Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Qinwei He

Exercise 8

Friday, June 23, 2017

Problem 1. *(Multiplicative property of $\phi(n)$)* Let m, n be tow numbers such that $\gcd(m, n) = 1$. Then

$$\phi(mn) = \phi(m)\phi(n).$$

Problem 2. *(Carmichael number)* Let n be composite, odd, no Carmichael number. Then

$$|\{a \in \mathbb{Z}_n \setminus \{0\} \mid a^{n-1} \not\equiv 1 \pmod{n}\}| \geq \frac{n}{2}.$$

Problem 3. (*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 $\{N, \ldots, 2N\}$, $N \in \mathbb{N}$.

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