Recent developments in primality testing

Carl Pomerance[1] <carl.pomerance@dartmouth.edu>

(Joint work with Hendrik Lenstra.)

In August, 2002, Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, all from the Indian Institute of Technology in Kanpur, announced a new algorithm to distinguish between prime numbers and composite numbers. Unlike earlier methods, their test is completely rigorous, deterministic, and runs in polynomial time. If n is prime and a is an integer, then the polynomials $(x+a)^n$ and x^n+a are congruent modulo n. Therefore they are also congruent modulo n and $f(x)$ for any integer polynomial $f(x)$. The heart of the procedure for testing n involves verifying such a congruence where a runs over a small set of integers, and $f(x)$ is a (craftily chosen) polynomial. In the original paper $f(x)$ is of the form x^r-1, where r is a prime with some additional properties. We have found a way to instead use polynomials like those that arise in the argument of Gauss for constructible regular polygons. It is important that the degree of $f(x)$ be large enough so that the primality test is valid, but not so large that the running time suffers. We are able to choose the degree fairly precisely using some tools from analytic number theory and a new result, due to Daniel Bleichenbacher and Vsevolod Lev, from combinatorial number theory. We thus achieve a rigorous and effective running time of about $(\log n)^6$, the heuristic complexity of the original test.

[1]Dartmouth College