INTRODUCTION TO POONEN'S RESEARCH

(for a scientifically literate layperson)

Bjorn Poonen studies number theory and algebraic geometry. In concrete terms, he is interested in solving polynomial equations with the requirement that the coordinates of the solutions be either integers (like -37) or rational numbers (like $-3/5$).

Such requirements add subtlety that can turn the simplest of problems into nightmares. For instance, it is obvious that the equation $x^2 + y^2 = 3$ has infinitely many solutions in real numbers, but are there any solutions in which both x and y are rational numbers? (It turns out that there are none.) In fact, one quickly reaches questions whose answer is not known. For instance, no one knows whether there exists a rectangular box such that its edges, the diagonals of its faces, and the long diagonals all have integer length — this again is a problem about integer solutions to a certain system of polynomial equations.

Problems of this type had been studied for their intrinsic interest since the time of the ancient Greeks. Starting in the 20th century they found unforeseen applications, in cryptography (e.g., to make online transactions secure) and the theory of error-correcting codes (e.g., to encode data on a DVD in such a way that it can be recovered even if errors are introduced).

Poonen's research focuses not on these applications, but rather on the fundamental mathematics underlying and surrounding them. A common thread in much of Poonen's work is to take ideas that previously have been useful in theory, and to transform them into methods that can be used to solve down-to-earth problems, with the aid of a computer. For example, it had been known for over a decade that the equation $x^2+y^3 = z^7$ has finitely many solutions in relatively prime integers, but only very recently did Poonen and his collaborators prove that there are exactly 16 solutions, the largest of which is $(21063928, -76271, 17)$. Thanks to the algorithms developed by Poonen and others, wide classes of polynomial equations can now be solved explicitly.

Poonen also works on the "dark side" of number theory, to prove undecidability results limiting what is computable. Before discussing this, consider the happier situation of polynomial equations in *real* numbers: Gaussian elimination lets one decide whether a system of linear equations has a solution in real numbers, and there is a sophisticated generalization that does the same for systems of polynomial equations of higher degree. On the other hand, in 1970 Matiyasevich proved that the problem of deciding whether a polynomial equation has an *integer* solution is equivalent to the halting problem of computer science, and hence there can be no algorithm for solving this problem in general. Research over the last four decades has not yet determined whether there is an algorithm for the analogous problem for *rational* solutions, but Poonen suspects that this too is unsolvable in general and he has been proving theorems heading in this direction.