Probability, Number Theory, and Computation

Eric Bach, University of Wisconsin

Every programmer knows that it is much easier to design an algorithm than to explain with a proof why it is correct. This situation is especially acute in computational number theory, where many of the best algorithms for "hard" problems are only supported by heuristic and experimental evidence.
There is a payoff, then, to number theorists who can learn to think probabilistically.

I will start by introducing some of the major models used in algorithmic and experimental number theory. These include random walks, random splitting, and occupancy problems such as coupon collection. As these models typically have sample spaces whose size is exponential (or worse), accurate analysis of them can be a challenge. To illustrate this point, I will finish by discussing some algorithms that are useful in the study of non- uniform coupon collection (joint work with Siddarth Barman and William Umboh).