Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 8

Friday, June 17, 2016

Problem 1. (*proof infinitely many primes*) Prove that there are infinitely many primes.

Hint: Assume there are finitely many primes and construct a P that is not divisible by the finite number primes.

Problem 2. (*MRPT error probability*) The Miller-Rabin Primality Test (MPRT) is applied m times, with $m \in \mathbb{N}$, to check whether n is prime. The number n is chosen according to a uniform distribution on the odd numbers in $\{N, \dots, 2N\}$, $N \in \mathbb{N}$.

a) Show that

$$P(\text{"}n \text{ is composite"} \mid \text{MRPT returns } m \text{ times "}n \text{ is prime"}) \leq \frac{\ln(N) - 2}{\ln(N) - 2 + 2^{2m+1}}.$$

b) How many repetitions m are needed to ensure that the above probability stays below $1/1000$ for $N = 2^{512}$?

Hint: Assume $P(\text{"}n \text{ is prime"}) = 2/\ln(N)$.

Problem 3. (*MRPT expected number of tests*) Let $n \in \mathbb{N}$ be odd and composite. Repeat the MRPT with uniformly distributed random numbers $a \in \{2, \dots, n-1\}$ until the output is "n is composite". Assume that the probability of the test outcome "n is prime" is $\frac{1}{4}$.

a) Compute the probability, that the number of such tests is equal to M, for $M \in \mathbb{N}$.

b) What is the expected value of the number of tests?

Problem 4. (*Miller-Rabin Primality Test*)

a) Use the Miller-Rabin Primality Test to prove that 341 is composite.

b) The Miller-Rabin Primality Test comprises a number of successive squarings. Suppose a 300-digit number n is given. How many squarings are needed in worst case during a single run of this primality test?