8.3

1(a) primitive roots of $26 = 2 \cdot 13$:

Note that 2 is a primitive root of 13:

$2 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^6 \equiv 12 \equiv -1 \Longrightarrow 2^{12} = 2^{\varphi(13)} \equiv 1 \pmod{13}$.

Then the primitive roots of 13 are $\equiv \{2, 2^5, 2^7, 2^{11}\} \equiv \{2, 6, 11, 7\}$ modulo 13. It follows that 7, 11, $2+13=15$, and $6+13=19$ are the 4 primitive roots of 26.

primitive roots of 25:

2 is a primitive root of 5, since $2 \equiv 2,\ 2^2 \equiv 4 \equiv -1,\ 2^4 \equiv 1 \pmod 5$.
The primitive roots of 5 are then $\{2, 2^3\} \equiv \{2, 3\}$. Now check the candidates for primitive roots of 25:

$2^4 \not\equiv 1 \pmod{25}$ ✓
$3^4 \not\equiv 1 \pmod{25}$ ✓
$7^4 \equiv 1 \pmod{25}$ ✗
$8^4 \not\equiv 1 \pmod{25}$ ✓

$12^2 = 144 \equiv -6 \Rightarrow 12^4 \not\equiv 1$ ✓
$13^2 \equiv -6 \Longrightarrow 13^4 \not\equiv 1$ ✓
$17^2 = 289 \equiv -11 \Rightarrow 17^4 \not\equiv 1$ ✓
$18^2 = 324 \equiv -1 \Longrightarrow 18^4 \equiv 1$ ✗

$22^2 \equiv 9 \Rightarrow 22^4 \not\equiv 1$ ✓
$23^2 \equiv 4 \Longrightarrow 23^4 \not\equiv 1$ ✓

Answer:
$\{2, 3, 8, 12, 13, 17, 22, 23\}$

1(b) <u>primitive roots of</u> 3^2:

2 is a primitive root of 3 with $2^2 \not\equiv 1 \pmod 9$; $5^2 \not\equiv 1 \pmod 9$, $8^2 \equiv 1 \pmod 9$. Thus, $\{2, 5\}$ are the primitive roots of 9.

<u>primitive roots of</u> $3^3 = 27$: In addition to 2 and 5, check:

$8^2 \equiv 1 \pmod 9$ ×

$11^2 \not\equiv 1 \pmod 9$ ✓

$14^2 \not\equiv 1 \pmod 9$ ✓

$17^2 \equiv 1 \pmod 9$ ×

$20^2 \not\equiv 1 \pmod 9$ ✓

$23^2 \not\equiv 1 \pmod 9$ ✓

$26^2 \equiv 1 \pmod 9$ ×

<u>Answer</u>: $\{2, 5, 11, 14, 20, 23\}$

i.e., $\{2+9k, 5+9k\}$

<u>primitive roots of</u> 81: Keep checking:

$29^2 \not\equiv 1 \pmod 9$ ✓

$32^2 \not\equiv 1$ ✓

$35^2 \equiv 1$ ×

$38^2 \not\equiv 1$ ✓

$41^2 \not\equiv 1$ ✓

$44^2 \equiv 1$ ×

$47^2 \not\equiv 1$ ✓

$50^2 \not\equiv 1$ ✓

$53^2 \equiv 1$ ×

$56^2 \not\equiv 1$ ✓

$59^2 \not\equiv 1$ ✓

$62^2 \equiv 1$ ×

$65^2 \not\equiv 1$ ✓

$68^2 \not\equiv 1$ ✓

$71^2 \equiv 1$ ×

$74^2 \not\equiv 1$ ✓

$77^2 \not\equiv 1$ ✓

$80^2 \equiv 1$ ×

<u>Answer</u>:

2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, 65, 68, 74, 77, i.e., $\{2+9k, 5+9k\}$

<u>8</u> $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r} \implies \lambda(n) := \operatorname{lcm}\{\lambda(2^{k_0}), \varphi(p_1^{k_1}), \ldots, \varphi(p_r^{k_r})\}$

(a) $n = 2, 4, p^k, 2p^k \implies \lambda(n) = \varphi(n)$

Just compute: $\lambda(2) = 1 = \varphi(2)$ ✓ $\quad \lambda(p^k) = \varphi(p^k)$ ✓

$\lambda(4) = 2 = \varphi(4)$ ✓ $\quad \lambda(2p^k) = \operatorname{lcm}\{\lambda(2), \varphi(p^k)\}$

$= \varphi(p^k) = \varphi(2p^k)$ ✓

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

<u>pf. via induction</u>: base case is trivial, since $\gcd(a,2) = 1 \implies a \equiv 1 \pmod 2$

Suppose that $\gcd(a, 2^k) = 1 \implies a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$ for some $k \geq 1$.

Then $2^k \mid a^{\lambda(2^k)} - 1$ & $2 \mid a^{\lambda(2^k)} + 1$, since a is odd,

so $2^{k+1} \mid (a^{\lambda(2^k)} - 1)(a^{\lambda(2^k)} + 1) = a^{2\lambda(2^k)} - 1 = a^{\lambda(2^{k+1})} - 1$,

i.e., $a^{\lambda(2^{k+1})} \equiv 1 \pmod{2^{k+1}}$. $\boxtimes$

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

Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$. Since $\gcd(a,n)=1$, $\gcd(a,p)=1$ for all primes $p \mid n$ and Euler $\implies a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$. For odd primes p, $\varphi(p^k) \mid \lambda(n)$, so this says that $a^{\lambda(n)} \equiv 1 \pmod{p^k}$; part (b) guarantees that $a^{\lambda(2^{k_0})} \equiv 1 \pmod{2^{k_0}} \implies a^{\lambda(n)} \equiv 1 \pmod{2^{k_0}}$.

It follows that $a^{\lambda(n)} \equiv 1 \pmod{n}$. $\blacksquare$

<u>10</u> $n \neq 2, 4, p^k, 2p^k$ (p an odd prime) $\Longrightarrow$ n has no primitive root.

<u>pf.</u> : If $n \neq 2, 4, p^k$, or $2p^k$, then $\lambda(n) \neq \varphi(n)$; in fact,

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

$$= \mathrm{lcm}\{\mathrm{lcm}\{\lambda(2^{k_0}), \varphi(p_1^{k_1})\}, \varphi(p_2^{k_2}), \ldots, \varphi(p_r^{k_r})\}$$

$$= \mathrm{lcm}\left\{\frac{\lambda(2^{k_0})\varphi(p_1^{k_1})}{d_1}, \varphi(p_2^{k_2}), \ldots, \varphi(p_r^{k_r})\right\} \qquad d_1 = \gcd(\lambda(2^{k_0}), \varphi(p_1^{k_1}))$$

$$= \mathrm{lcm}\left\{\mathrm{lcm}\left\{\frac{\lambda(2^{k_0})\varphi(p_1^{k_1})}{d_1}, \varphi(p_2^{k_2})\right\}, \varphi(p_3^{k_3}), \ldots, \varphi(p_r^{k_r})\right\}$$

$$= \mathrm{lcm}\left\{\frac{\lambda(2^{k_0})\varphi(p_1^{k_1})\varphi(p_2^{k_2})}{d_1 d_2}, \varphi(p_3^{k_3}), \ldots, \varphi(p_r^{k_r})\right\},$$

$$d_2 = \gcd\left(\frac{\lambda(2^{k_0})\varphi(p_1^{k_1})}{d_1}, \varphi(p_2^{k_2})\right)$$

$$= \cdots = \frac{\lambda(2^{k_0})\varphi(p_1^{k_1})\cdots\varphi(p_r^{k_r})}{d_1 d_2 \cdots d_r} \quad \#$$

$= \dfrac{\varphi(n)}{D}$, where D is even.

Thus, $\lambda(n) = \dfrac{\varphi(n)}{2m} \implies \lambda(n) \,\Big|\, \dfrac{\varphi(n)}{2}$ as in the hint.

By part (b), $\gcd(a,n) = 1 \implies a^{\lambda(n)} \equiv 1 \pmod{n}$

$\implies a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$

$\implies$ order of a is $< \varphi(n)$, so

a cannot be a primitive root of n.

$\boxtimes$

8.4 **2** Note that 2 is a primitive root of 11. Now compute:

$2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 5$, $2^5 \equiv 10$, $2^6 \equiv 9$, $2^7 \equiv 7$,

$2^8 \equiv 3$, $2^9 \equiv 6$, $2^{10} \equiv 1$. Index table:

a	1	2	3	4	5	6	7	8	9	10
ind a	10	1	8	2	4	9	7	3	6	5

(a) $7x^3 \equiv 3 \pmod{11}$

$\mathrm{ind}\,7 + 3\,\mathrm{ind}\,x \equiv \mathrm{ind}\,3 \pmod{10}$

$3\,\mathrm{ind}\,x \equiv 1 \pmod{10}$: $\underline{1 \text{ sol'n}}$

$3\,\mathrm{ind}\,x = 10k + 1$

$k = 2 \Longrightarrow \mathrm{ind}\,x = 7$

$\Longrightarrow \underline{\underline{x = 7}}$

(b) $3x^4 \equiv 5 \pmod{11}$

$\mathrm{ind}\,3 + 4\,\mathrm{ind}\,x \equiv \mathrm{ind}\,5 \pmod{10}$

$4\,\mathrm{ind}\,x \equiv -4 \equiv 6 \pmod{10}$: 2 sol'ns

$2\,\mathrm{ind}\,x \equiv 3 \pmod{5}$

$2\,\mathrm{ind}\,x = 5k + 3$

$k = 1 \Longrightarrow \mathrm{ind}\,x = 4 \Longrightarrow \underline{\underline{x = 5}}$

$k = 3 \Longrightarrow \mathrm{ind}\,x = 9 \Longrightarrow \underline{\underline{x = 6}}$

(c) $x^8 \equiv 10 \pmod{11} \Longleftrightarrow 8\,\mathrm{ind}\,x \equiv 5 \pmod{10}$: no sol'n since $2 \nmid 5$.

6 Compute: $5^1 \equiv 5$, $5^2 \equiv 8$, $5^3 \equiv 6$, $5^4 \equiv 13$, $5^5 \equiv 14$,
mod 17
$5^6 \equiv 2$, $5^7 \equiv 10$, $5^8 \equiv 16$, $5^9 \equiv 12$, $5^{10} \equiv 9$,
$5^{11} \equiv 11$, $5^{12} \equiv 4$, $5^{13} \equiv 3$, $5^{14} \equiv 15$, $5^{15} \equiv 7$, $5^{16} \equiv 1$.

Index table

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ind a	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

$x^{12} \equiv 13 \pmod{17}$

~~12 indx ≡~~

$12 \,\text{ind}\, x \equiv 4 \pmod{16}$
4 sol'ns

$3 \,\text{ind}\, x \equiv 1 \pmod 4$

$3 \,\text{ind}\, x = 4k+1$

$k=2 \Rightarrow \text{ind}\, x = 3$
$\underline{x=6}$

$k=5 \Rightarrow \text{ind}\, x = 7$
$\underline{x=10}$

$k=8 \Rightarrow \text{ind}\, x = 11$
$\underline{x=11}$

$k=11 \Rightarrow \text{ind}\, x = 15$
$\underline{x=7}$

$8x^5 \equiv 10 \pmod{17}$

$\text{ind}\, 8 + 5 \,\text{ind}\, x \equiv \text{ind}\, 10 \pmod{16}$

$5 \,\text{ind}\, x \equiv 5 \pmod{16}$
1 sol'n

$\text{ind}\, x \equiv 1 \pmod{16}$
$\underline{x=5}$

$9x^8 \equiv 8 \pmod{17}$

$\text{ind}\, 9 + 8 \,\text{ind}\, x \equiv \text{ind}\, 8 \pmod{16}$

$8 \,\text{ind}\, x \equiv 8 \pmod{16}$
8 sol'ns!

$\text{ind}\, x \equiv 1 \pmod 2$

$\text{ind}\, x = 1, 3, 5, 7, 9, 11, 13, 15$

$x = 5, 6, 14, 10, 12, 11, 7, 3$

$7^x \equiv 7 \pmod{17} \iff x \,\text{ind}\, 7 \equiv \text{ind}\, 7 \pmod{16}$

$\Rightarrow x \equiv 1 \pmod{16}$

$\Rightarrow x = 1$

<u>12</u> $x^5 \equiv 13 \pmod{23} \iff 5 \,\mathrm{ind}\, x \equiv \mathrm{ind}\, 13 \pmod{22}$

Since $\gcd(5, 22) = 1$ and $1 \mid \mathrm{ind}\, 13$, this congruence has a unique solution. $(x = 3)$

$x^7 \equiv 15 \pmod{29} \iff 7 \,\mathrm{ind}\, x \equiv \mathrm{ind}\, 15 \pmod{28}$

Since $\gcd(7, 28) = 7$, we have to determine whether $7 \mid \mathrm{ind}\, 15$. It turns out that 2 is a primitive root of 29 and $\mathrm{ind}_2 15 = 27$ — $7 \nmid \mathrm{ind}\, 15$, so this congruence has no solution.

12 $\quad x^5 \equiv 13 \pmod{23}$

$\Longleftrightarrow \quad 5\,\mathrm{ind}\,x \equiv \mathrm{ind}\,13 \pmod{22}$ $\qquad \gcd(5,22)=1$

primitive root : 5

$5^1 = 5,\ 5^2 \equiv 2,\ 5^3 \equiv 10,$

$5^4 \equiv 4,\ 5^5 \equiv 20,\ 5^6 \equiv 8,$

$5^7 \equiv 17,\ 5^8 \equiv 16,\ 5^9 \equiv 11,$

$5^{10} \equiv 9,\ 5^{11} \equiv 22,\ 5^{12} \equiv 18,$

$\cancel{5^{13} \equiv 8},\ 5^{14}$

$x^7 \equiv 15 \pmod{29}$

$\Longleftrightarrow \quad 7\,\mathrm{ind}\,x \equiv \mathrm{ind}\,15 \pmod{28}$

$\boxed{\text{need } 7 \mid \mathrm{ind}\,15} \rightarrow$ No!

2 is a primitive root for 29

ind	2	ind	a
1	2	16	25
2	4	17	21
3	8	18	13
4	16	19	26
5	3	20	23
6	6	21	17
7	12	22	5
8	24	23	10
9	19	24	20
10	9	25	11
11	18	26	22
12	7	27	15
13	14		
14	28		
15	27		

15 Let r be a primitive root of the odd prime p.

Then $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ and $r^{\operatorname{ind} a + \frac{p-1}{2}} \equiv a \cdot (-1) = -a$

$\equiv p - a \pmod{p}$.

Also, $r^{\operatorname{ind}(p-a)} \equiv p - a \pmod{p}$, so $r^{\operatorname{ind}(p-a)} \equiv r^{\operatorname{ind} a + \frac{p-1}{2}} \pmod{p}$

$\Longleftrightarrow \operatorname{ind}(p-a) \equiv \operatorname{ind} a + \frac{p-1}{2} \pmod{p-1}$.

$\square$