7.2 **10** If every prime that divides n also divides m, then $\varphi(nm) = n\varphi(m)$.

Let $n = p_1^{k_1} \cdots p_r^{k_r}$ and $m = p_1^{j_1} \cdots p_r^{j_r} Q$, ~~where~~ and $p_i \nmid Q$ for any i. Then

$$\begin{aligned}
\varphi(nm) &= \varphi(p_1^{k_1+j_1} \cdots p_r^{k_r+j_r} Q) \\
&= \varphi(p_1^{k_1+j_1}) \cdots \varphi(p_r^{k_r+j_r})\varphi(Q) \\
&= (p_1^{k_1+j_1} - p_1^{k_1+j_1-1}) \cdots (p_r^{k_r+j_r} - p^{k_r+j_r-1})\varphi(Q) \\
&= p_1^{k_1}(p_1^{j_1} - p_1^{j_1-1}) \cdots p_r^{k_r}(p_r^{j_r} - p_r^{j_r-1})\varphi(Q) \\
&= p_1^{k_1} \cdots p_r^{k_r}(p_1^{j_1} - p_1^{j_1-1}) \cdots (p_r^{j_r} - p_r^{j_r-1})\varphi(Q) \\
&= n\varphi(m).
\end{aligned}$$

∎

<u>Corollary</u>: $\varphi(n^2) = n\varphi(n) \ \forall \ n \in \mathbb{N}$.

11(a) $\varphi(n) \mid n-1 \implies n$ is square-free.

Let $n = p_1^{k_1} \cdots p_r^{k_r}$, so that $\varphi(n) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1})$.

If the exponent $k_i > 1$, then $p_i \mid \varphi(n) \implies p_i \mid n-1$, which clearly cannot happen. Thus, $k_i = 1 \ \forall i$ and n is square-free.

11(b) $n = 2^k$ or $n = 2^k 3^j \implies \varphi(n) \mid n$.

Compute :

$$\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1} \mid 2^k \implies \varphi(n) \mid n. \checkmark$$

$$\begin{aligned}
\varphi(2^k 3^j) &= \varphi(2^k)\varphi(3^j) \\
&= (2^k - 2^{k-1})(3^j - 3^{j-1}) \\
&= \underbrace{2^{k-1}} \cdot \underbrace{3^{j-1}(2)} \\
&= 2^k 3^{j-1} \mid 2^k 3^j \implies \varphi(n) \mid n. \checkmark
\end{aligned}$$

13 $d \mid n \implies \varphi(d) \mid \varphi(n)$

Let $n = p_1^{k_1} \cdots p_r^{k_r}$, so that $d = p_1^{j_1} \cdots p_r^{j_r}$ for $j_i \le k_i$, $1 \le i \le r$.

Then $\varphi(d) = (p_1^{j_1} - p_1^{j_1 - 1}) \cdots (p_r^{j_r} - p_r^{j_r - 1})$, and we have

$$\varphi(d) \cdot p_1^{k_1 - j_1} \cdot \ldots \cdot p_r^{k_r - j_r} = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1})$$

$$= \varphi(n),$$

so $\varphi(d) \mid \varphi(n)$. $\blacksquare$

7.3 9 $2^{100,000} \pmod{77}$:

$77 = 7 \cdot 11$, so $\varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$

Euler's Thm. $\Longrightarrow 2^{60} \equiv 1 \pmod{77} \Longrightarrow (2^{60})^{1666} \equiv 1 \pmod{77}$

$$\Longrightarrow 2^{99,960} \equiv 1 \pmod{77}.$$

It remains to compute $2^{40} \pmod{77}$:

$$2^{10} = 1024 \equiv 23 \pmod{77}$$

$$\Longrightarrow \quad 2^{20} \equiv 529 \equiv 67 \equiv -10 \pmod{77}$$

$$\Longrightarrow \quad 2^{40} \equiv 100 \equiv 23 \pmod{77}.$$

Thus, $2^{100,000} \equiv 23 \pmod{77}$.

10 For any integer a, $a^{4n+1} \equiv a \pmod{10}$.

Case 1: $\gcd(a, 10) = 1$

Euler $\Longrightarrow a^{\varphi(10)} \equiv 1 \pmod{10}$, $\varphi(10) = \varphi(2)\varphi(5) = 4$

$\Longrightarrow a^4 \equiv 1 \pmod{10} \Longrightarrow a^{4n} \equiv 1 \pmod{10}$

$\Longrightarrow a^{4n+1} \equiv a \pmod{10}$.

Case 2: $10 \mid a$ easy!

Case 3: $5 \mid a$, $2 \nmid a$

$a^{4n+1} - a = a(a^{4n} - 1)$: a ends in 5, $a^{4n} - 1$ ends in 4,

so $a(a^{4n} - 1)$ ends in 0.

Case 4: $2 \mid a$, $5 \nmid a$

$a^{4n+1} - a$ is even!

Euler $\Longrightarrow a^{\varphi(5)} \equiv 1 \pmod{5} \Longrightarrow a^4 \equiv 1 \pmod{5}$

$\Longrightarrow a^{4n+1} \equiv a \pmod{5} \Longrightarrow a^{4n+1} \equiv a \pmod{10}$.

12 (a) Compute:

$-31 \equiv 5 \pmod 9$, $-16 \equiv 2 \pmod 9$, $-8 \equiv 1 \pmod 9$,

$13 \equiv 4 \pmod 9$, $25 \equiv 7 \pmod 9$, $80 \equiv 8 \pmod 9$, so

$\{-31, -16, -8, 13, 25, 80\} \equiv \{1, 2, 4, 5, 7, 8\} \bmod 9$ ✓

(Note: $\varphi(9) = 6$)

(b) Compute:

$3 \equiv 3 \pmod{14}$, $3^2 \equiv 9 \pmod{14}$, $3^3 \equiv 13 \pmod{14}$,

$3^4 \equiv 11 \pmod{14}$, $3^5 \equiv 5 \pmod{14}$, $3^6 \equiv 1 \pmod{14}$, so

$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\} \equiv \{1, 3, 5, 9, 11, 13\} \bmod 14$. ✓

(Note: $\varphi(14) = 6$)

<u>12(c)</u> Since $\varphi(27) = 3^3 - 3^2 = 18$, Euler $\Longrightarrow 2^{18} \equiv 1 \pmod{27}$.

If $2^k \equiv 1 \pmod{27}$ for some k with $1 \le k \le 18$, then $k \mid 18$.

Now check: $2 \equiv 2 \pmod{27}$, $2^2 \equiv 4 \pmod{27}$, $2^3 \equiv 8 \pmod{27}$,

$$2^6 \equiv 10 \pmod{27}, \quad 2^9 \equiv 26 \pmod{27}.$$

Thus, 18 is the smallest exponent k s.t. $2^k \equiv 1 \pmod{27}$.

It follows that $\{2^k : 1 \le k \le 18\}$ are incongruent mod 27:

if $2^j \equiv 2^k \pmod{27}$ for $j > k$, $1 \le k < j \le 18$, then

$$2^{j-k} \equiv 1 \pmod{27} \Longrightarrow \underbrace{j-k=0}_{j=k} \text{ or } \underbrace{j-k=18}_{\text{No!}}.$$

$\blacksquare$

7.4 **1**

$$\sum_{d \mid n} (-1)^{n/d} \varphi(d) = \begin{cases} 0, & n \text{ even} \\ -n, & n \text{ odd} \end{cases}$$

case 1 n odd:

$$\underbrace{\sum_{d \mid n} (-1)^{n/d}}_{n \text{ odd} \Rightarrow \frac{n}{d} \text{ odd} \Rightarrow (-1)^{n/d} = -1.} \varphi(d) = -\sum_{d \mid n} \varphi(d) = -n$$

case 2 n even: $n = 2^k m$ for some $k \geq 1$ and m odd

Then $d \mid n \Longrightarrow d \mid m$ $\underline{\text{or}}$ $d = 2^j q$ for $j \leq k$ and $q \mid m$.

Now compute:

$$\sum_{d \mid n} (-1)^{\frac{n}{d}} \varphi(d) = \sum_{d \mid m} (-1)^{\frac{n}{d}} \varphi(d) + \sum_{j=1}^{k} \left[\sum_{\substack{d = 2^j q \\ q \mid m}} (-1)^{\frac{n}{d}} \varphi(d) \right]$$

For this sum,

$\frac{n}{d} = \frac{2^k m}{d}$, $d \mid m$

$\Longrightarrow \frac{n}{d}$ is even $\Longrightarrow (-1)^{\frac{n}{d}} = +1.$

$d = 2^j q$, $q \mid m \Longrightarrow$

$\frac{n}{d}$ is even for $j < k$,

$\frac{n}{d}$ odd for $j = k$.

Thus:

$$\sum_{d|n} (-1)^{\frac{n}{d}} \varphi(d) = \sum_{d|m} (-1)^{\frac{n}{d}} \varphi(d) + \sum_{j=1}^{k} \left[\sum_{\substack{d=2^j q \\ q|m}} (-1)^{\frac{n}{d}} \varphi(d) \right]$$

$$= \sum_{d|m} \varphi(d) + \left[\sum_{\substack{d=2q \\ q|m}} \varphi(2q) + \sum_{q|m} \varphi(4q) + \dots + \sum_{q|m} \varphi(2^{k-1} q) - \sum_{q|m} \varphi(2^k q) \right]$$

$$= m + \left[\sum_{q|m} \varphi(q) + \sum_{q|m} \overbrace{\varphi(4)}^{2} \varphi(q) + \dots + \sum_{q|m} \varphi(2^{k-1}) \varphi(q) - \sum_{q|m} \varphi(2^k) \varphi(q) \right]$$

$$= m + \left[1 + \overbrace{(4-2)}^{\varphi(4)} + \overbrace{(8-4)}^{\varphi(8)} + \dots + (2^{k-1} - 2^{k-2}) - (2^k - 2^{k-1}) \right] \varphi(q)$$

Σ over $q|m$

$$= m + \left[1 - 2 + 2^{k-1} + 2^{k-1} - 2^k \right] \sum_{q \mid m} \varphi(q)$$

$$= m + (-1) \sum_{q \mid m} \varphi(q) = m - m = 0.$$

:)

<u>4</u> $\varphi(c)$, 6.2: $\displaystyle\sum_{d \mid n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$, $n = p_1^{k_1} \cdots p_r^{k_r}$.

Then $\displaystyle n \sum_{d \mid n} \frac{\mu(d)}{d} = p_1^{k_1} \cdots p_r^{k_r} \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$

$$= \left(p_1^{k_1} - p_1^{k_1 - 1}\right) \cdots \left(p_r^{k_r} - p_r^{k_r - 1}\right)$$

$$= \varphi(n).$$

$\boxtimes$