Exercise 9

Problem 4

$$x \equiv 3 \mod 11$$

$$x \equiv 5 \mod 13$$

$$x \equiv 7 \mod 15$$

$$x \equiv 9 \mod 17$$

$$x = 3a_1 + 5a_2 + 7a_3 + 9a_4$$

$a_1 \equiv 1 \mod 11 \qquad a_2 \equiv a_3 \equiv a_4 \equiv 0 \mod 11$

$a_2 \equiv 1 \mod 13 \qquad a_1 \equiv a_3 \equiv a_4 \equiv 0 \mod 13$

$a_3 \equiv 1 \mod 15 \qquad a_1 \equiv a_2 \equiv a_4 \equiv 0 \mod 15$

$a_4 \equiv 1 \mod 17 \qquad a_1 \equiv a_2 \equiv a_3 \equiv 0 \mod 17$

$$a_1 = 13 \times 15 \times 17 \times b_1$$

$$b_1 (15 \times 13 \times 17) \equiv 1 \mod 11$$

$$b_1 = (15 \times 13 \times 17)^{-1} \mod 11 = 3$$

$$a_1 = 3 \times 13 \times 15 \times 17$$

$a_2 = 11 \times 15 \times 17 \times b_2$ $\quad b_2 = (11 \times 15 \times 17)^{-1} \bmod 13$

$a_3 = 11 \times 13 \times 17 \times b_3$ $\quad b_3 = (11 \times 13 \times 17)^{-1} \bmod 15$

$a_4 = 11 \times 13 \times 15 \times b_4$ $\quad b_4 = (11 \times 13 \times 15)^{-1} \bmod 17$

$b_2 = 4 \quad b_3 = 1 \quad b_4 = 0$

$x = 3a_1 + 5a_2 + 7a_3 + 9a_4 \mod (11 \times 13 \times 15 \times 17)$

$= 36457 \mod 36465$

Problem 2. $\exists\, a$: primitive element mod n,

$\exists\, \varphi(\varphi(n))$ many.

$a^K \equiv 1 \mod n \Rightarrow K = \varphi(n)$.

K smallest number

$\mathbb{Z}_{\varphi(n)} = \{1, 2, \ldots, \varphi(n)\} \longrightarrow \mathbb{Z}^*_{\varphi(n)} = \{r_1, r_2, \ldots, r_{\varphi(\varphi(n))}\}$

$\{a^{r_i} : r_i \in \mathbb{Z}^*_{\varphi(n)}\}$

Let $a^{r_i} \equiv a^{r_j} \bmod n$, w.l.o.g.

assume $r_j > r_i \Rightarrow a^{r_j - r_i} \equiv 1 \bmod n$

$r_j - r_i < \varphi(n)$

※ contradiction.

$\Rightarrow$ all a^{r_i}'s are different.

$$(a^{r_i})^K \equiv 1 \bmod n \Rightarrow a^{r_i K} \equiv 1 \bmod n$$

$$\xrightarrow[\text{prim. elem.}]{a} \varphi(n) \mid r_i \cdot K$$

a. prim. elem. mod n. $a^K \equiv 1 \bmod n$

$\Rightarrow \varphi(n) \mid K$

$(r_i, \varphi(n)) = 1 \Rightarrow \varphi(n) \mid K$.

$\Rightarrow \operatorname{ord}_n a^{r_i} = \varphi(n)$

$\Rightarrow a^{r_i}$ is a prim. elem.

$\varphi(\varphi(n))$ prim. elem. mod n.

Problem 3.

a) discrete log. of 18 and 1 in $\mathbb{Z}^*_{79}$

with the generator $\underline{\underline{3}}$

$\log_3 18 = x$

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

$\log_3 1 = x$

$3^x \equiv 1 \mod 79$

$x = 78$

b) if $y = 1$ or $y = -1$ mod 79
mod n

$\varphi(n)$ and $\varphi(n)/2$

if $y \neq \pm 1 \Rightarrow \varphi(n) \Rightarrow 78$ tryings

Problem 4: $p > 3$ $\quad p-1 = \prod_{i=1}^{k} p_i^{t_i}$

$a \in \mathbb{Z}_p^*$ is a primitive elem. $\Longleftrightarrow$

$$a^{\frac{p-1}{p_i}} \not\equiv 1 \mod p \quad \forall i \in \{1, \dots, k\}$$

$(\Rightarrow)$

$a^{p-1} \equiv 1 \mod p$ and $\mathrm{ord}_p a = p-1$

$\Rightarrow a^k \not\equiv 1 \mod p \quad k < p-1$

$\Rightarrow a^{p-1/p_i} \not\equiv 1 \mod p$.

$(\Leftarrow)$

Suppose a is not a primitive elem.

$a^k \equiv 1 \mod p$ and $k < p-1 \Rightarrow$

$k \mid p-1 \Rightarrow k = \prod_{i=1} p_i^{t_i'}$

$\boxed{\mathrm{ord}_p a = k \Rightarrow k \mid \varphi(p)}$

and $\exists t_j'$: $\left.\begin{array}{l} t_j' < t_j \\ t_j' \leq t_j - 1 \end{array}\right\} \Rightarrow k \mid \frac{p-1}{p_j}$

$\Rightarrow a^{p-1/p_j} \equiv 1 \mod p$. X