01204211 Discrete Mathematics
Lecture 17: Primality testing (2)

Jittat Fakcharoenphol

October 5, 2015

Efficient algorithms

This lecture proves that the two forms of the Fermat's Little Theorem are equivalent. It also considers two efficient algorithms for

- computing powers a^n,
- finding the greatest common divisors.

These two algorithms will be useful for our primality testing algorithm based on the Fermat's Little Theorem that we shall outline at the end of this lecture.