutions lie surprisingly deep. An example, still unsolved to this day, is the twin prime conjecture asserting that gaps between consecutive primes are infinitely often as small as they possibly could be – in other words, that there are infinitely many pairs of primes p and $p+2$ ('twin prime' pairs).

To illuminate the underlying structure, it is often convenient in number-theoretic investigations to work not only over the traditional setting of the integers but also over other systems sharing many of the same properties. An important example is the system of integer polynomials considered modulo a prime number p, or more generally the system of polynomials over a finite field. The doctoral thesis of the principal investigator contains a study of the twin prime conjecture and many related elementary-sounding questions in this setting. In this thesis, several methods particular to the polynomial setting (i.e., with no obvious rational analogue) are proposed for the study of such problems.

The PI proposes working with Kevin Ford (UIUC) on questions in elementary and analytic number theory in both the classical (integer) setting and the setting of polynomials over finite fields, with the objective of settling questions of arithmetic interest in both settings.

Many of the methods used to attack questions in the polynomial setting are adaptations of methods belonging to rational number theory. It would therefore be of great benefit to examine the implications for polynomial arithmetic of recent work in classical analytic number theory, much of which Ford is well-acquainted with. In addition, some of the methods introduced by the principal investigator that are peculiar to the polynomial setting are of a bootstrapping nature. In order for them to succeed, they require 'classical' input (for example, from sieve methods and the circle method, both of which Ford is an expert in). It is hoped that the PI's investigations of rational number theory will allow new sources of input to such methods, and thus contribute to new results in the polynomial setting. It is also expected that many of these polynomial results will feed back to the rational setting, and that much of the proposer's research in rational number theory will be of interest independent of applications to polynomials.

Such activities have broader implications. With the advent of modern cryptography, number theory has become a branch of applied mathematics, and the theory of finite fields admits applications also to coding theory and information theory. Irreducible polynomials are needed to model and compute in finite fields, and so understanding the distribution of such polynomials is important apart from its intrinsic interest. Moreover, because the methods employed by the PI lie at the intersection of number theory and algebraic/arithmetic geometry, there is much potential for interdisciplinary interaction. Finally, a substantial amount of the PI's work on polynomial arithmetic is quite accessible to students with only a moderate background in modern algebra, and so one expects that these activities would lead to many viable projects for talented and motivated undergraduates.