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

Exercise 7

Friday, June 10, 2016

Problem 1. *(determine 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. (*proof Euler's theorem*) Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$. Furthermore, let $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^*$. Prove that

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Problem 3. (*proof Wilson's primality criterion*)

Wilson's primality criterion: An integer $n > 1$ is prime $\Leftrightarrow$ $(n-1)! \equiv -1 (\bmod\, n)$.

a) Prove Wilson's primality criterion.

b) Check if 29 is a prime number by using the criterion above.

c) Is this criterion useful in practical applications?