**Prof. Dr. Rudolf Mathar, Dr. Michael Reyer**

# Tutorial 9
# - Proposed Solution -

Friday, June 21, 2019

## Solution of Problem 1

There is the following system of linear congruences:

$$\begin{aligned} x &\equiv 3 \pmod{11} \\ x &\equiv 5 \pmod{13} \\ x &\equiv 7 \pmod{15} \\ x &\equiv 9 \pmod{17}. \end{aligned}$$

**a)** Compute the smallest positive solution using the Chinese Remainder Theorem.

$$\begin{aligned} M &= 11 \cdot 13 \cdot 15 \cdot 17 = 36465 \\ M_1 &= \frac{M}{m_1} = \frac{M}{11} = 3315 \\ M_2 &= \frac{M}{13} = 2805 \\ M_3 &= \frac{M}{15} = 2431 \\ M_4 &= \frac{M}{17} = 2145 \\ Y_1 &= M_1^{-1} \mod m_1 = 3315^{-1} \mod 11 = 3 \\ Y_2 &= 2805^{-1} \mod 13 = 4 \\ Y_3 &= 2431^{-1} \mod 15 = 1 \\ Y_4 &= 2145^{-1} \mod 17 = 6 \end{aligned}$$

It follows

$$\begin{aligned} x &= 3 \cdot 3315 \cdot 3 + 5 \cdot 2805 \cdot 4 + 7 \cdot 2431 \cdot 1 + 9 \cdot 2145 \cdot 6 \mod 36465 \\ &= 218782 \mod 36465 = 36457. \end{aligned}$$

## Solution of Problem 2

Suppose that $a$ is a primitive element modulo $n$ and let the number $r \in \{1, \ldots, \varphi(n)\}$ satisfy $\gcd(r, \varphi(n)) = 1$. Let $s = a^r \mod n$ and consider the set $\{s, \ldots, s^{\varphi(n)}\}$. First see that if

$s^i \equiv s^j \pmod{n}$ for $1 \leq j < i \leq \varphi(n)$, then $a^{r(i-j)} \equiv 1 \pmod{n}$. Since $a$ is a primitive element modulo $n$ and $\gcd(r, \varphi(n)) = 1$ 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 $n$.

Since $a$ is a primitive element, all elements of the set $\{1 \leq r \leq \varphi(n) \mid \gcd(r, \varphi(n)) = 1\}$ are different primitive elements modulo $n$. Hence, there exist at least $\varphi(\varphi(n))$ many of them.

On the other hand, if $\gcd(r, \varphi(n)) = d > 1$, then $s^{\frac{\varphi(n)}{d}} = a^{\frac{r\varphi(n)}{d}} = (a^{\varphi(n)})^{\frac{r}{d}} \equiv 1 \pmod{n}$. Hence, $s = a^r$ is no primitive element, if $\gcd(r, \varphi(n)) > 1$, thus, there exists exactly $\varphi(\varphi(n))$ many primitive elements.

## Solution of Problem 3

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

- We need to solve $x = \log_3 18 = 2^2 \cdot 3$.

| $x$ | $3^x \mod 79$ | |
|---|---|---|
| 0 | 1 | |
| 1 | 3 | Now we just need to find $3^x \equiv 2 \pmod{79}$ |
| 2 | 9 | |
| 3 | 27 | |
| 4 | $81 \equiv 2$ | |
| 6 | $729 \equiv 18$ | |

  Hence, $3^6 = 3^1 \cdot 3^1 \cdot 3^4 \equiv 3 \cdot 3 \cdot 2 = 18 \pmod{79}$.

- It holds $\log_3 1 = 0$.

**b)** For trivial cases where $y = 1$ or $y = -1$, 0 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 4

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

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

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

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

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

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

□