Schwarz-Zippel Lemma

Boran Erol

March 2024

Starting from Lecture 10 of Ryan O'Donnell CS Theory Toolkit. He also has some resources he recommends.

We can construct and work with F_q in $polylog(q)$ time. In certain rare cases, we need randomization.

For p a prime, F_p is a field. In particular, it's a Euclidean domain, so you can efficiently find the inverse using the extended GCD algorithm by solving Bezout's Identity.

An important open problem is TCS is whether we can compute the gcd of two numbers using an efficient parallel algorithm.

One catch to working with F_p is that we sometimes need to find some prime p that's of exponential size in n. We can work with such fields since representing elements of this field is polynomial time. However, how do we find such a p in the first place? The answer is disappointing: sample a random number and test whether it's prime. We don't know whether a deterministic algorithm exists for finding primes. Notice that this is a Las Vegas algorithm and it's fast since primes are dense. This algorithm is in RP.

Lemma 0.1 (Schwarz-Zippel)**.**