PROBLEM I Assume $A = \{a \in P \mid a \mid m\} = \{q_i \mid i = 1, \cdots, s\}$, where $P \subset \mathbb{N}$, $\forall p \in P$, p is prime, $s = |A|$. Prove: g is the primative root mod $m \iff g$ is q_i-tic non-residue mod m, $\forall i = 1, \cdots, s$.

SOLUTION . On one hand, assume g is q_i-th power residue of m, then $g \equiv h^{q_i} \mod m$. So $g^{\frac{\phi(m)}{q_i}} \equiv h^{\phi(m)} \equiv 1 \mod m$, contradiction!

On the other hand, assume $o(g) < \phi(m)$. Easily $o(g) \mid \phi(m)$, so $\frac{\phi(m)}{o(g)} \in \mathbb{Z}$. So $\exists i, q_i \mid \frac{\phi(m)}{o(g)}$. Then $g^{\frac{\phi(m)}{q_i}} \equiv 1 \mod m$. Then g is q_i-th power residue of m. □

PROBLEM II Prove:

1. 10 is the primative root mod $17, 257$.
2. The length of repetend of $\frac{1}{17}$ is 16, the length of repetend of $\frac{1}{257}$ is 256.

SOLUTION . Easily $\phi(17) = 16 = 2^4$. So we only need to check $10^8 \not\equiv 1 \mod 17$. Easily $10^8 \equiv 100^4 \equiv (-2)^4 \equiv 2^4 \equiv -1 \mod 17$. So 10 is primative root of 17.

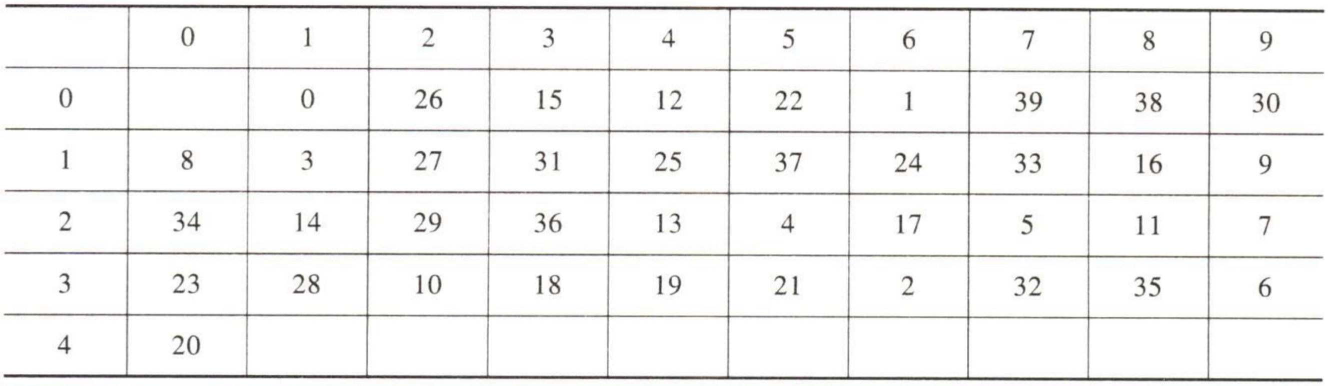
Easily $\phi(257) = 256 = 2^8$, so we only need to check $10^{128} \not\equiv 1 \mod 257$. By calculation easily to get that $10^{128} \equiv -1 \mod 257$. So 10 is primative root of 17.

Since 10 is primative root of $17, 257$, we know the length of loop-body of $\frac{1}{17}, \frac{1}{257}$ are $16, 256$. □

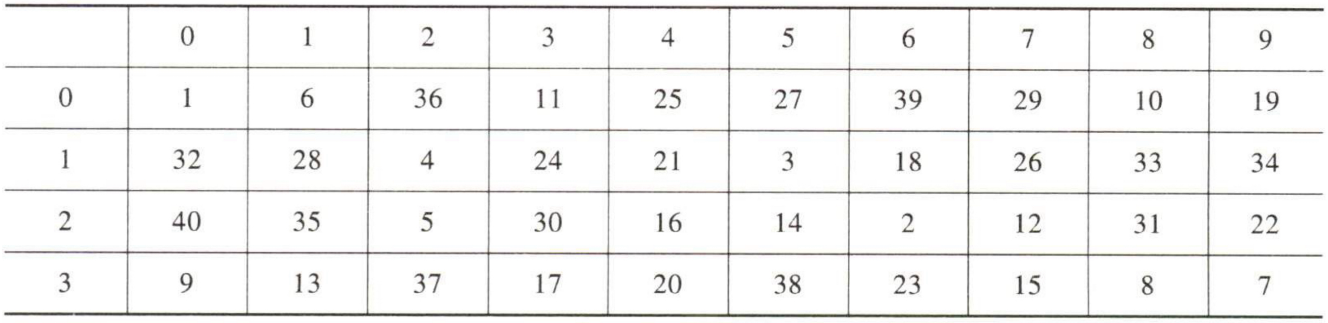
PROBLEM III Apply index table to solve the equation

$$x^{15} \equiv 14 \pmod{41}.$$

SOLUTION . Use 6 as primative root of 41, we have this table of index:



	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									



	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Then $x^{15} \equiv 14 \mod 41 \iff 15 \operatorname{ind} x \equiv \operatorname{ind} 14 \mod 40 \iff 3 \operatorname{ind} x \equiv 5 \mod 8 \iff \operatorname{ind} x \equiv 7 \mod 8$. So $\operatorname{ind} x = 7, 15, 22, 29, 36$. So $x \equiv 29, 3, 5, 22, 23 \mod 41$. □

PROBLEM IV Assume $m > 2$ has primative root, prove for any primative root g of m, we have $\operatorname{ind}_g -1 = \frac{1}{2}\phi(m)$.

SOLUTION. We have $g^{\phi(m)} \equiv 1 \mod m$. So $\operatorname{ind}_g 1 = 0$. Since $(-1)^2 \equiv 1 \mod m$, we have $2 \operatorname{ind}_g -1 \equiv \operatorname{ind}_g 1 \mod \phi(m)$. So $\operatorname{ind}_g -1 \equiv 0 \mod \frac{\phi(m)}{2}$. But obviously $\operatorname{ind}_g -1 \neq 0$, so we obtain $\operatorname{ind}_g -1 = \frac{\phi(m)}{2}$. □

PROBLEM V Assume g_1, g_2 are two primative root mod m, prove:

1. $\operatorname{ind}_{g_1} g \cdot \operatorname{ind}_g g_1 \equiv 1 \pmod{\phi(m)}$;
2. $\operatorname{ind}_g a \equiv \operatorname{ind}_g g_1 \cdot \operatorname{ind}_{g_1} a \pmod{\phi(m)}$

SOLUTION.

1. Let $a = \operatorname{ind}_{g_1} g, b = \operatorname{ind}_g g_1$. By the defination, we can get that $g_1^a \equiv g \pmod{\phi(m)}, g^b \equiv g_1 \pmod{\phi(m)}$. Then $(g_1^a)^b = g_1^{ab} \equiv g^b \equiv g_1 \pmod{\phi(m)}$. Since g_1 is the primative root of m, then $ab \equiv 1 \pmod{\phi(m)}$.
2. Only need to check $g^{\operatorname{ind}_g g_1 \cdot \operatorname{ind}_{g_1} a} \equiv a \mod m$. Easily $g^{\operatorname{ind}_g g_1 \cdot \operatorname{ind}_{g_1} a} \equiv g_1^{\operatorname{ind}_{g_1} a} \equiv a \mod m$.

□