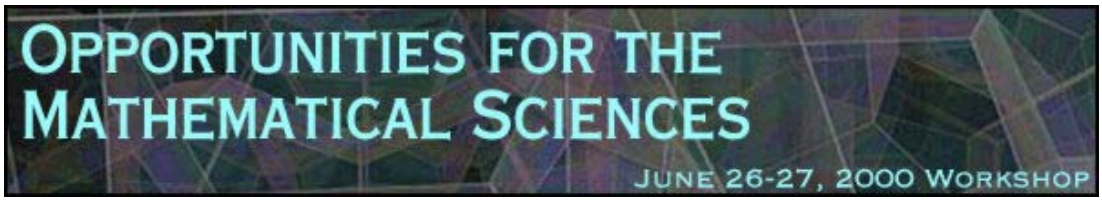

Number Theory and its Connections to Geometry and Analysis

B. MAZUR

The impetus to unify theories has been with us since, at least, the days of Empedocles and Anaxagoras. Much mathematics and physics has been inspired by the drive to unify language, methods, and results. This is indeed famously so in physics where the challenge is to produce a truly unified single theory which accounts for all known interactions. The aim of the Erlangen program at the end of the nineteenth century was to unify geometry and algebra (specifically: group theory). The aim of the Langlands program in the latter part of the twentieth is to unify algebraic number theory and analysis (specifically: representation theory).

The proof of Fermat's Last Theorem (Wiles, Taylor-Wiles) involves, and perhaps requires, a viewpoint that brings together complex analysis, automorphic forms, group representation theory, cohomological techniques whose origin was in topology, ideas from algebraic geometry and commutative algebra, and (of course) a great amount of number theory. The advances stemming from the study of the Seiberg-Witten equations, or of mirror symmetry, occupy an intellectual space that is a meeting-ground for algebraic geometry, symplectic geometry, differential geometry, and the powerful unifying intuitions imported from physics.

"Unification of the educational cultures" is often a consequence of unified theories. And this tends to mean that the younger generation of scientists, brought up in with a broader education in their subject—with a broader sense of what their subject consists of—will have richer scientific goals.

One element of the special richness that number theory, in particular, enjoys at present is that its current open problems stretch from string-theoretic issues to the most basic questions regarding the placement of the prime numbers within the natural numbers; from algebraic geometry, to sphere-packing, to coding and cryptography. Questions that have immediate applications (e.g., how safe is my Internet communication from prying eyes, or prying computers?) are inseparable from fundamental problems in number theory (e.g., find an efficient algorithm to factor integers). The most theoretical aspects of the subject intertwine with the most experimental aspects, and many fundamental "phenomenological" experiments in number theory have direct consequences in the "real" world and the "virtual" world (e.g., putting computer algorithms to rigorous test).

A concrete example?

I will describe, in relatively nontechnical language, one example of a piece of mathematics that unites number-theory, number-experiment, and algorithm-experiment. I am referring to a recent preprint of Noam Elkies, "Rational points near curves and small nonzero $|x^3-y^2|$ via lattice reduction." Elkies' article is, in my opinion, a model for the kind of "full union" these aspects of the subject (theory/experiment/algorithm) will surely enjoy in the future. There are important directions in number theory that would be well served by such a union.

Algebra tends to deal in equalities, in exact equations. Number theory often does. For example, in the Fermat problem, one asks for triples of perfect n^{th} powers a^n, b^n, c^n where the last perfect n^{th} power is exactly the sum of the first two, not just approximately so. You are not interested in "near-misses."

Or are you? It may come as a surprise how many number-theoretic problems there

are which ask for the solution to some "exact equation"--but which, when you jiggle these problems and ask for the structure of their "near-misses," produce yet more profound problems with broader implications. One does not have to go far to see examples of this:

1. Consider the ancient theorem (ascribed to Theaetetus) which asserts that if d is a natural number which is not a perfect square of an integer, then $d^{1/2}$ is irrational. That is, $X^2 - dY^2$ is never zero unless X and Y both are. If you ask "near-miss versions" of this— e.g.., how close to zero can $X^2 - dY^2$ get, and how often—you find yourself with the famous problems first considered by Brahmagupta in the seventh century, or Bhaskára in the twelfth (and, of course, the seventeenth century European mathematicians, Fermat included). The full elucidation of this near-miss problem, which brings in the theory of continued fractions and of quadratic number fields, is still not entirely understood. Moreover, the "partial elucidation" of this near-miss problem that is currently available to us has found immense applications.

2. Consider the following (superficially similar) problem. The polynomial $X^3 - Y^2$ can, of course, achieve the value zero when X is a perfect square. Suppose, however, that X is not a perfect square. How close to zero can $X^3 - Y^2$ get, for appropriate choice of Y? A celebrated conjecture of Hall formulates a neat (still conjectural!) answer to this question[3] which is now but a special case of some grand conjectures of Vojta. Vojta made his conjectures by "unifying" the language of Nevanlinna's work in complex variables, with Diophantine geometry. Hall's conjecture, and Vojta's generalizations are also directly related to the fundamental "ABC-conjecture" due to Masser and Oesterlé, which provides a "quantitative" version of the following qualitative assertion: there is a strong inhibition for two (relatively prime) natural numbers which are highly divisible by perfect powers to have the property that their sum is also highly divisible by a perfect power.

Elkies' article is concerned with a general program for investigating the "near-miss" arithmetic of polynomial relations (and "near-polynomial" relations). Take, for example, the case of projective plane curves given by the zeroes $F(x,y,z) = 0$, where $F(x,y,z)$ is a homogeneous polynomial with integer coefficients. In this case we wish to study the number N of relatively prime triples of integers (x,y,z), each of these integers being of size less than a given bound B, such that the absolute value of $F(x,y,z)$ is small, say less than a quantity C. More specifically, we want to understand the asymptotics of N in terms of the bounds B and C. Questions of this sort are at the heart of much pure research and of many practical applications in present-day number theory. In asking them one is in very difficult theoretical terrain, and to make progress it is important to augment one's analyses with intensive computer experimentation. Elkies has done his work devising algorithms that markedly extend the range of values that are feasible for computation, thereby giving number theorists an opportunity to achieve greater intimacy with the phenomena that show up only at large numbers. Elkies' algorithms reduce the computation to large quantities of lattice reductions. His algorithm, by its very nature, "parallelizes" well. Moreover it can be analyzed quite cleanly in terms of theoretical running-time, this analysis being of interest on its own, but also of interest for the most practical of reasons.

The research program inherent in what I have tried to describe in the preceding paragraph pushes to the extreme limit of present-day capabilities the purest mathematics, and the most applied technology of computation. It also unifies them, the pure and the applied, making each goad the other on.

---

[3] Hall's conjecture would have it that for any exponent a <1/2 there is a constant $C_a > 0$ such that $|X^3 - Y^2|$ is greater than $C_a X^a$ for all $X < Y$ such that $X^3 - Y^2$ is not zero. Back to Text

Last Modified: Oct 17, 2001

Previous page | Top of this page | Next page

The National Science Foundation, 4201 Wilson Boulevard, Arlington, Virginia 22230, USA
Tel: (703) 292-5111, FIRS: (800) 877-8339 | TDD: (800) 281-8749