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

Exercise 7
- Proposed Solution -

Friday, June 10, 2016

Solution of Problem 1

Let $\varphi : \mathbb{N} \to \mathbb{N}$ the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$ with $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.

a) Let $n = p$ be prime. It follows for the multiplicative group that:

$$\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid \gcd(a, p) = 1\} = \{1, 2, \dots, p-1\} \Rightarrow \varphi(p) = p - 1\,.$$

b) The power p^k has only one prime factor. So p^k has a common divisors that are not equal to one: These are only the multiples of p. For $1 \le a \le p^k$:

$$1 \cdot p\,, \quad 2 \cdot p\,, \quad \dots\,, \quad p^{k-1} \cdot p = p^k\,.$$

And it follows that

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)\,.$$

c) Let $n = p\,q$ for two primes $p \neq q$. It holds for $1 \le a < p\,q$

1) $p \mid a \vee q \mid a \Rightarrow \gcd(a, p\,q) > 1$, and
2) $p \nmid a \wedge q \nmid a \Rightarrow \gcd(a, p\,q) = 1$.

It follows $\mathbb{Z}_{p\,q}^* = \underbrace{\{1 \le a \le p\,q-1\}}_{p\,q-1 \text{ elements}} \setminus \left[\underbrace{\{1 \le a \le p\,q-1 \mid p \mid a\}}_{q-1 \text{ elements}} \,\dot\cup\, \underbrace{\{1 \le a \le p\,q-1 \mid q \mid a\}}_{p-1 \text{ elements}}\right]$.
Hence: $\varphi(p\,q) = (p\,q-1) - (q-1) - (p-1) = p\,q - p - q + 1 = (p-1)(q-1) = \varphi(p)\,\varphi(q)$.

d) Apply the Euler phi-function on n with the following steps:

1. Factorize all prime factors of the given n
2. Apply the rules in a) to c), correspondingly.

$\varphi(4913) = \varphi(17^3) \overset{\text{(b)}}{=} 17^2(17-1) = 4624$, and
$\varphi(899) = \varphi(30^2 - 1^2) = \varphi((30-1)(30+1)) = \varphi(29 \cdot 31) \overset{\text{(c)}}{=} 28 \cdot 30 = 840$.

Solution of Problem 2

Let $n \in \mathbb{N}$, $a \in \mathbb{Z}_n^*$ with $\mathbb{Z}_n^* = \{b \in \mathbb{Z}_n \mid \gcd(b,n) = 1\}$.
Consider the map $\Psi : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ defined by $\Psi(x) = ax \mod n$, with $x \in \mathbb{Z}_n^*$.

1) Show that Ψ is well-defined, i.e., $\forall x \in \mathbb{Z}_n^* \Rightarrow ax \in \mathbb{Z}_n^*$.
   $\mathbb{Z}_n^*$ is a multiplicative group, i.e., $\forall x \in \mathbb{Z}_n^*, \forall a \in \mathbb{Z}_n^* \Rightarrow (ax) \in \mathbb{Z}_n^*$. $\square$

2) Show that Ψ is surjective, i.e., $\forall y \in \mathbb{Z}_n^* \ \exists x \in \mathbb{Z}_n^* : \Psi(x) = y$.
   $y \equiv ax \pmod n \Rightarrow a^{-1}y \equiv x \pmod n \Rightarrow \Psi(a^{-1}y) \equiv y \pmod n$.
   Since $\gcd(a,n) = 1$ holds for all $a \Rightarrow \exists a^{-1} \pmod n$. $\square$

3) Show that $\Psi(x)$ is injective, i.e., for $x \not\equiv y \Rightarrow \Psi(x) \not\equiv \Psi(y)$.
   Indirect proof:
   Let $ax \equiv ay \pmod n$. Since $\gcd(a,n) = 1 \Rightarrow \exists a^{-1} \in \mathbb{Z}_n^* : x \equiv y \pmod n$. $\square$

4) From 2) and 3) $\Rightarrow \Psi(x)$ is bijective. $\square$

5) Show that the inverse $a^{-1} \pmod n$ is unique.
   Indirect proof:
   Let $u \not\equiv v \in \mathbb{Z}_n^*$ be inverses of a, i.e., $ua \equiv 1 \pmod n$ and $va \equiv 1 \pmod n$ holds.
   But $u \equiv u(va) \equiv (ua)v \equiv v \pmod n$ is a contradiction $\Rightarrow$ the inverse is unique.
   $\Rightarrow \forall a \in \mathbb{Z}_n^* \ \exists! a^{-1}$. $\square$

6) Show that $a^{\varphi(n)} \equiv 1 \pmod n$:

$$1 \equiv \underbrace{(\textstyle\prod_{x\in\mathbb{Z}_n^*} x)(\prod_{x\in\mathbb{Z}_n^*} x^{-1})}_{\text{5) pairs of unique inverses}} \equiv \underbrace{(\textstyle\prod_{x\in\mathbb{Z}_n^*} \Psi(x))}_{\text{4) bijective fct.}}(\textstyle\prod_{x\in\mathbb{Z}_n^*} x^{-1}) \equiv (\prod_{x\in\mathbb{Z}_n^*} ax)(\prod_{x\in\mathbb{Z}_n^*} x^{-1})$$
$$\equiv a^{\varphi(n)}(\textstyle\prod_{x\in\mathbb{Z}_n^*} x)(\prod_{x\in\mathbb{Z}_n^*} x^{-1}) \equiv a^{\varphi(n)} \pmod n. \quad \blacksquare$$

Solution of Problem 3

a) "$\Rightarrow$" 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.

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

"$\Leftarrow$" Let $n = ab$ and hence composite with $a, b \neq 1$ prime. Thus $a|n$ and $a|(n-1)!$. From $(n-1)! \equiv -1 \Rightarrow (n-1)! + 1 \equiv 0$, we obtain $a|((n-1)!+1) \Rightarrow a|1 \Rightarrow a = 1 \Rightarrow n$ must be prime. $\lightning$

b) Compute the factorial of 28:

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

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.