JOSHUA HOLDEN, Rose-Hulman Institute of Technology

Counting solutions to exponential congruences using p-adic methods

Congruences involving exponential functions are common in modern cryptography and have also come up in questions of pure number theory and in electrical engineering. These functions include the well-known discrete exponentiation map, the self-power map, the discrete Lambert map, and exponential Welch permutations. The number of solutions to such congruences depends, of course, on the range of inputs involved. In some cases we have been able to count the number of solutions exactly, and if the modulus is a prime power, we have found that p-adic methods are very helpful in this. In other cases, the number of solutions can only be estimated. In these cases, experimental observations and heuristics inspired by theory are among the main tools. Some of this is joint work with Margaret Robinson.