Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 7

Friday, May 31, 2019

Problem 1. *(Properties of φ)* Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$.

a) Determine $\varphi(p)$ for a prime p.

b) Determine $\varphi(p^k)$ for a prime p and $k \in \mathbb{N}$.

c) Determine $\varphi(p \cdot q)$ for two different primes $p \neq q$.

d) Determine $\varphi(4913)$ and $\varphi(899)$.

Problem 2. *(Multiplicative property of $\varphi(n)$)* Let m, n be two numbers such that $\gcd(m, n) = 1$. Then

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

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 $\{N, \dots, 2N\}$, $N \in \mathbb{N}$.

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