Chair for Theoretical Information Technology
RWTH AACHEN UNIVERSITY

Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 8
- Proposed Solution -

Friday, June 7, 2019

Solution of Problem 1

a) "⇒" Let n with $n > 1$ be prime. Then, each factor m of $(n-1)!$ is in the multiplicative group $\mathbb{Z}_n^*$. Each factor m has a multiplicative inverse modulo n. The factors 1 and $n-1$ are obviously inverse to themselves. The factorial multiplies all these factors. The entire product must be 1 since all pairs of inverses yield 1.

$$(n-1)! \equiv \prod_{i=1}^{n-1} i \equiv \underbrace{(n-1)}_{\text{self-inv.}} \underbrace{(n-2)\cdot \ldots \cdot 3 \cdot 2}_{\text{pairs of inv. } \equiv 1} \cdot \underbrace{1}_{\text{self-inv.}} \equiv (n-1) \equiv -1 \pmod{n}$$

"⇐" Let $n = a\,b$, and hence, composite with $a, b \neq 1$ prime. Thus, $a \mid n$ and $a \mid (n-1)!$. From $(n-1)! \equiv -1 \pmod{n} \Rightarrow (n-1)! + 1 \equiv 0 \pmod{n}$, we obtain $a \mid ((n-1)! + 1) \Rightarrow a \mid 1 \Rightarrow a = 1 \Rightarrow n$ must be prime. ↯

b) Compute the factorial of 28:

$$\begin{aligned} 28! = {} & \overbrace{(28\cdot 27)}^{2}\cdot\overbrace{(26\cdot 25)}^{12}\cdot\overbrace{(24\cdot 23)}^{1}\cdot\overbrace{(22\cdot 21)}^{27}\cdot\overbrace{(20\cdot 19)}^{3}\cdot\overbrace{(18\cdot 17)}^{16} \\ & \underbrace{(16\cdot 15)}_{8}\cdot\underbrace{(14\cdot 13)}_{8}\cdot\underbrace{(12\cdot 11)}_{16}\cdot\underbrace{(10\cdot 9\cdot 8)}_{24}\cdot\underbrace{(7\cdot 6\cdot 5\cdot 4)}_{28}\cdot\underbrace{(3\cdot 2)}_{6} \\ = {} & \underbrace{(2\cdot 12\cdot 1\cdot 27\cdot 3)}_{1}\cdot\underbrace{(16\cdot 8\cdot 8\cdot 16)}_{-1}\cdot\underbrace{(24\cdot 28\cdot 6)}_{1} \equiv -1 \mod 29 \end{aligned}$$

Thus, 29 is prime as shown by Wilson's primality criterion.

c) Using this criterion is computationally inefficient, since computing the factorial is very time-consuming.

Solution of Problem 2

a) Just calculate $b_k = a^{k!} \mod n$, $k = 1, 2, 3, \ldots$ until you find a non-trivial factor by calculating $\gcd(b_k, n)$.

b) When $n = 1403$ and $a = 2$, the process of Pollard's $p-1$ algorithm is

b	d
$b_1 = a \mod 1403 = 2$	$d_1 = \gcd(1, 1403) = 1$
$b_2 = b_1^2 \mod 1403 = 4$	$d_2 = \gcd(3, 1403) = 1$
$b_3 = b_2^3 \mod 1403 = 64$	$d_3 = \gcd(63, 1403) = 1$
$b_4 = b_3^4 \mod 1403 = 142$	$d_4 = \gcd(141, 1403) = 1$
$b_5 = b_4^5 \mod 1403 = 794$	$d_5 = \gcd(793, 1403) = 61$

Therefore, 61 is a non-trivial factor of 1403 and $1403 = 23 \cdot 61$. $B = 5$ is sufficient as $p - 1 = 60 = 2^2 \cdot 3 \cdot 5$.

c) When $n = 25547$ and $a = 2$, the process of Pollard's $p - 1$ algorithm is

b	d
$b_1 = a \bmod 25547 = 2$	$d_1 = \gcd(1, 25547) = 1$
$b_2 = b_1^2 \bmod 25547 = 4$	$d_2 = \gcd(3, 25547) = 1$
$b_3 = b_2^3 \bmod 25547 = 64$	$d_3 = \gcd(63, 25547) = 1$
$b_4 = b_3^4 \bmod 25547 = 18384$	$d_4 = \gcd(18383, 25547) = 1$
$b_5 = b_4^5 \bmod 25547 = 23616$	$d_5 = \gcd(23615, 25547) = 1$
$b_6 = b_5^6 \bmod 25547 = 18620$	$d_6 = \gcd(18619, 25547) = 433$

Therefore, 433 is a non-trivial factor of 25547 and $25547 = 433 \cdot 59$. $B = 5$ is sufficient as $(p-1) = 432 = 2^4 \cdot 3^3$. These are factors within 6!, but not 5!. Note that $q-1 = 58 = 2 \cdot 29$ such that this factorization could only be found calculating b_{29}.

Solution of Problem 3

Chinese Remainder Theorem:
Let $m_1, \ldots, m_r$ be pair-wise relatively prime, i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j \in \{1, \ldots, r\}$, and furthermore let $a_1, \ldots, a_r \in \mathbb{N}$. Then, the system of congruences

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

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

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

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

a) Show that (1) is a valid solution for the system of congruences:

Let $i \neq j \in \{1, \ldots, r\}$. Since $m_j \mid M_i$ holds for all $i \neq j$, it follows:

$$M_i \equiv 0 \pmod{m_j}. \tag{2}$$

Furthermore, we have $y_j M_j \equiv 1 \pmod{m_j}$.

Note that from coprime factors of M, we obtain:

$$\gcd(M_j, m_j) = 1 \Rightarrow \exists\, y_j \equiv M_j^{-1} \pmod{m_j}, \tag{3}$$

and the solution of (1) modulo a corresponding m_j can be simplified to:

$$x \equiv \sum_{i=1}^{r} a_i M_i y_i \overset{(2)}{\equiv} a_j M_j y_j \overset{(3)}{\equiv} a_j \pmod{m_j}.$$

b) Show that the given solution is unique for the system of congruences:

Assume that two different solutions y, z exist:

$$
\begin{aligned}
y &\equiv a_i \pmod{m_i} \ \wedge \ z \equiv a_i \pmod{m_i}, \ i = 1, \ldots, r, \\
\Rightarrow 0 &\equiv (y - z) \pmod{m_i} \\
\Rightarrow & \, m_i \mid (y - z) \\
\Rightarrow & \, M \mid (y - z), \text{ as } m_1, \ldots, m_r \text{ are relatively prime for } i = 1, \ldots, r, \\
\Rightarrow y &\equiv z \pmod{M}.
\end{aligned}
$$

This is a contradiction, therefore the solution is unique.