Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 8

Friday, June 7, 2019

Problem 1. (*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?

Problem 2. *(Pollard's p-1 factoring algorithm)* Pollard's $p-1$ algorithm is an integer factoring algorithm. Evaluate $a^{B!} \mod n$ for factoring.

a) Do you need to determine B or how can you determine B?

b) Please find the non-trivial factors of $n = 1403$ using Pollard's $p-1$ algorithm with $a = 2$.

c) Please find the non-trivial factors of $n = 25547$ using Pollard's $p-1$ algorithm with $a = 2$.

Problem 3. *(Proof Chinese Remainder Theorem)*
Prove the Chinese Remainder Theorem: Suppose $m_1, \ldots, m_r$ are pairwise relatively prime, $a_1, \ldots, a_r \in \mathbb{N}$.

The system of r congruences

$$x \equiv a_i \pmod{m_i}, \qquad i = 1, \ldots, r,$$

has a unique solution modulo $M = \prod_{i=1}^{r} m_i$ given by

$$x \equiv \sum_{i=1}^{r} a_i\, M_i\, y_i \pmod{M},$$

where $M_i = M/m_i$, $y_i = M_i^{-1} \pmod{m_i}, i = 1, \ldots, r$.