8.3 Composite Numbers Having Primitive Roots

Note Title 3/10/2006

1. (a) Find the four primitive roots of 26 and the eight primitive roots of 25

Proof of Corollary to Th. 8.9 shows that if r is an odd primitive root of p^k, then it is a primitive root of $2p^k$.

$\therefore$ Since $26 = 2 \cdot 13$, find odd primitive roots of 13. There are $\phi(13-1) = \phi(12)$ incongruent primitive roots of 13.
$\phi(12) = (2^2-2)(3-1) = 4$

Check 2^{12}: By Euler's Th., $2^{\phi(13)} = 2^{12} \equiv 1 \pmod{13}$
Order of 2 mod 13 must divide 12 (Th. 8.1), and $2^1, 2^2, 2^3, 2^4, 2^5, 2^6 \not\equiv 1 \pmod{13}$.
$\therefore$ 2 is a primitive root of 13.

By Th. 8.3, other integers having order 12 mod 13 are powers of 2^k s.t. $\gcd(k, 12) = 1$
$\therefore k = 1, 5, 7, 11$.

$\therefore 2^1 \equiv 2, 2^5 \equiv 6, 2^7 \equiv 11, 2^{11} \equiv 7 \pmod{13}$.
So, four incongruent prim. roots of 13 are 2, 6, 7, 11.

$\therefore$ Four odd primitive roots of 13 are
$(2+13), (6+13), 7, 11$, or $7, 11, 15, 19$

$\therefore$ $\underline{7, 11, 15, 19}$ will be prim. roots for $2 \cdot 13 = 26$

For 25, $25 = 5^2$. Proof of Lemma 2 and Th. 8.9
Show if r is a primitive root of p s.t.
$r^{p-1} \not\equiv 1 \pmod{p^2}$, Then r is a prim. root of p^k.

$2^{5-1} = 16 \not\equiv 1 \pmod{5^2} \Rightarrow 2$ a prim. root of 25
since 2 is a prim. root of 5.

$\phi(25) = 5^2 - 5 = 20$
$\therefore$ Look at 2^k s.t. $\gcd(k, 20) = 1$.
$\therefore$ $k = 1, 3, 7, 9, 11, 13, 17, 19$ and $2^k \equiv 1 \pmod{25}$

$2^3 \equiv \underline{8}$, $2^7 = 128 \equiv \underline{3}$, $2^9 = 2^7 \cdot 2^2 \equiv \underline{12}$,
$2^{11} = 2^9 \cdot 2^2 \equiv 12 \cdot 4 = 48 \equiv \underline{23}$
$2^{13} = 2^{11} \cdot 2^2 \equiv 23 \cdot 4 = 92 \equiv \underline{17}$
$2^{17} = 2^9 \cdot 2^7 \cdot 2 \equiv 12 \cdot 3 \cdot 2 = 72 \equiv \underline{22}$
$2^{19} = 2^{17} \cdot 2^2 \equiv 22 \cdot 4 = 88 \equiv \underline{13}$

$\therefore$ Primitive roots of 25 : 2, 3, 8, 12, 13, 17, 22, 23

(8). Determine all the primitive roots of 3^2, 3^3, and 3^4.

Note 3^k has primitive roots by Th. 8.10

2 is a primitive root of 3
$\therefore$ either 2 or 2+3 will be primitive roots of 3^k, $k \geq 2$.

Since, if r is a prim. root of p, then order of $r \pmod{p^2}$ is $(p-1)$ or $p(p-1)$

$\therefore$ Order of $2 \pmod{3^2}$ is $(3-1)$ or $\phi(3^2)$
But $2^2 = 4 \not\equiv 1 \pmod{3^2}$, so $2^{\phi(3^2)} \equiv 1 \pmod{3^2}$,
so 2 is a primitive root of 3^2, 3^3, and 3^4

3^2: There are $\phi(\phi(3^2)) = \phi(6) = 2$ prim. roots
Since $\phi(3^2) = 6$, By Th. 8.3, 2^h will have order 6 $\Leftrightarrow$ $\gcd(h, 6) = 1$, or $h = 1, 5$
$\therefore 2^5 = 32 \equiv 5 \pmod{3^2}$
$\therefore$ primitive roots are $\underline{2, 5}$

3^3: $\phi(3^3) = 3^3 - 3^2 = 18$, $\phi(18) = 6$
$\therefore$ 6 prim. roots, and all are of form 2^k, s.t. $\gcd(k, 18) = 1$, or $k = 1, 5, 7, 11, 13, 17$
$2^5 = 32 \equiv \underline{5} \pmod{27}$

$2^7 \equiv 5 \cdot 2^2 = \underline{20} \pmod{27}$

$2^{11} \equiv 5 \cdot 5 \cdot 2 = 50 \equiv \underline{23} \pmod{27}$

$2^{13} \equiv 23 \cdot 2^2 = 92 \equiv \underline{11} \pmod{27}$

$2^{17} = 2^{11} \cdot 2^5 \cdot 2 \equiv 23 \cdot 5 \cdot 2 = 230 \equiv -40 \equiv \underline{14} \pmod{27}$

$\therefore$ prim. roots are 2, 5, 11, 14, 20, 23

3^4: $\phi(3^4) = 3^4 - 3^3 = 81 - 27 = 54 = 2 \cdot 3^3$

$\phi(54) = \phi(3^3) = 18$

$\therefore$ 18 primitive roots, all of form 2^k s.t. $\gcd(k, 54) = 1$.

$\therefore k = 1, 5, 5^2, 7, 7^2, 5 \cdot 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$

$\therefore 2^1 = \underline{2}$, $2^5 = \underline{32}$, $2^7 = 128 \equiv \underline{47}$

$2^{11} \equiv 47 \cdot 2^4 \equiv \underline{23}$, $2^{13} \equiv 23 \cdot 2^2 \equiv \underline{11}$

$2^{17} \equiv 11 \cdot 2^4 \equiv \underline{14}$, $2^{19} \equiv 14 \cdot 2^2 = \underline{56}$

$2^{23} \equiv 56 \cdot 2^4 \equiv \underline{5}$, $2^{29} \equiv 5 \cdot 2^5 \cdot 2 = 320 \equiv \underline{77}$

$2^{31} \equiv 77 \cdot 2^2 \equiv \underline{65}$, $2^{37} \equiv 65 \cdot 2^5 \cdot 2 \equiv \underline{29}$

$2^{41} \equiv 29 \cdot 2^4 \equiv \underline{59}$, $2^{43} \equiv 59 \cdot 2^2 \equiv \underline{74}$

$2^{47} \equiv 74 \cdot 2^4 \equiv \underline{50}$, $2^{53} \equiv 50 \cdot 2^6 \equiv \underline{41}$

$2^{5^2} = 2^{25} \equiv 5 \cdot 2^2 \equiv \underline{20}$, $2^{7^2} = 2^{49} \equiv 50 \cdot 4 \equiv \underline{38}$

$2^{5 \cdot 7} = 2^{35} \equiv 65 \cdot 2^4 \equiv \underline{68}$

$\therefore$ 2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, 65, 68, 74, 77 are prim. roots

2. For an odd prime p, establish:

(a) There are as many [incongruent] primitive roots of $2p^n$ as p^n

Pf: By Th. 8.9 and its corollary, p^n and $2p^n$ have prim. roots, where p is an odd prime and $n \geq 1$.

By corollary to Th. 8.4 (p.161), there are exactly $\phi(\phi(2p^n))$ prim. roots for $2p^n$, and exactly $\phi(\phi(p^n))$ prim. roots for p^n. (i.e., incongruent prim. roots).

For m, n s.t. $\gcd(m,n)=1$, $\phi(mn)=\phi(m)\phi(n)$, and $\gcd(2,p^n)=1$ since p is odd.

$\therefore \phi(2p^n) = \phi(2)\phi(p^n) = \phi(p^n)$ as $\phi(2)=1$.

$\therefore \phi(2p^n) = \phi(p^n) \Rightarrow \underline{\phi(\phi(2p^n)) = \phi(\phi(p^n))}$

Note also that proof of corollary to Th. 8.9 shows if r is an odd prim. root of p^k, it is also a prim. root of $2p^k$.
Similarly, if r is a primitive root of $2p^k$,

Then $\gcd(r, 2p^k) = 1$, r is odd.

If n is order of $r \pmod{p^k}$, Then $n \le \phi(p^k)$

Also, $r^n \equiv 1 \pmod{p^k} \Rightarrow r^n - 1 = xp^k$, some x.

But $r^n - 1$ is even, so $x = 2y$, some y,

so $r^n \equiv 1 \pmod{2p^k}$.

$\therefore n \ge \phi(2p^k) = \phi(p^k)$.

$\therefore n \ge \phi(p^k)$ and $n \le \phi(p^k) \Rightarrow n = \phi(p^k)$

$\therefore r$ is a primitive root of p^k.

So, if r is an even prim. root of p^k, Then choose r' to be $r + p^k$ so r' is odd and $\therefore$ a prim. root of $2p^k$.

(b) Any primitive root r of p^n is a primitive root of p.

Pf: $\gcd(r, p^n) = 1 \Rightarrow \gcd(r, p) = 1$.

Let k be order of $r \pmod{p}$

$\therefore r^k \equiv 1 \pmod{p}$

$\therefore k \mid \phi(p) \Rightarrow k \mid (p-1)$ [1]

Also, $r^k = 1 + sp$, some s.

So, for $n > 1$,

$$r^{kp^{n-1}} = (1+sp)^{p^{n-1}}$$

$$= 1 + \binom{p^{n-1}}{1} sp + \binom{p^{n-1}}{2}(sp)^2 + \dots + (sp)^{p^{n-1}}$$

But $p^{n-1} \mid \binom{p^{n-1}}{k}$, for $1 \le l < p^{n-1}$, and

$p \mid (sp)^k$, for $1 \le k \le p^{n-1}$.

$$\therefore p^n \mid \left[\binom{p^{n-1}}{1} sp + \binom{p^{n-1}}{2}(sp)^2 + \dots + (sp)^{p^{n-1}}\right]$$

$\therefore r^{kp^{n-1}} \equiv 1 \pmod{p^n}$

$\therefore$ Since r is a prim. root of p^n, then

$\phi(p^n) \mid kp^{n-1}$, by Th. 8.1.

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

$\therefore (p-1) \mid k$ [2]

[1] and [2] $\Rightarrow k = p-1$, so order of r mod p is $p-1$, so r is a prim. root of p.

(c) A primitive root of p^2 is also a prim. root of p^n for $n \geq 2$.

Pf: Let r be a primitive root of p^2.
By (b), r is also a prim. root of p.

Note $r^{p-1} \not\equiv 1 \pmod{p^2}$ since $\phi(p^2) = p(p-1)$ and r is a prim. root of p^2.

$\therefore$ r is a prim. root of p s.t. $r^{p-1} \not\equiv 1 \pmod{p^2}$, and proof to Th. 8.9 shows this r is a prim. root of p^n for $n \geq 1$

$\therefore$ This r is certainly a prim. root for p^n, $n \geq 2$.

3. If r is a primitive root of p^2, p being an odd prime, show that the solutions of the congruence $x^{p-1} \equiv 1 \pmod{p^2}$ are precisely the integers $r^p, r^{2p}, \ldots, r^{(p-1)p}$.

Pf: Note if x is a solution to $x^{p-1} \equiv 1 \pmod{p^2}$, then it is a solution to $x^{p-1} \equiv 1 \pmod{p}$, since $a \equiv b \pmod{p^2} \Rightarrow a \equiv b \pmod{p}$.

Corollary to Th. 8.5 says $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ solutions.

$\therefore x^{p-1} \equiv 1 \pmod{p^2}$ has at most $(p-1)$ solutions.

Note that for $k \geq 1$,

$(r^{kp})^{p-1} = (r^{p(p-1)})^k = (r^{\phi(p^2)})^k \equiv 1^k = 1 \pmod{p^2}$,
as r is a prim. root of p^2.

$\therefore$ The $p-1$ integers $r^p, \ldots, r^{(p-1)p}$ satisfy
$x^{p-1} \equiv 1 \pmod{p^2}$

Note that $r^p, r^{2p}, \ldots, r^{(p-1)p}$ are incongruent.
For let $r^{ap} \equiv r^{bp} \pmod{p^2}$ for $1 \leq a, b \leq p-1$,
$a \neq b$. Assume $a > b$ (same proof for $b > a$).
$\therefore r^{(a-b)p} \equiv 1 \pmod{p^2}$ contradicting
order of r as $p(p-1)$ since $a-b < p-1$.

$\therefore$ The $p-1$ integers $r^p, \ldots, r^{(p-1)p}$ are
incongruent solutions to $x^{p-1} \equiv 1 \pmod{p^2}$
and so are a complete set of solutions.

4. (a) Prove that 3 is a primitive root of all integers of the form 7^k and $2 \cdot 7^k$

Pf: $3^1 \not\equiv 1 \pmod 7$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$,
$3^6 \equiv 1 \pmod 7$

$\therefore 3^{\phi(7)} = 3^6 \equiv 1 \pmod 7$, and so
3 is a primitive root of 7.

$\therefore$ order of 3 mod 7^2 is $(7-1)$ or $7(7-1)$
But $3^4 = 81 \equiv 32 \pmod{7^2}$
$\therefore 3^6 \equiv 9 \cdot 32 \equiv 43 \pmod{7^2}$
$\therefore 3^6 \not\equiv 1 \pmod{7^2}$
$\therefore$ order of 3 $\pmod{7^2}$ is $7(7-1) = \phi(7^2)$

$\therefore$ Lemma 2 (p. 170) shows that for $k \geq 2$,
$$3^{7^{k-2}(7-1)} \not\equiv 1 \pmod{7^k}$$

And Th. 8.9 shows 3 is a prim. root of 7^k for $k \geq 1$.

Since 3 is an odd prim. root for 7^k, Corollary (p. 171) shows 3 is a prim. root of $2 \cdot 7^k$

[i.e., just need to show 3 a prim. root of p and $3^{p-1} \not\equiv 1 \pmod{p^2}$. Then 3 a prim. root of 7^k
For $2 \cdot 7^k$, now just need 3 is odd].

(6) Find a primitive root for any integer of the form 17^k.

Just need to find a prim. root r of 17 s.t. $r^{16} \not\equiv 1 \pmod{17^2}$.

Try 2: $2^4 = 16 \equiv -1 \pmod{17}$
$\therefore 2^8 \equiv 1 \pmod{17}$
$\therefore$ order of 2 mod 17 $\neq \phi(17)$

Try 3: $3^3 \equiv 10 \pmod{17}$
$3^4 \equiv -4 \pmod{17}$, $3^5 \equiv -12 \equiv 5$, $3^6 \equiv 15$
$3^7 \equiv -40 \equiv -6$, $3^8 \equiv -18 \equiv -1$, $3^9 \equiv -3$, $3^{10} \equiv -9$
$3^{11} \equiv -27 \equiv 7$, $3^{12} \equiv 21 \equiv 4$, $3^{13} \equiv 12$
$3^{14} \equiv 36 \equiv 2$, $3^{15} \equiv 6$
$\therefore 3^{16} \equiv 18 \equiv 1 \pmod{17}$

$\therefore$ 3 a primitive root of 17

$3^4 \equiv 81 \pmod{17^2}$, $3^8 \equiv 81^2 = 6561 \equiv 203$
$\therefore 3^{16} \equiv 203^2 = 41209 \equiv 171 \not\equiv 1 \pmod{17^2}$.

$\therefore$ 3 is a primitive root of 17^k, $k \geq 1$.

5. Obtain all the primitive roots of 41 and 82.

Table on p. 166 states 6 is a prim. root of 41.

Proof of Th. 8.4 shows all other primitive roots are congruent to one of $6^1, \ldots, 6^{40}$

41 has $\phi(\phi(41)) = \phi(40) = (2^3-2^2)(5-1) = 16$ incongruent prim. roots.

By Th. 8.3, since 6 has order 40, then 6^h has order $40/\gcd(h,40)$. $\therefore$ If $\gcd(h,40)=1$, then 6^h will have order 40, and $\therefore$ be a prim. root.

$\gcd(h,40)=1 \Rightarrow$

$h = 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39$

For 82, $\phi(82) = \phi(2 \cdot 41) = \phi(41)$

$\therefore$ 82 also has 16 prim. roots.

$\therefore$ if r is a prim. root of 41, then r or $r+41$, whichever is odd, will also be a prim. root of 82.

$\therefore$ For 41: $6^1 \equiv \underline{6}$, $6^3 \equiv \underline{11}$, $6^7 \equiv \underline{29}$, $6^9 \equiv \underline{19}$, $6^{11} \equiv \underline{28}$, $6^{13} \equiv \underline{24}$, $6^{17} \equiv \underline{26}$, $6^{19} \equiv \underline{34}$, $6^{21} \equiv \underline{35}$, $6^{23} \equiv \underline{30}$, $6^{27} \equiv \underline{12}$, $6^{29} \equiv \underline{22}$, $6^{31} \equiv \underline{13}$, $6^{33} \equiv \underline{17}$, $6^{37} \equiv \underline{15}$, $6^{39} \equiv \underline{7}$

$\therefore$ 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35

$\therefore$ For 82: 47, 7, 11, 53, 13, 15, 17, 19, 63, 65, 67, 69, 29, 71, 75, 35

or 7, 11, 13, 15, 17, 19, 29, 35, 47, 53, 63, 65, 67, 69, 71, 75

6. (a) Prove that a prim. root r of p^k, p an odd prime, is a prim. root of $2p^k \Leftrightarrow r$ is an odd integer.

(1) If r is odd, then $\gcd(r, 2p^k) = 1$. [1]
Let n be order of r mod $2p^k$.
$\therefore$ n must divide, (by Th. 8.1), $\phi(2p^k)$

But $\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$

by [1] and ϕ multiplicative

But $r^n \equiv 1 \pmod{2p^k} \Rightarrow r^n - 1 = a\,2p^k$, some a,
$\Rightarrow r^n - 1 = (2a)\,p^k$
$\Rightarrow r^n \equiv 1 \pmod{p^k}$.
But r a prim. root of $p^k \Rightarrow \phi(p^k) \mid n$ by Th. 8.1.

$\therefore$ $n \mid \phi(p^k)$ and $\phi(p^k) \mid n \Rightarrow n = \phi(p^k)$.

$\therefore$ odd r prim. root of $p^k \Rightarrow r$ a prim. root of $2p^k$

(2) Let r be a prim. root of p^k, p odd, and suppose r is also a prim. root of $2p^k$.
Then clearly $\gcd(r, 2p^k) = 1$, and since $2p^k$ is even, then r is odd.

(b) Confirm that $3, 3^3, 3^5$, and 3^9 are prim-roots of $578 = 2\cdot 17^2$, but that 3^4 and 3^{17} are not.

By 4(b), 3 is a prim. root of 17^2, and so by 6(a), is a prim root of $2\cdot 17^2$.

By Th. 8.3, 3^h will also have order $\phi(17^2)$ if $\gcd(h, \phi(17^2)) = 1$

But $\phi(17^2) = 17^2 - 17 = 17(16) = 2^4\cdot 17$

Since for $h = 1, 3, 5, 9$ $\gcd(h, 2^4\cdot 17) = 1$, Then $3^1, 3^3, 3^5, 3^9$ will also have order $\phi(17^2)$

$\therefore 3, 3^3, 3^5, 3^9$ are all prim. roots of 17^2, and are all odd, so by 6(a), are also prim. roots of $2\cdot 17^2$.

For 3^4, $\gcd(4, 2^4\cdot 17) = 4$, so order of 3^4 mod 17^2 is $\dfrac{\phi(17^2)}{4} = 2^2\cdot 17 \neq \phi(17^2)$

For 3^{17}, $\gcd(17, 2^4\cdot 17) = 17$, so order of 3^{17} mod 17^2 is $\dfrac{\phi(17^2)}{17} = 2^4 \neq \phi(17^2)$

$\therefore$ 3^4 and 3^{17} are not prim. roots of 17^2

The note written in problem 2(a) shows that if r is a prim. root of $2p^k$, then it is a prim. root of p^k.

$\therefore$ 3^4 and 3^{17} are not prim. roots of $2 \cdot 17^2$.

7. Assume r is a primitive root of the odd prime p and $(r+tp)^{p-1} \not\equiv 1 \pmod{p^2}$. Show $r+tp$ is a primitive root of p^k for each $k \geq 1$.

Pf; Since $r \equiv r+tp \pmod{p}$, then r and $r+tp$ have same order. $\therefore$ $r+tp$ is also a prim. root of p.

Since any prim. root of p has order mod p^2 of $(p-1)$ or $p(p-1)$, then $r+tp$ has order mod p^2 of $(p-1)$ or $p(p-1)$.

Since $(r+tp)^{p-1} \not\equiv 1 \pmod{p^2}$, order of $r+tp$ is not $(p-1)$, and so must be $p(p-1) = \phi(p^2)$.

$\therefore$ $r+tp$, a prim. root of p, is also a prim. root of p^2, and the proof of Lemma 2 and Th. 8-9 show that $r+tp$ is a prim. root of p^k, $k \geq 1$.

8. If $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n>1$, define the universal exponent $\lambda(n)$ of n by

$$\lambda(n) = \mathrm{lcm}\left(\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r})\right)$$

where $\lambda(2) = 1$, $\lambda(2^2) = 2$, $\lambda(2^k) = 2^{k-2}$ for $k \geq 3$. Prove the following statements concerning the universal exponent:

(a) For $n = 2, 4, p^k, 2p^k$, where p is an odd prime, $\lambda(n) = \phi(n)$

Pf: $\lambda(2) = 1$ by def., $\phi(2) = 2^1 - 2^0 = 1$ by Th. 7.3
$\lambda(4) = \lambda(2^2) = 2$ by def., $\phi(2^2) = 2^2 - 2^1 = 2$

For $n = 2p^k$, note $\mathrm{lcm}(1, x) = x$.

$$\lambda(n) = \mathrm{lcm}(\lambda(2), \phi(p^k)) = \mathrm{lcm}(1, \phi(p^k)) = \phi(p^k) = \phi(n)$$

For $n = p^k$, $\lambda(n) = \text{lcm}(\phi(p^k)) = \phi(p^k) = \phi(n)$

(b) If $\gcd(a, 2^k) = 1$, then $a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$

Pf: By Euler's Th., $a^{\phi(2^k)} \equiv 1 \pmod{2^k}$

$\phi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$

For $k=1$, $\phi(2^k) = 1 = \lambda(2^k)$

$k=2$, $\phi(2^k) = 2 = \lambda(2^2) = \lambda(2^k)$

$\therefore$ For $k = 1, 2$, $a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$

For $k \geq 3$, $\lambda(2^k) = 2^{k-2}$

Proof of Th. 8.3 showed for $k \geq 3$,

$\underline{\underline{a^{2^{k-2}}}} \equiv 1 \pmod{2^k}$. $\therefore a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$

Alternatively, $\lambda(2^{k+1}) = 2^{(k+1)-2} = 2^{k-1}$

$= 2 \cdot 2^{k-2} = 2\lambda(2^k)$

for $k \geq 3$.

$\therefore$ Using induction, have proved true for $k = 1, 2$.

Assume true for $k = 3$

$$\therefore a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$$

$$\therefore a^{\lambda(2^k)} = 1 + r2^k$$

$$\therefore a^{2\lambda(2^k)} = (1 + r2^k)^2$$

$$\therefore a^{\lambda(2^{k+1})} = 1 + 2r2^k + r^2 2^{2k}$$

$$= 1 + r2^{k+1} + r^2 2^{k-1} \cdot 2^{k+1}$$

$$= 1 + (r + r^2 \cdot 2^{k-1}) 2^{k+1}$$

$$\therefore a^{\lambda(2^{k+1})} \equiv 1 \pmod{2^{k+1}}$$

$\therefore$ true for all k.

(c) If $\gcd(a, n) = 1$, then $a^{\lambda(n)} \equiv 1 \pmod{n}$

Pf: Let $n = p^k$, p odd. $\therefore \lambda(n) = \phi(n)$ by (a).

$$\therefore a^{\lambda(n)} = a^{\phi(n)} \equiv 1 \pmod{n}, \text{ by Euler's Th.}$$

Note that by corollary 2, p. 24,

if $\left.\begin{array}{l} c \equiv 0 \pmod{p_1} \\ c \equiv 0 \pmod{p_2} \end{array}\right\}$, then $c \equiv 0 \pmod{p_1 p_2}$, where $\gcd(p_1, p_2) = 1$.

$\therefore$ if $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, then by (b) & (c),

$$a^{\lambda(2^{k_0})} \equiv 1 \pmod{2^{k_0}}$$

$$\therefore a^{\mathrm{lcm}[\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r})]} \equiv 1 \pmod{2^{k_0}}$$

since $\lambda(2^{k_0}) \mid \mathrm{lcm}[\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r})]$

$$\therefore a^{\lambda(n)} \equiv 1 \pmod{2^{k_0}} \quad [1]$$

(or $a^{\lambda(n)} - 1 \equiv 0 \pmod{2^{k_0}}$)

$$a^{\lambda(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}$$

$$\therefore a^{\mathrm{lcm}[\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r})]} \equiv 1 \pmod{p_i^{k_i}}$$

since $\lambda(p_i^{k_i}) \mid \mathrm{lcm}[\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r})]$

as $\lambda(p_i^{k_i}) = \phi(p_i^{k_i})$ by (a)

$$\therefore a^{\lambda(n)} \equiv 1 \pmod{p_i^{k_i}} \quad [2]$$

(or, $a^{\lambda(n)} - 1 \equiv 0 \pmod{p_i^{k_i}}$)

$\therefore$ By [1] & [2], $a^{\lambda(n)} \equiv 1 \pmod{n}$

9. Verify that, for $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, $\lambda(5040) = 12$ and $\phi(5040) = 1152$.

By def. in #8, $\lambda(5040) = \operatorname{lcm}(\lambda(2^4), \phi(3^2), \phi(5), \phi(7))$

$$= \operatorname{lcm}(2^2, 3^2 - 3, 4, 6)$$

$$= \operatorname{lcm}(2^2, 2\cdot 3, 2^2, 2\cdot 3) = 2^2 \cdot 3 = \underline{12}$$

$$\phi(5040) = (2^4 - 2^3)\cdot(3^2 - 3)(4)(6)$$
$$= (8)(6)(4)(6) = \underline{1152}$$

10. Use Problem 8 to show that if $n \neq 2, 4, p^k, 2p^k$, where p is an odd prime, Then n has no primitive root.

Pf: Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ be The prime factorization

Note from Th. 2.8, $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$.
$\therefore \operatorname{lcm}(a,b) \mid ab$ and $\operatorname{lcm}(a,b) \leq ab$.

If $k_0 \neq 0$, Then since $n \neq 2, 4$, or $2p^k$, Then $k_0 \geq 3$, so $\lambda(2^{k_0}) = 2^{k_0 - 2} < 2^{k_0 - 1} = \phi(2^{k_0})$
$\therefore \lambda(2^{k_0}) = \frac{1}{2}\phi(2^{k_0})$
$\therefore \lambda(n) = \operatorname{lcm}(\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$

$= \operatorname{lcm}(2^{k_0-2}, \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$

$< \operatorname{lcm}(2^{k_0-1}, \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$, by prob. #1, section 6.1

$= \operatorname{lcm}(\phi(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$

$\leq \phi(n)$

$\therefore \lambda(n) < \phi(n)$, and from 8.(c),

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

$\therefore$ n has no primitive root for $k_0 \neq 0$.

If $k_0 = 0$, then $\lambda(n) = \operatorname{lcm}(\phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$

Each $\phi(p_i^{k_i})$ is even, and $r > 1$ (i.e., more than one prime factor).

$\therefore$ let $\phi(p_i^{k_i}) = 2s_i$

$\therefore \gcd(\phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r})) = \gcd(2s_1, \ldots, 2s_r) \geq 2$

$\therefore \operatorname{lcm}(\phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r})) \cdot \gcd(\phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$

$\geq 2 \operatorname{lcm}(\phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$

$\therefore$ Since $\gcd(a,b)\cdot \operatorname{lcm}(a,b) = ab$, then

$$\phi(n) = \phi(p_1^{k_1})\cdots\phi(p_r^{k_r}) \geq 2\operatorname{lcm}(\phi(p_1^{k_1}),\dots,\phi(p_r^{k_r}))$$
$$> \operatorname{lcm}(\phi(p_1^{k_1}),\dots,\phi(p_r^{k_r}))$$
$$= \lambda(n)$$

$\therefore$ $\lambda(n) < \phi(n)$ for $k_0 = 0$, and from 8.(c),

$a^{\lambda(n)} \equiv 1 \pmod{n}$.

$\therefore$ for $n \neq 2, 4, p^k, 2p^k$, $\lambda(n) < \phi(n)$,

and $a^{\lambda(n)} \equiv 1 \pmod{n}$.

$\therefore$ n has no primitive root.

11. (a) Prove that if $\gcd(a,n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has the solution $x \equiv b\,a^{\lambda(n)-1} \pmod{n}$.

Pf: By 8.(c), $a^{\lambda(n)} \equiv 1 \pmod{n}$, so

$$b\,a^{\lambda(n)} \equiv b \pmod{n}$$

$\therefore b \cdot a \cdot a^{\lambda(n)-1} \equiv b \pmod{n}$

$\therefore a\left(b a^{\lambda(n)-1}\right) \equiv b \pmod{n}$

$\therefore x \equiv b a^{\lambda(n)-1} \pmod{n}$ is a solution.

(b) Use part (a) to solve $13x \equiv 2 \pmod{40}$ and $3x \equiv 13 \pmod{77}$

$13x \equiv 2 \pmod{40}$. Note $\gcd(13, 40) = 1$.

$\therefore$ By (a) $x \equiv 2 \cdot 13^{\lambda(40)-1}$

Since $40 = 2^3 \cdot 5$, $\lambda(40) = \operatorname{lcm}(\lambda(2^3), \phi(5))$
$= \operatorname{lcm}(2, 4) = 4$.

$\therefore x \equiv 2 \cdot 13^3 \pmod{40}$, $2 \cdot 13^3 = 4394$
$4394 \equiv 34 \pmod{40}$.

$\therefore \underline{x \equiv 2 \cdot 13^3 \equiv 34 \pmod{40}}$

$3x \equiv 13 \pmod{77}$. Note $\gcd(3, 77) = 1$.

$\therefore$ By (a), $x \equiv 13 \cdot 3^{\lambda(77)-1}$

$77 = 7 \cdot 11$, so $\lambda(n) = \operatorname{lcm}(\phi(7), \phi(11))$

$$= \mathrm{lcm}(6, 10) = 30$$

$$\therefore\ x \equiv 13 \cdot 3^{29} \pmod{77}$$

$$3^4 \equiv 4,\quad 3^8 \equiv 16,\quad 3^{12} \equiv 64,\quad 3^{24} \equiv 4096 \equiv 15$$

$$3^{28} \equiv 60,\quad 3^{29} \equiv 180 \equiv 26,\quad 13 \cdot 3^{29} \equiv 13 \cdot 26$$

$$= 338 \equiv 30$$

$$\underline{\therefore\ x \equiv 13 \cdot 3^{29} \equiv 30 \pmod{77}}$$