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

Exercise 9
Friday, June 23, 2017

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.

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

   b) Please find the non-trivial factors of 1081 using Pollard's $p-1$ algorithm with $a = 2$.

   c) What can you tell from **a)** and **b)** and explain why.

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

$$x \equiv a_i \,(\bmod\, m_i), \qquad i = 1, \ldots, r,$$

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

$$x \equiv \sum_{i=1}^{r} a_i\, M_i\, y_i \quad (\bmod\, M),$$

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