? Smallest n with $d(n) = 8$?

Ch. 6.

3. Last digit of 7^{355}.

Note that $7^4 = (7^2)^2 = 49^2 \equiv (-1)^2 \equiv 1 \pmod{10}$.

So $7^{355} = 7^{4 \cdot 88 + 3} = (7^4)^{88} 7^3$

$\equiv 1^{88} \cdot 7^3 \pmod{10}$

$\equiv 7^2 \cdot 7 \pmod{10}$

$\equiv 9 \cdot 7 \pmod{10}$

$\equiv 3 \pmod{10}$.

7. $165 = 3 \cdot 5 \cdot 11$.

$314^2 \equiv 1 \pmod{3}$, so $314^{164} = (314^{82})^2 \equiv 1 \pmod{3}$

$314^4 \equiv 1 \pmod{5}$, so $314^{164} = (314^{41})^4 \equiv 1 \pmod{5}$

$314^{10} \equiv 1 \pmod{11}$, so 314^{164}

$= 314^{16 \cdot 10 + 4}$

$\equiv (314^{10})^{16} (314)^4 \pmod{11}$

$\equiv 314^4 \pmod{11}$

$\equiv 6^4 \pmod{11}$

(because $314 \equiv 6 \pmod{11}$)

$\equiv 36^2 \pmod{11}$

$\equiv 3^2 \pmod{11}$

$\equiv 9 \pmod{11}$.

7. Smallest n with $d(n) = 8$?

So solve $x \equiv 1 \pmod 3$

$x \equiv 1 \pmod 5$

$x \equiv 9 \pmod{11}$

or equivalently, $x \equiv 1 \pmod{15}$, $x \equiv 9 \pmod{11}$.

If $x = 15t + 1$

$15t + 1 \equiv 9 \pmod{11}$

$15t \equiv 8 \pmod{11}$

$15t \equiv 30 \pmod{11}$

So $t \equiv 2 \pmod{11}$

and $x \equiv 31 \pmod{165}$,

So the remainder is 31.

10(b). Theorem. Suppose that you can write $n = qr$, where q and r are distinct > 1 ~~coprime to each other~~. Then $(n-1)! \equiv 0 \pmod n$.

~~(Note: other theorem statements are possible too! But beware that $(4-1)! \not\equiv 0 \pmod 4$).~~

Proof. We have

$(n-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots\cdots n-1.$

Since q and r both appear on the right side, with $q, r \leq n-1$, we have

$qr \mid (n-1)!$ and $(n-1)! \equiv 0 \pmod{qr}$.

In particular, is true for every composite n other than 4.

7. Smallest n with $d(n) = 8$?

Recall, if $n = p_1^{e_1} p_2^{e_2} p_3^{e_3}$

then $d(n) = (e_1 + 1)(e_2 + 1)(e_3 + 1)$.

So: $n = p^7$ or $n = p_1^3 p_2$ or $n = p_1 p_2 p_3$.

Smallest of each form: $2^7 = 128$

$2^3 \cdot 3 = 24$

$2 \cdot 3 \cdot 5 = 30$.

24 is the smallest.

Similarly, if $d(n) = 10$,

$n = p^9$ or $n = p_1^4 p_2$.

$2^9 = 512$

$2^4 \cdot 3 = 48$. So 48 is the smallest.

13. (1) Suppose n is a square.

Then $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with all e_k even.

And $d(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$

with every $e_i + 1$ odd, so $d(n)$ must be odd also.

(2) Alternative proof.

Let $1 = m_1, \cdots, m_k$ be the divisors of n less than $\sqrt{n}$.

Then the divisors of n are

$m_1, \cdots, m_k, \frac{n}{m_1}, \frac{n}{m_2}, \cdots, \frac{n}{m_k}$ and $\sqrt{n}$.

So there are $2k+1$ of them which is odd.

11. $\sigma(2^e pq) - 2^e pq$

$= \sigma(2^e)\sigma(p)\sigma(q) - 2^e pq$

$= (2^{e+1}-1)(p+1)(q+1) - 2^e pq$

$= (2^{e+1}-1)(3\cdot 2^e)(3\cdot 2^{e-1}) - 2^e(3\cdot 2^e - 1)(3\cdot 2^{e-1}-1)$

$= 9\cdot 2^{3e} - 9\cdot 2^{2e-1} - 9\cdot 2^{3e-1} + 3\cdot 2^{2e} + 3\cdot 2^{2e-1} - 2^e$

$= 9\cdot 2^{3e-1} - 6\cdot 2^{2e-1} + 3\cdot 2^{2e} - 2^e$

$= 9\cdot 2^{3e-1} - 2^e = 2^e(3^2\cdot 2^{2e-1} - 1) = 2^e r.$

$\sigma(2^e r) - 2^e r$

$= \sigma(2^e)\sigma(r) - 2^e r$

$= (2^{e+1}-1)(r+1) - 2^e r$

$= (2^{e+1}-1)(9\cdot 2^{2e-1}) - 2^e(9\cdot 2^{2e-1} - 1)$

$= 9\cdot 2^{3e} - 9\cdot 2^{2e-1} - 9\cdot 2^{3e-1} + 2^e$

$= 2^e(9\cdot 2^{2e} - 9\cdot 2^{e-1} - 9\cdot 2^{2e-1} + 1)$

$= 2^e(9\cdot 2^{2e-1} - 9\cdot 2^{e-1} + 1)$

$= 2^e(3\cdot 2^e - 1)(3\cdot 2^{e-1} - 1)$ as desired.

p. 112/9.

$15 + 33 = 48$

$$\begin{array}{r} {}^{1}\\ 48 \\ 24 \\ \hline 73 \end{array}$$

in base 9.

$$\begin{array}{r} 42 \\ \cdot\ 12 \\ \hline 84 \\ 42 \\ \hline 514 \end{array}$$

$$\begin{array}{r} {}^{5\ 1}\\ 1620 \\ -\ 1453 \\ \hline 156 \end{array}$$

$$\begin{array}{r} {}^{2}\\ 314 \\ \cdot\ 152 \\ \hline {}^{1}\ 628 \\ 1672 \\ 314 \\ \hline 48848 \end{array}$$

p. 126/9.

$\frac{1}{3}$:

$$\begin{array}{r} .01010\,10\ldots \\ 11 \,\overline{)\,1.00000000} \\ 11 \\ \hline 100 \\ 11 \\ \hline 10 \end{array}$$

period 2.

We see : $2^0 \equiv 1 \pmod 3$

$2^1 \equiv 2 \pmod 3$

$\boxed{2^2 \equiv 1 \pmod 3}$ ← This is the period.

$\frac{1}{5}$:

$$
\begin{array}{r|l}
 & .00110011\cdots \\
101 & 1.000000000 \\
 & \underline{101} \\
 & \quad 110 \\
 & \quad \underline{101} \\
 & \qquad 1000 \\
 & \qquad \underline{\ \ 101} \\
 & \qquad \ \ 110 \ \text{etc.}
\end{array}
$$

period 4 :

$2^0 \equiv 1 \pmod 5$
$2^1 \equiv 2 \pmod 5$
$2^2 \equiv 4 \pmod 5$
$2^3 \equiv 3 \pmod 5$
$2^4 \equiv 1 \pmod 5$ ⟵ This is the period.

Similarly:

$\frac{1}{7}$ has period $\underline{3}$ because $2^3 \equiv 1 \pmod 7$

9: $\pmod 9$, powers of 2 are
$1, 2, 4, 8, 7, 5, \boxed{1}$ So period is 6.

11: $\pmod{11}$, powers of 2 are
$1, 2, 4, 8, 5, 10, 9, 7, 3, 6, \boxed{1}$
So period is 10.

You knew the period would divide $\varphi(11) = 10$.

14. Four solutions of $\phi(n) = 16$.

Use the multiplicative property:

$\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(8) = 4$

~~[illegible]~~

~~[illegible]~~

So $\phi(40) = \phi(5)\phi(8) = 16$.

$\phi(60) = \phi(5)\phi(3)\phi(4) = 4 \cdot 2 \cdot 2 = 16$.

Also $\phi(17) = 16$

and $\phi(32) = 16$.

Moreover $\phi(34) = \phi(2)\phi(17) = 1 \cdot 16 = 16$

and $\phi(16) = 8 \Rightarrow \phi(48) = \phi(3) \cdot \phi(16) = 16$.

There are six total.

17. If $(m,n) = 2$ then $\phi(mn) = 2\phi(m)\phi(n)$.

Proof. Write $m = 2^a r$ and $n = 2^b s$, where $a, b \geq 1$, r, s both odd.

~~[illegible]~~

~~without loss of generality assume that [illegible]~~

$$\begin{aligned}
\text{Then } \phi(mn) &= \phi(2^a r \cdot 2^b s) \\
&= \phi(2^{a+b} \cdot r \cdot s) \\
&= \phi(2^{a+b})\phi(rs) \quad \left(\begin{array}{l}\text{Since } (m,n) = 2, \\ r \text{ and } s \text{ have no} \\ \text{common factor.}\end{array}\right) \\
&= \phi(2^{a+b})\phi(r)\phi(s). \\
&= 2^{a+b-1}\phi(r)\phi(s).
\end{aligned}$$

~~[illegible]~~

$$\begin{aligned}
\text{And } \phi(m)\phi(n) &= \phi(2^a)\phi(r)\phi(2^b)\phi(s) = 2^{a-1} \cdot \phi(r) \cdot 2^{b-1} \cdot \phi(s) \\
&= 2^{a+b-2}\phi(r)\phi(s).
\end{aligned}$$

The first expression is twice the second.