

NumberTheory 11

白永乐

202011150087

202011150087@mail.bnu.edu.cn

2024 年 5 月 31 日

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

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

PROBLEM II Prove:

1. 10 is the primitive 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 $10^8 \not\equiv 1 \pmod{17}$. Easily $10^8 \equiv 100^4 \equiv (-2)^4 \equiv 2^4 \equiv -1 \pmod{17}$. So 10 is primitive root of 17.

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

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

PROBLEM III Apply index table to solve the equation

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

SOLUTION. Use 6 as primitive 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 $x^{15} \equiv 14 \pmod{41} \iff 15 \text{ind } x \equiv \text{ind } 14 \pmod{40} \iff 3 \text{ind } x \equiv 5 \pmod{8} \iff \text{ind } x \equiv 7 \pmod{8}$. So $\text{ind } x = 7, 15, 22, 29, 36$. So $x \equiv 29, 3, 5, 22, 23 \pmod{41}$. \square

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

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

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

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

SOLUTION. 1. Let $a = \text{ind}_{g_1} g, b = \text{ind}_g g_1$. By the definition, 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 primitive root of m , then $ab \equiv 1 \pmod{\phi(m)}$.

2. Only need to check $g^{\text{ind}_g g_1 \cdot \text{ind}_{g_1} a} \equiv a \pmod{m}$. Easily $g^{\text{ind}_g g_1 \cdot \text{ind}_{g_1} a} \equiv g_1^{\text{ind}_{g_1} a} \equiv a \pmod{m}$.

\square