

(11)

H.W. Problems for Chapter 8

Ex. 1: 1, 2, 12; Ex. 2: 1, 4, 6; Ex. 3: 1, 2, 4.

Ex. 1 #1 (a)

$$\left. \begin{aligned} 2^{16} &\equiv 1 \pmod{17} \\ 2^8 &\equiv -1 \pmod{17} \\ 2^4 &\equiv -1 \pmod{17} \end{aligned} \right\} \begin{array}{l} \text{The order of } 2 \pmod{17} \\ \text{is } 8. \end{array}$$

Similarly,

$$3^{16} \equiv 1, \quad 3^8 \equiv -1 \Rightarrow \text{The order of } 3 \pmod{17} \text{ is } 16.$$

$$5^{16} \equiv 1, \quad 5^8 \equiv -1 \Rightarrow \text{The order of } 5 \pmod{17} \text{ is } 16.$$

(b) $\phi(19) = 18$, the factors of 18 are: 9, 6, 3, 2:

$$2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^6 \equiv 7, \quad 2^9 \equiv 18 \equiv -1, \quad 2^{18} \equiv 1 \\ \Rightarrow \text{order of } 2 \pmod{19} \text{ is } 18.$$

$$3^2 \equiv 9, \quad 3^3 \equiv 8, \quad 3^6 \equiv 7, \quad 3^9 \equiv 1, \quad 3^{18} \equiv 1 \\ \Rightarrow \text{order of } 3 \pmod{19} \text{ is } 18.$$

$$5^2 \equiv 6, \quad 5^3 \equiv 11, \quad 5^6 \equiv 7, \quad 5^9 \equiv 1 \Rightarrow \\ \text{order of } 5 \pmod{19} \text{ is } 9.$$

(c) $\phi(23) = 22$. The factors are: 11, 2.

$$2^2 \equiv 4, \quad 2^{11} \equiv 1 \Rightarrow \text{order of } 2 \pmod{23} \text{ is } 11.$$

$$3^2 \equiv 9, \quad 3^{11} \equiv 1 \Rightarrow \text{order of } 3 \pmod{23} \text{ is } 11.$$

$$5^2 \equiv 2, \quad 5^{11} \equiv -1, \quad 5^{22} \equiv 1 \Rightarrow \text{order of } 5 \pmod{23} \text{ is } 22.$$

(12)

Sl. 1 #2

(a) Since a has order $hk \pmod n$,

$$a^{hk} \equiv 1 \pmod n.$$

$$\Rightarrow (a^h)^k \equiv 1 \pmod n.$$

Suppose $(a^h)^l \equiv 1 \pmod n$ for some $l \geq 1$.

Then $hk | hl$, hence $k | l$. Therefore $k \leq l$.

Therefore, a^h has order k .

(b) $a^{2k} \equiv 1 \pmod p$, and p is an odd prime,

$$\Rightarrow p | (a^k - 1)(a^k + 1).$$

Since $p \nmid a^k - 1$ (otherwise, a has order $\leq k \pmod p$),

$$p | a^k + 1. \text{ Hence } a^k \equiv -1 \pmod p.$$

(c) Proving by contradiction, we assume that

$n = d \cdot \beta$, $d, \beta > 1$. By Euler's Thm,

$$a^{\phi(n)} \equiv a^{\phi(d)\phi(\beta)} \equiv 1 \pmod n.$$

Thus a has order $\leq \phi(d)\phi(\beta) = \phi(n) < n-1$,

contradicting the assumption that a has order $n-1$. \square

Ex. 1 #12

(a) The candidates for the primitive roots of $10 = 2 \cdot 5$ are #'s that are relatively prime to 10:

$$3, 7, 9.$$

$$\phi(10) = \phi(2 \cdot 5) = 4.$$

$$3^2 \equiv -1, \quad 3^4 \equiv 1 \pmod{10} \Rightarrow 3 \text{ is a primitive root of } 10.$$

$$7^2 \equiv -1, \quad 7^4 \equiv 1 \pmod{10} \Rightarrow 7 \text{ is a primitive root of } 10.$$

Since $\phi(\phi(10)) = \phi(4) = 4 - 2 = 2$, 10 has two primitive roots 3 and 7.

(b) $\phi(17) = 16$, $\phi(16) = 8$. Therefore, 17 has 8 primitive roots, corresponding to 1, 3, 5, 7, 9, 11, 13, 15 — numbers that are relatively prime to 16.

$$3^1 \equiv 3, \quad 3^3 \equiv 10, \quad 3^5 \equiv 5, \quad 3^7 \equiv 11, \quad 3^9 \equiv 14,$$

$$3^9 \equiv 14, \quad 3^{11} \equiv 7, \quad 3^{13} \equiv 12, \quad 3^{15} \equiv 6 \text{ are}$$

the primitive roots of 17.

(14)

Ex. 2 #1

$$(a) \quad x^2 \equiv 1 \pmod{p} \Rightarrow p \mid x^2 - 1 = (x-1)(x+1)$$

$$\Rightarrow p \mid (x-1) \quad \text{or} \quad p \mid x+1.$$

$$\Rightarrow x = 1 + pm \quad \text{or} \quad x = (p-1) + mp.$$

Thus the only incongruent solutions are 1, $p-1$.

(b) By the Corollary of Lagrange's Thm,

$$x^{p-1} - 1 \equiv 0 \quad \text{has exactly } p-1 \text{ solutions.}$$

$$\text{Since } x^{p-1} - 1 = (x-1)(x^{p-2} + x^{p-3} + \dots + x + 1)$$

And by Lagrange's Thm,

$$x - 1 \equiv 0 \pmod{p}$$

$$\& \quad x^{p-2} + x^{p-3} + \dots + x + 1 \equiv 0 \pmod{p} \text{ has}$$

at most 1 & $p-2$ solutions respectively,

$$x^{p-2} + x^{p-3} + \dots + x + 1 \equiv 0 \pmod{p} \text{ has exactly } p-2 \text{ solutions.}$$

Ex. 2 #4

(a) The integers that has order 6 mod 43 are integers of the form

$$3^r, \quad \text{where } \gcd(r, \phi(43)) = \gcd(r, 42) = 6.$$

There are $\phi(6) = \phi(2)\phi(3) = 2$ such r 's: 7, 35.

$$3^7 \equiv 37, \quad 3^{35} \equiv 7 \pmod{43}.$$

Therefore, the answer is: 7, 37.

(15)

(b) The integers that has order 21 are of the form

$$3^r, \text{ where } \gcd(r, \phi(43)) = \gcd(r, 42) = 21.$$

There are $\phi(21) = \phi(3) \cdot \phi(7) = 2 \cdot 6 = 12$ of them:

$$r = 2, 4, 8, 10, 16, 20, 22, 26, 32, 34, 38, 40.$$

The corresponding integers are, after mod 43,

$$3^2 \equiv 9, \quad 3^4 \equiv 38, \quad 3^8 \equiv 25, \quad 3^{10} \equiv 10,$$

$$3^{16} \equiv 23, \quad 3^{20} \equiv 14, \quad 3^{22} \equiv 40, \quad 3^{26} \equiv 15,$$

$$3^{32} \equiv 13, \quad 3^{34} \equiv 31, \quad 3^{38} \equiv 17, \quad 3^{40} \equiv 24.$$

Ex. 2 # 6

(a) Since r has order $p-1 \pmod{p}$,

$$(r^{(p-1)/2})^2 \equiv 1 \pmod{p}$$

$$\text{and } r^{(p-1)/2} \not\equiv 1 \pmod{p} \quad \left. \vphantom{\begin{matrix} (r^{(p-1)/2})^2 \equiv 1 \pmod{p} \\ \text{and } r^{(p-1)/2} \not\equiv 1 \pmod{p} \end{matrix}} \right\} \Rightarrow p \mid r^{\frac{p-1}{2}} + 1$$

$$\text{Hence } r^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

(b) By (a), $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

$$r'^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

$$\text{Hence } (r \cdot r')^{\frac{p-1}{2}} \equiv (-1)(-1) \equiv 1 \pmod{p}$$

Therefore $r \cdot r'$ is NOT a primitive root.

(c) Suppose $(r')^k \equiv 1 \pmod{p}$, then

$$(r \cdot r')^k \equiv r^k \cdot 1 \equiv 1 \pmod{p}. \text{ Hence } p-1 \mid k. \text{ Therefore, } r' \text{ is a primitive root of } p.$$

(16)

Ex. 3 #1 (a) $26 = 2 \cdot 13 = 2p$, therefore it has primitive roots. $\phi(\phi(26)) = \phi(\phi(2) \cdot \phi(13)) = \phi(1 \cdot 12) = \phi(12) = \phi(3) \phi(2^2) = 2 \cdot 2 = 4$.

Hence there are 4 primitive roots of 26.

We can check that 2, 6, 7, 11 are primitive roots of $p=13$.

Since 7, 11 are odd, they are also primitive roots of $2p=26$.

For 2 and 6, $2+p=2+13=15$ & $6+p=19$ are primitive roots of $2p=26$.

Therefore, 26 has primitive roots 7, 11, 15, 19.

For $25 = 5^2$. There are $\phi(\phi(25)) = \phi(20) = \phi(2^2) \phi(5) = 2 \cdot 4 = 8$ primitive roots.

Since $2^{20} \equiv 1 \pmod{25}$
& $2^{10} \equiv -1 \pmod{25}$.

Therefore, 2 is the primitive root of 25. The a 's that are ≤ 25 and relatively prime to 25 are: 1, 3, 7, 9, 11, 13, 17, 19. Thus 25 has primitive roots:

$$2^1, 2^3 \equiv 8, 2^7 \equiv 3, 2^9 \equiv 12, 2^{11} \equiv 23, 2^{13} \equiv 17 \\ 2^{17} \equiv 23, 2^{19} \equiv 13 \pmod{25}.$$

(17)

(b) 2 is a primitive root of 3, and $2^2 \not\equiv 1 \pmod{3^2}$,

hence 2 is the primitive roots of 3^k , $k \geq 1$.

For 3^2 : $\phi(3^2) = 3^2 - 3 = 6$. $\phi(\phi(3^2)) = \phi(6) = \phi(2)\phi(3) = 2$.

The 2 primitive roots are:

$$2, 2^5 \equiv 5 \pmod{3^2}$$

For 3^3 : $\phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$. $\phi(\phi(3^3)) = \phi(18) = \phi(2)\phi(3^2) = 1 \cdot 6 = 6$

The 6 primitive roots are:

$$2, 2^5 \equiv 5, 2^7 \equiv 20, 2^{11} \equiv 23, 2^{13} \equiv 11, 2^{17} \equiv 14 \pmod{3^3}.$$

(H8)

Ex 3 #2

(a) The # of primitive roots of $2p^n$ is

$$\begin{aligned}\phi(\phi(2p^n)) &= \phi(\phi(2)\phi(p^n)) = \phi(1 \cdot (p^2 - p^{n-1})) \\ &= \phi(p^2 - p^{n-1}).\end{aligned}$$

The # of primitive roots of p^n is

$$\phi(\phi(p^n)) = \phi(p^n - p^{n-1}).$$

Hence these two #'s are the same.

(b) Let r be a primitive root of p^n . Then

r has order $\phi(p^n) = p^{n-1}(p-1) \pmod{p^n}$.

Assume that $r^h \equiv 1 \pmod{p}$. Then

$r^h \equiv 1 + ap \pmod{p^2}$ for some integer a . Hence

$$r^{ph} \equiv (1 + ap)^p \equiv 1 \pmod{p^2};$$

Similarly,

$$r^{p^{n-1}h} \equiv 1 \pmod{p^n}.$$

Therefore $h \mid p-1$. Hence r has order $p-1 \pmod{p}$, and r is a primitive root of p .

(c) Let r be a primitive root of p^2 . Since $\phi(p^2) = p(p-1)$.

Then $r^{p-1} \not\equiv 1 \pmod{p^2}$. Assume that r has order $k \pmod{p^n}$. Then

$$r^k \equiv 1 \pmod{p^n} \implies r^k \equiv 1 \pmod{p}.$$

Hence $p-1 \mid k$. On the other hand,

(149)

$k \mid \phi(p^n) = p^{n-1}(p-1)$. Hence $k = p^m(p-1)$, $0 \leq m \leq n-1$.

If $m \leq n-1$, then $k \mid p^{n-2}(p-1)$ and hence

$$r^{p^{n-2}(p-1)} \equiv 1 \pmod{p^n},$$

which contradicts to Lemma 2 in Section 8.3.

Ex. 3 #4

(a) $3^6 \equiv 1 \pmod{7}$

$$3^2 \equiv 2 \pmod{7}, \quad 3^3 \equiv -1 \pmod{7}$$

Hence 3 is a primitive root of 7.

Since $3^{7-1} = 3^6 \not\equiv 1 \pmod{7^2}$, we

know that 3 is also a primitive root of 7^n , $n \geq 1$.

Since 3 is odd, we know that 3 is a primitive root of $2 \cdot 7^n$, $n \geq 1$.

(b) First, we check that 3 is a primitive root of 17:

$$3^{\phi(17)} \equiv 3^{16} \equiv 1 \pmod{17}$$

$$3^8 \equiv -1 \pmod{17}.$$

Also $3^{16} \not\equiv 1 \pmod{17^2}$. Hence

3 is a primitive root for 17^n , $n \geq 1$.