Do the following exercises from the text:
Section 4.1: 5, 8, 26, 27

5. Find the least residue modulo 5 of 3^2 and 3^{20}.

▶ **Solution.** Since $3^2 \equiv 4 \equiv -1 \pmod 5$, and $3^{20} = (3^2)^{10} \equiv (-1)^{10} \equiv 1 \pmod 5$, the least residues of 3^2 and 3^{20} modulo 5 are 4 and 1, respectively. ◀

8. Show that the numbers -13, -9, -4, -1, 9, 18, 21 for a complete residue system modulo 7.

▶ **Solution.** There are 7 numbers, and the least residues modulo 7 are 1, 5, 3, 6, 2, 4, 0, respectively, no two of which are equal, so they form a complete residue system modulo 7. ◀

26. If p is a prime and $a^2 \equiv 1 \pmod p$, prove that $a \equiv \pm 1 \pmod p$.

▶ **Solution.** Since $a^2 \equiv 1 \pmod p$, it follows that $p \mid (a^2 - 1)$. Thus, $p \mid (a-1)(a+1)$ and by Euclid's lemma, $p \mid (a-1)$ or $p \mid (a+1)$. If $p \mid (a-1)$, then $a \equiv 1 \pmod p$ and if $p \mid (a+1)$ then $a \equiv -1 \pmod p$. Therefore, $a \equiv \pm 1 \pmod p$. ◀

27. Give an example to show that the result of Exercise 26 is not necessarily valid if p is not a prime.

▶ **Solution.** $3^2 \equiv 1 \pmod 8$, but $3 \not\equiv \pm 1 \pmod 8$. ◀

Section 4.2: 1 (b), (d); 6 (a)

1. Check the following numbers for divisibility by 3, 9, and 11.

(b) 113,058 **(d)** 371,684

▶ **Solution.** (b) $s = 1+1+3+0+5+8 = 18$ and $t = 8-5+0-3+1-1 = 0$ so 113,058 is divisible by 3, 9, and 11.

(d) $s = 29$ and $t = 5$ so 371,684 is not divisible by 3, 9, or 11. ◀

6. Let a and s be as in Theorem 4.12.

(a) Prove that $4 \mid a$ if and only if $4 \mid (10a_1 + a_0)$.

▶ **Solution.** $a = \sum_{k=0}^{n} a_k 10^k = (a_0 + 10a_1) + \sum_{k=2}^{n} a_k 10^k = (10a_1 + a_0) + 100 \sum_{k=2}^{n} a_k 10^{k-2}$. Since $4 \mid 100$ it follows that $4 \mid a$ if and only if $4 \mid (10a_1 + a_0$. ◀

Section 4.3: 5, 7, 8, 23

5. Show that the numbers 3, 3^2, 3^3, 3^4, 3^5, 3^6 for a reduced residue system modulo 7.

▶ **Solution.** By direct calculation, we have that $3 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 6 \pmod 7$, $3^4 \equiv 4 \pmod 7$, $3^5 \equiv 5 \pmod 7$, and $3^6 \equiv 1 \pmod 7$. Since 1, 2, 3, 4, 5, 6 form a reduced residue system modulo 7, so do 3, 3^2, 3^3, 3^4, 3^5, 3^6. ◀

7. If p is an odd prime and $p \nmid a$, show that $a^{(p-1)/2} \equiv \pm 1 \pmod p$.

▶ **Solution.** Since p is an odd prime and $p \nmid a$ Fermat's theorem applies to give $a^{p-1} \equiv 1 \pmod p$. Since p is odd, $p-1$ is even and $a^{p-1} = (a^{(p-1)/2})^2$. Thus, if $b = a^{(p-1)/2}$ we have $b^2 \equiv 1 \pmod p$ and by Exercise 26 of Section 4.1, it follows that $b \equiv \pm 1 \pmod p$, that is, $a^{(p-1)/2} \equiv \pm 1 \pmod p$. ◀

8. Give an example to show that the result of Exercise 8 is not necessarily true if p is replaced by an arbitrary positive integer n with $(a, n) = 1$.

▶ **Solution.** If we replace p by 15 and a by 4, we have

$$4^{(n-1)/2} = 4^7 = (4^2)^3 \cdot 4 \equiv (1)^3 \cdot 4 \equiv 4 \pmod{15}$$

. ◀

23. Show by example that $\phi(mn)$ is not necessarily equal to $\phi(m)\phi(n)$ if $(m, n) \neq 1$.

▶ **Solution.** $\phi(12) = 4$, $\phi(6) = 2$, $\phi(2) = 1$, so $\phi(12) \neq \phi(6)\phi(2)$. ◀

Section 5.1: 1 (b) (d); 4, 5

1. Solve the following conditional congruences.

(b) $15x \equiv 3 \pmod 9$

▶ **Solution.** Since $(15, 9) = 3$ there are 3 non-congruent solutions modulo 9. Since $15 \equiv 6 \pmod 9$ the congruence is equivalent to $6x \equiv 3 \pmod 9$, which by inspection has a solution $x_0 = 2$. The remaining incongruent solutions are $x_1 = 2 + 3 = 5$ and $x_2 = 2 + 2 \cdot 3 = 8$. ◀

(d) $35x \equiv 15 \pmod{182}$

▶ **Solution.** Since $(35, 182) = 7$ and $7 \nmid 15$, there are no solutions to this congruence equation. ◀

4. When a man cashed a check, the clerk mistook the number of cents for the number of dollars and vice versa. After spending 68 cents, the man discovered that he still had precisely twice as much money as the amount for which the check was originally written. What is the smallest amount for which the check could have been written?

▶ **Solution.** Let x denote the number of dollars and y the number of cents for which the check was originally written. Then $100y+x-68 = 2(100x+y)$ or $98y-199x = 68$. Apply the Euclidean Algorithm to get $98(-67) - 199(-33) = 1$ and multiply by 68 to get $98(-4556) - 199(-2244) = 68$. Thus, one solution in integers of $98y - 199x = 68$ is $y_0 = -4556$ and $x_0 = -2244$. By Theorem 5.2, the other solutions in integers are $x_k = -2244 + 98k$ and $y_k = -4556 - k(-199)$. The smallest k that will give positive values for x_k and y_k is $k = 23$. This gives $x_k = -2244 + 98 \cdot 23 = 10$ and $y_k = -4556 + 23 \cdot 199 = 21$. Thus, the check was written for \$10.21. ◀

Problems not from the text:

1. For each part, find the smallest positive x that solves the simultaneous congruences.

   (a) $x \equiv 3 \pmod 7$ and $x \equiv 5 \pmod 9$

   ▶ **Solution.** $7 \cdot 4 + 9 \cdot (-3) = 1$ so $-27 \equiv 1 \pmod 7$ and $-27 \equiv 0 \pmod 7$, while $28 \equiv 1 \pmod 9$ and $28 \equiv 0 \pmod 7$. Thus, $x = 3 \cdot (-27) + 5 \cdot 28 = 59$ satisfies the congruences and all other solutions are congruent modulo $9 \cdot 7 = 63$. Thus, 59 is the smallest positive solution. ◀

   (b) $x \equiv 3 \pmod{37}$ and $x \equiv 1 \pmod{87}$.

   ▶ **Solution.** Use the Euclidean Algorithm to find (37, 87):

87	37		
1	0	87	
0	1	37	
1	−2	13	$= 87 - 2 \cdot 37$
−2	5	11	$= 37 - 2 \cdot 13$
3	−7	2	$= 13 - 1 \cdot 11$
−17	40	1	$= 11 - 5 \cdot 2$

   Thus, $37 \cdot 40 + 87 \cdot (-17) = 1$ and a solution to the simultaneous congruences is

$$x_0 = 3 \cdot 87 \cdot (-17) + 1 \cdot 37 \cdot 40 = -2957.$$

   Other solutions are congruent to x_0 modulo $37 \cdot 87 = 3219$. Thus, the smallest positive solution is $-2957 + 3219 = 262$. ◀

2. Show that the integers $m = 3^k \cdot 568$ and $n = 3^k \cdot 638$, where $k \geq 0$, satisfy simultaneously

$$\tau(m) = \tau(n), \qquad \sigma(m) = \sigma(n), \text{ and } \qquad \phi(m) = \phi(m).$$

▶ **Solution.** The prime factorizations are $m = 3^k \cdot 2^3 \cdot 71$ and $n = 3^k \cdot 2 \cdot 11 \cdot 29$. Then

$$\begin{aligned}
\tau(m) &= (k+1)(3+1)(1+1) = 8(k+1) \\
\tau(n) &= (k+1)(1+1)(1+1)(1+1) = 8(k+1) = \tau(m) \\
\sigma(m) &= \sigma(3^k)\left(\frac{2^4-1}{2-1}\right) \cdot (1+71) = \sigma(3^k) \cdot 15 \cdot 72 = \sigma(3^k) \cdot 1080 \\
\sigma(n) &= \sigma(3^k) \cdot (2+1)(11+1)(29+1) = \sigma(3^k) \cdot 3 \cdot 12 \cdot 30 = 1080 = \sigma(m) \\
\phi(m) &= \phi(3^k)\phi(2^3)\phi(71) = \phi(3^k) \cdot 4 \cdot 70 = \phi(3^k) \cdot 280 \\
\phi(n) &= \phi(3^k)\phi(2)\phi(11)\phi(29) = \phi(3^k) \cdot 1 \cdot 10 \cdot 28 = \phi(3^k) \cdot 280 = \phi(m)
\end{aligned}$$

◀

3. Establish each of the following assertions:

   (a) If n is an odd integer, then $\phi(2n) = \phi(n)$.

   ▶ **Solution.** Since n is odd, $(2, n) = 1$. Since ϕ is multiplicative,$\phi(2n) = \phi(2)\phi(n) = \phi(n)$ because $\phi(2) = 1$. ◀

   (b) If n is an even integer, then $\phi(2n) = 2\phi(n)$

   ▶ **Solution.** Since n is even, $n = 2^k m$ where m is odd and $k \geq 1$. Then $\phi(2n) = \phi(2 \cdot 2^k m) = \phi(2^{k+1}m) = \phi(2^{k+1})\phi(m) = 2^k\phi(m) = 2 \cdot 2^{k-1} \cdot \phi(m) = 2\phi(2^k)\phi(m) = 2\phi(2^k m) = 2\phi(n)$. ◀

   (c) $\phi(3n) = 3\phi(n)$ if and only if $3 \mid n$.

   (d) $\phi(3n) = 2\phi(n)$ if and only if $3 \nmid n$.

   ▶ **Solution.** (c) and (d) are done together as follows: If $3 \mid n$ then $n = 3^k m$ where $(3, m) = 1$ and $k \geq 1$. Then

$$\begin{aligned}
\phi(3n) &= \phi(3^{k+1}m) = \phi(3^{k+1})\phi(m) \\
&= (3^{k+1} - 3^k)\phi(m) = 3(3^k - 3^{k-1})\phi(m) = 3\phi(3^k)\phi(m) \\
&= 3\phi(3^k m) = 3\phi(n).
\end{aligned}$$

   If $3 \nmid n$, then $(3, n) = 1$ and $\phi(3n) = \phi(3)\phi(n) = 2\phi(n)$.
   Since these two cases cover all possibilities for $3n$, both (c) and (d) are true. ◀