It's Easy to Get Interested in Number Theory An Interview With Karl Rubin

By Ivars Peterson

Educated at Princeton and Harvard, Professor Karl Rubin held a number of positions before becoming the Thorp Professor of Mathematics at the University of California, Irvine. Stops at Ohio State, Columbia, and Stanford led Rubin to Irvine, where his main research focus is on number theory and elliptic curves. A former Putnam and Sloan Fellow, Rubin's accomplishments also include the AMS Cole Prize in Number Theory, a Guggenheim Fellowship, and the NSF Presidential Young Investigator Award. The author of nearly 60 published papers, Rubin delivered an MAA Distinguished Lecture in May.

Ivars Peterson: Did you become interested in mathematics at a young age? What attracted you to mathematics?

Karl Rubin: I grew up in a scientific family. My mother and sister are astronomers, and both of my brothers are geologists. My father was trained in chemistry and physics but was essentially an applied mathematician, and he especially encouraged me in mathematics.

Beginning when I was in junior high school my father would bring home mathematics books from the library for me. For a long time I just ignored them, but eventually I started reading them. *What is Mathematics*, by Courant and Robbins is one that I remember. Hardy and Wright's *The Theory of Numbers* is another. By the time I finished high school I was pretty sure I wanted to be a mathematician.

I always enjoyed puzzles, and my enjoyment of mathematics was a natural outgrowth of that.

IP: What people or experiences most influenced the direction of your studies? Your subsequent career?

KR: In addition to my parents, the Arnold Ross summer program at Ohio State had a big influence on me. In the 1970s the National Science Foundation was supporting a lot of summer programs for high school students. I think the Ross program was unique in the way it went very deeply into one subject, which happened to be number theory. For the eight weeks of the program, the daily routine Monday through Friday was a one-hour lecture at 9 a.m., followed by a problem set that took most of the next 23 hours to complete. The problem sets would lead the students from numerical discoveries to conjectures to proofs.

I spent two summers in the Ross program as a student while in high school, two more as a counselor while in college, and I have continued to be involved with the program off and on up to the present. In addition to receiving an introduction to real mathematics, and a great example of how to teach mathematics, it was very valuable to meet a group of like-minded students.

I was also fortunate to have a number of good mathematics teachers in the Washington, D.C., public schools. I had many good teachers later as well, but I was pretty well set on my path by then.

When I was an undergraduate at Princeton, the professor who had the greatest influence on me was Kenkichi Iwasawa. But it wasn't until I got to graduate school at Harvard that I learned that there was something called Iwasawa theory, which has been central in a lot of my work. The direction of my research in graduate school and thereafter is due mostly to my advisor, Andrew Wiles, and to John Coates. More recently my work has been influenced by two of my coauthors, Alice Silverberg (who introduced me to cryptography) and Barry Mazur.

IP: How would you describe your main research areas? Why are these areas particularly exciting to you?

KR: I work in algebraic number theory and arithmetic algebraic geometry. A major focus of number theory is solving polynomial equations in integers or rational numbers, and algebraic geometry is a natural tool for approaching such problems. I am especially interested in elliptic curves. Elliptic curves have genus one, and are defined by cubic polynomials. They fall in between curves of genus zero (conic sections, defined by quadratic polynomials), where we know almost everything we want, and curves of genus two or more (defined by higher-degree polynomials), which are more complicated. Elliptic curves have a very rich structure, so progress is possible, but there are still many unanswered questions about them.

In recent years I have also been working on applications of number theory and algebraic geometry to cryptography.

One attractive thing about number theory is that there are many questions that are easy to state, but with solutions that are very deep. Fermat's Last Theorem is a good example. The fact that modern, highly abstract mathematics can be used to solve such an old problem indicates to me that mathematics is moving in the right direction. It's easy to get interested in number theory at a young age, because the questions are relatively accessible. In my case, I never moved away.

IP: Are applications, in cryptography, for example, now an important force in driving number theory research?

KR: Applications are one important force, but certainly not the only one. About twenty years ago people discovered that elliptic curves have applications to cryptography. I have done some work on problems inspired by cryptography, with applications to cryptography. I find it great fun when the things I'm interested in turn out to have useful and surprising applications. I suspect many other "pure mathematicians" feel the same way. But I still spend most of my time on problems with no currently known applications.

IP: What role, if any, can (computational) experiments play in number theory?

KR: Experiments are often very important, and they play some part in most of my work. One important role is as an indication of what to expect, what to try to prove. For example, in the 1950s, Birch and Swinnerton-Dyer carried out some numerical experiments with elliptic curves, which led to what is now the Birch and Swinnerton-Dyer conjecture. This conjecture is one of the Clay Mathematics Institute one million dollar Millennium problems, and has been a driving force behind a lot of modern number theory and arithmetic algebraic geometry.

Computations can also play a role after a theorem has been proved. To me, an abstract result becomes much more exciting if one can use it to produce interesting concrete examples. Examples can give a better understanding of a theorem, and can lead to a better or more useful result.

Personally, I enjoy such calculations. I'm grateful that algorithmic number theorists, clever programmers, and modern computers have given all of us the opportunity to perform computations that would have been unimaginable when I was a student.

IP: What do you see as key questions worthy of future mathematical exploration in number theory?

KR: There are lots of them. The most famous are two of the Clay Millennium problems, the Riemann Hypothesis and the Birch and Swinnerton-Dyer conjecture. Other questions that are particularly interesting to me include questions about rational points on curves.

For example, we still don't know in general how to decide whether a curve of genus one has a rational point. There are also many interesting questions about ranks of elliptic curves that we have no idea how to answer.

In another direction, there are interesting computational questions where progress would have immediate real-world impact. How hard is it to factor large integers? What is the fastest way to solve the discrete logarithm problem in a finite field, or on an elliptic curve over a finite field?

Classroom Capsules Online

The committee working to get more articles in the Classroom Capsules data bank met in the Carriage House at the MAA Headquarters June 2 – 4, 2008. The intention mirrors that of the long running section in the *College Mathematics Journal*: to offer ideas that can be used in the teaching of mainline undergraduate mathematics courses. These include new proofs, new connections to applications or other areas of mathematics, examples, historic tidbits, and more, all kept short and presented in a form ready to use.

Those working on the project, shown from left to right in the picture are Danrun Huang, Paul Zorn, Byungchul Cha, Lang Moore (Executive Editor of MathDL), Olaf Stackelberg, Sue Doree, and Wayne Roberts (Editor of Classroom Capsules).

To visit the Classroom Capsules site, go to http://www.maa.org and scroll down until you see the MAA Resources box.