Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 10
- Proposed Solution -

Friday, June 29, 2018

Solution of Problem 1

Suppose that a is a primitive element modulo n and let the number $r \in \{1, \ldots, \varphi(n)\}$ satisfy $(r, \phi(n)) = 1$. Put $s = a^r$ and consider the set $\{s, \ldots, s^{\varphi(n)}\}$. First see that if $s^i = s^j \mod n$ for $1 \leq j < i \leq n$, then $a^{r(i-j)} = 1 \mod n$. Since a is a primitive element modulo n and $(r, \phi(n)) = 1$ we have :

$$\varphi(n) \mid r(i-j) \implies \varphi(n) \mid i-j,$$

but the latter is impossible if $i \neq j$ $(0 < i - j < \varphi(n)$. Therefore all elements of the set $\{s, \ldots, s^{\varphi(n)}\}$ should be different modulo n which implies that the set is the multiplicative group modulo n. Hence s is a primitive element modulo n.

Now since a is a primitive element, then all elements of the set $\{1 \leq r \leq \varphi(n)\} : (r, \phi(n)) = 1\}$ are different primitive elements modulo n. Hence there exist $\varphi(\varphi(n))$ many of them.

Solution of Problem 2

a) The task is to compute $x = \log_3 y$ with $x \in \mathbb{Z}_{79}^*$ and y either 18 or 1.

- We solve $x = \log_3 18$ by an exhaustive search.

x	$3^x \mod 79$
0	1
1	3
2	9
3	27
4	$81 \equiv 2$
6	$729 \equiv 18$

$$\Rightarrow \log_3 18 \equiv 6 \mod 79$$

- We want to solve $x = \log_3 1$. From Theorem 6.2 (Euler, Fermat) we know that:

$$a^{p-1} \equiv 1 \mod 79$$

$$\Rightarrow \log_3 1 = p - 1 = 78 \mod 79$$

b) For trivial cases where $x = 1$ or $= -1$, $\varphi(n)$ or $\varphi(n)/2$ are the solutions and no search is required. In other cases, the worst case, it would be 76 tryings. Multiplication of large numbers is computationally complex. No efficient algorithm for the calculation of the discrete logarithm is known.

Solution of Problem 3

Proof. "$\Rightarrow$" If a is a primitive element modulo p, then, by definition, $\text{ord}_p(a) = p - 1$. Since $\frac{p-1}{p_i} < p - 1 = \text{ord}_p(a)$,

$$\forall i : a^{\frac{p-1}{p_i}} \not\equiv 1 \mod p\,.$$

"$\Leftarrow$" If a is *not* a primitive Element modulo p, then $\text{ord}_p(a) = k$ and $k|(p-1)$. Then

$$\exists c \neq 1 \text{ with } p - 1 = k \cdot c\,.$$

Since $c \neq 1$, it holds that $p_i|c$ for some i. For that i, we get

$$a^{\frac{p-1}{p_i}} \equiv a^{\frac{k\cdot c}{p_i}} \equiv \underbrace{(a^k)}_{\equiv 1,\ \text{since } k=\text{ord}_p(a)}{}^{\frac{c}{p_i}} \equiv 1 \mod p\,.$$

□