Euclidean Functions of Computable Euclidean Domains

Professor Rod Downey
School of Mathematics, Statistics and Operations Research
Victoria University of Wellington, New Zealand

Date: 12 September 2013
Time: 4.00pm – 5.00pm
Venue: MAS Executive Classroom 2, MAS-03-07
School of Physical and Mathematical Sciences

This talk treats the security when a given random number is partially leaked to a third party. In this one of the first algorithms discussed in almost any elementary algebra course is Euclid's algorithm for computing the greatest common divisor of two integers. In a first course in abstract algebra, this idea is explained by describing both Z and Q[X] as Euclidean domains. Recall the definition of Euclidean domains:

Definition: A commutative ring R is a Euclidean domain if R is an integral domain and there is a function f from R/{0} to N, the set of natural numbers, such that for any a, d in R, if d is not zero, then there exists a q in R such that either a+qd=0 or f(a+qd)<f(d). The function f is called a (finitely-valued) Euclidean function for R.

We can extend this definition by changing N to ON, where ON is the class of ordinals, i.e., f is now a function f from R/{0} to ON, and call R a transfinite Euclidean domain. In this case, the function f is a transfinately-valued Euclidean function for R. It was proven in a pretty obscure publication that there are transfinite Euclidean domains that are not Euclidean. There are a lot of questions around this fact.

Less well known is that we can define a Euclidian domain via a hierarchy of sets with the property that it exhausts the set R/{0} of nonzero elements if and only if R is a (transfinite) Euclidean domain. At the bottom level R(0) of this hierarchy, we have the units. At the next level R(1), we have all those elements which either exactly divide all elements or give remainder a unit upon division. More generally, at level R(α), we have all those elements which either exactly divide all elements or give remainder in R(α) upon division. This defines a minimal Euclidian function.

In this talk I will look at the effective content and the reverse mathematics of Euclidian domains and in particular, the existence of minimal Euclidian functions. Lots of open questions remain. The talk will be at a reasonably elementary level, notable more for wonderful open questions rather than the depth of the theorems. It is a joint work with Asher Kach.

Speaker Biography

Prof. Rod Downey works in mathematical logic, particularly in computability and complexity theory. He has numerous awards, including Hamilton prize, The New Zealand Association of Scientists Research Medal, New Zealand Mathematical Society Research Award, The Shoenfield Prize. He is a fellow of Royal Society of New Zealand, The Association of Computing Machinery, The New Zealand Mathematical Society, The American Mathematical Society, and was an invited speaker at ICM in Madrid.

Host: Associate Professor Wu Guohua, Associate Chair-SPMS (Graduate Studies), SPMS/Division of Mathematical Sciences