1. If $a = 2^4 13^2 19$ and $b = 2^3 5^2 13$ then find the prime factorization of

   (a) $(a,\, b)$

   ▶ **Solution.** $(a,\, b) = 2^3 \cdot 13$ ◀

   (b) $[a,\, b]$

   ▶ **Solution.** $[a,\, b] = 2^4 5^2 13^2 19$ ◀

   (c) $(a^2,\, b^3)$

   ▶ **Solution.** $a^2 = 2^8 13^4 19^2$ and $b^3 = 2^9 5^6 13^3$ so $(a^2,\, b^3) = 2^9 13^4 5^6 19^2$. ◀

2. Prove that any whole number amount greater than 23 cents could be made up using an unlimited supply of 5 cent and 7 cent coupons.

   ▶ **Solution.** Prove by induction. For the base step, $24 = 2 \cdot 5 + 2 \cdot 7$.

   Induction Step: Assume that $k = x \cdot 5 + y \cdot 7$ with $x,\, y \geq 0$ and $k \geq 24$. If $y \geq 2$ then $k + 1 = (x + 1) \cdot 5 + (y - 2) \cdot 7$, that is, remove two 7's and add three 5's.

   If $x \geq 4$ then $k + 1 = (x - 4) \cdot 5 + (y + 3) \cdot 7$, that is, remove four 5's and add three 7's.

   One of these two cases must occur since $x \leq 3$, $y \leq 1$ only give $k \leq 3 \cdot 5 + 1 \cdot 7 = 22 < 24$.

   Hence, if $k \geq 24$ can be written as $5x + 7y$ for $x,\, y \geq 0$, then so can $k + 1$. Hence the principle of induction implies that all integers ≥ 24 can be written in the form $5x + 7y$. ◀

3. (a) Evaluate $\phi(3000)$.

   ▶ **Solution.** $3000 = 3 \cdot 2^3 \cdot 5^3$ so $\phi(3000) = \phi(3)\phi(2^3)\phi(5^3) = (3 - 1)(2^3 - 2^2)(5^3 - 5^2) = 3 \cdot 4 \cdot 100 = 1200$. ◀

   (b) Find the remainder when 11^{2402} is divided by 3000.

   ▶ **Solution.** From Euler's theorem $11^{2402} = 11^{2 \cdot 1200 + 2} = \left(11^{1200}\right)^2 \cdot 11^2 \equiv 1^2 \cdot 11^2 \equiv 121 \pmod{3000}$. Thus, the remainder when 11^{2402} is divided by 300 is 121. ◀

4. Use induction to prove that $6^n \equiv 5n + 1 \pmod{25}$ for all positive integers n.

   ▶ **Solution.** For the base step, $6^1 = 6 = 5 \cdot 1 + 1$ so $6^1 \equiv 5 \cdot 1 + 1 \pmod{25}$.

   Induction step: Assume that $6^k \equiv 5k + 1 \pmod{25}$ for some positive integer k. Then

$$
\begin{aligned}
6^{k+1} &= 6^k \cdot 6 = 6^k(5 + 1) \\
&\equiv (5k + 1)(5 + 1) \pmod{25} \qquad \text{by the induction hypothesis} \\
&\equiv 25k + 5k + 5 + 1 = 25k + 5(k + 1) + 1 \pmod{25} \\
&\equiv 5(k + 1) + 1 \pmod{25}.
\end{aligned}
$$

   Thus, if $6^n \equiv 5n + 1$ for $n = k$ then it is also true for $n = k + 1$, and by the induction principle, it is valid for all $n \geq 1$. ◀

5. Use induction to prove that $2^n \mid (2n)!$

▶ **Solution.** For the base step, $2^1 = 2 = 2!$ so $2^1 \mid (2 \cdot 1)!$.

Induction step: Assume that $2^k \mid (2k)!$. This means that $(2k)! = 2^k \cdot c$ for some integer c. Then,

$$\begin{aligned}(2(k+1))! &= (2(k+1))(2k+1)(2k)! \\ &= 2(k+1)(2k+1) \cdot 2^k \cdot c \\ &= 2^{k+1} \cdot (k+1)(2k+1)c.\end{aligned}$$

Hence, if $2^k \mid (2k)!$ then $2^{k+1} \mid (2(k+1))!$ and by the principle of induction, $2^n \mid (2n)!$ for all positive integers. ◀

6. Give a proof that there are infinitely many primes.

▶ **Solution.** Let $p_1, p_2, \ldots, p_r$ be any finite set of prime numbers. Define $N = p_1 \cdot p_2 \cdots p_r + 1$. Then N is an integer and hence there is a prime divisor q of N. q cannot be one of the primes $p_1, p_2, \ldots, p_r$, since, if q is one of these primes, then $q \mid p_1 \cdot p_2 \cdots p_r$ and since $q \mid N$ it would follow that $q \mid (N - p_1 \cdot p_2 \cdots p_r)$ or $q \mid 1$. But any prime is greater than 1 and so $q \nmid 1$. Hence, q must be different from $p_1 \cdot p_2 \cdots p_r$. Therefore, any finite list cannot contain all primes, so there is an infinite number of primes. ◀

7. Find all right-angled triangles with relatively prime integer sides and base of given length:

   (a) 28

   ▶ **Solution.** $x = 2st = 28$ so $st = 14$ which gives two cases: $s = 1$, $t = 14$ and $s = 2$, $t = 7$.
   Case 1: $x = 28$, $y = t^2 - s^2 = 14^2 - 1^2 = 195$, $z = t^2 + s^2 = 14^2 + 1^2 = 197$
   Case 2: $x = 28$, $y = t^2 - s^2 = 7^2 - 2^2 = 45$, $z = t^2 + s^2 = 7^2 + 2^2 = 53$ ◀

   (b) 55

   ▶ **Solution.** $y = 55 = t^2 - s^2 = (t+s)(t-s)$
   Case 1: $t + s = 55$, $t - s = 1$. Solving for t, s gives $t = 28$, $s = 27$. Thus,

$$x = 2st = 1512, \quad y = 55, \quad z = t^2 + s^2 = 1513.$$

   Case 2: $t + s = 11$, $t - s = 5$ so $t = 8$, $s = 3$. Thus,

$$x = 2st, \quad y = 55, \quad z = t^2 + s^2 = 73.$$

◀

8. (a) Find the prime factorization of 600.

   ▶ **Solution.** $600 = 2^3 \cdot 3 \cdot 5^2$ ◀

(b) $\tau(n)$ is the number of positive divisors of n. Evaluate $\tau(600)$.

▶ **Solution.** $\tau(600) = \tau(2^3 \cdot 3 \cdot 5^2) = \tau(2^3)\tau(3)\tau(5^2) = (3+1)(1+1)(2+1) = 24$ ◀

(c) $\sigma(n)$ is the sum of the positive divisors of n. Evaluate $\sigma(600)$.

▶ **Solution.**

$$\begin{aligned}\sigma(600) &= \sigma(2^3 \cdot 3 \cdot 5^2) = \sigma(2^3)\sigma(3)\sigma(5^2) \\ &= \frac{2^{3+1}-1}{2-1}(1+3)\frac{5^{2+1}-1}{5-1} = 15 \cdot 4 \cdot 31 \\ &= 1860.\end{aligned}$$

◀

(d) $\phi(n)$ is the Euler phi function. Evaluate $\phi(600)$.

▶ **Solution.**

$$\begin{aligned}\phi(600) &= \phi(2^3 \cdot 3 \cdot 5^2) = \phi(2^3)\phi(3)\phi(5^2) \\ &= (2^3 - 2^2)(3-1)(5^2-5) = 4 \cdot 2 \cdot 20 \\ &= 160.\end{aligned}$$

◀

(e) $\mu(n)$ is the Möbius function. Evaluate $\mu(600)$.

▶ **Solution.** Since $4 \mid 600$, $\mu(600) = 0$. ◀

9. Give a non-trivial factor of $2^{55} - 1$. (Bonus points for two.)

▶ **Solution.**

$$\begin{aligned}2^{55} - 1 &= (2^5)^{11} - 1 \\ &= (2^5 - 1)((2^5)^{10} + (2^5)^9 + (2^5)^8 + (2^5)^7 + (2^5)^6 + (2^5)^5 + (2^5)^4 + (2^5)^3 + (2^5)^2 + 2^5 + 1)\end{aligned}$$

Therefore, $2^5 - 1 = 31$ is a factor of $2^{55} - 1$. Similarly,

$$\begin{aligned}2^{55} - 1 &= (2^{11})^5 - 1 \\ &= (2^{11} - 1)((2^{11})^4 + (2^{11})^3 + (2^{11})^2 + (2^{11})^1 + 1)\end{aligned}$$

Therefore, $2^{11} - 1 = 2048 - 1 = 2047$ is also a factor of $2^{55} - 1$. ◀

10. Prove that if $a \mid b$ and $a \mid c$ then $a^2 \mid 7bc$.

▶ **Solution.** If $a \mid b$ then $b = ak$ for some integer k. If $a \mid c$, then $c = am$ for some integer m. Then

$$7bc = 7(ak)(am) = a^2(7km),$$

and thus $a^2 \mid 7bc$. ◀

11. Use congruences to prove that $x^2 - 5y^2 = 3$ has no integer solutions.

▶ **Solution.** If $x^2 - 5y^2 = 3$ then $x^2 = 3 + 5y^2$ so $x^2 \equiv 3 \pmod 5$. However, if $x \equiv 0 \pmod 5$ then $x^2 \equiv 0 \pmod 5$, if $x \equiv \pm 1 \pmod 5$ then $x^2 \equiv 1 \pmod 5$, and if $x \equiv \pm 2 \pmod 5$ then $x^2 \equiv 4 \pmod 5$. Since these cases account for all integers x, it follows that $x^2 \not\equiv 3 \pmod 5$ so the given equation has no integer solutions. ◀

12. (a) If $F(n) = \sum_{d \mid n} \sigma(d)$ then evaluate $F(175)$.

▶ **Solution.** Since $\sigma(n)$ is a multiplicative function, so is $F(n)$. Thus, to evaluate $F(175)$ it is only necessary to evaluae $F(7)$ and $F(5^2)$ since $175 = 5^2 \cdot 7$. But,

$$F(7) = \sigma(1) + \sigma(7) = 1 + (1 + 7) = 9,$$

and

$$F(5^2) = \sigma(1) + \sigma(5) + \sigma(5^2) = 1 + (1 + 5) + (1 + 5 + 5^2) = 38.$$

Therefore, $F(175) = F(5^2 \cdot 7) = F(5^2)F(7) = 38 \cdot 9 = 342$. ◀

(b) Evaluate $\sigma(22,491)$. (Hint: $22,491 = 27 \cdot 49 \cdot 17$.)

▶ **Solution.** Since $\sigma(n)$ is multiplicative,

$$\begin{aligned}
\sigma(22,491) &= \sigma(3^3 \cdot 7^2 \cdot 17) \\
&= \sigma(3^3)\sigma(7^2)\sigma(17) \\
&= (1 + 3 + 3^2 + 3^3)(1 + 7 + 7^2)(1 + 17) \\
&= 40 \cdot 57 \cdot 18 = 41,040.
\end{aligned}$$

◀

13. Suppose $g(n)$ is a multiplicative function satisfying $\tau(n)^2 = \sum_{d \mid n} g(d)$.

(a) Use the Möbius inversion formula to give a formula for $g(n)$.

▶ **Solution.** From the Möbius inversion formula $g(n) = \sum_{d \mid n} \mu(d)\tau^2(n/d)$. ◀

(b) Evaluate $g(5^3)$.

▶ **Solution.** If p is a prime, then

$$\begin{aligned} g(p^k) &= \mu(1)\tau^2(p^k) + \mu(p)\tau^2(p^{k-1}) + \mu(p^2)\tau^2(p^{k-2}) + \cdots \\ &= (k+1)^2 - k^2, \end{aligned}$$

since $\mu(p^t) = 0$ for $t \geq 2$. Therefore, $g(5^3) = 4^2 - 3^2 = 7$. ◀

(c) Evaluate $g(700)$.

▶ **Solution.** Since g is multiplicative and $700 = 2^2 \cdot 5^2 \cdot 7$ we have that

$$g(700) = g(2^2)g(5^2)g(7) = (3^2 - 2^2)(3^2 - 2^2)(2^2 - 1^2) = 75.$$

◀

14. (a) What can you say about the prime factorization of n if $\tau(n) = 8$?

▶ **Solution.** If $\tau(n) = 8$, then $n = p_1^{k_1} \cdots p_r^{k_r}$ is the prime factorization of n and possible factorization of $\tau(n)$ are given by

$$\tau(p_1^{k_1} \cdots p_r^{k_r}) = (k_1 + 1) \cdots (k_r + 1) = 8 = 2 \cdot 4 = 2 \cdot 2 \cdot 2.$$

This gives $n = p^7$, $n = p_1(p_2)^3$, or $n = p_1 p_2 p_3$ ◀

(b) What is the smallest n with $\tau(n) = 8$.

▶ **Solution.** The smallest n with $\tau(n) = 8$ is obtained by taking the smallest possible primes in calculating n in part (a). $2^7 = 128$, $2^2 \cdot 3 = 24$, and $2 \cdot 3 \cdot 5 = 30$. Therefore, the smallest n with $\tau(n) = 8$ is $n = 24$. ◀

(c) Find three n with $\phi(n) = 16$.

▶ **Solution.** $\phi(p_1^{k_1} \cdots p_r^{k_r}) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1) = 2^4$. If $p - 1 \mid 2^4$ then $p = 2, 3, 5, 17$ and if $p^{k-1} \mid 2^4$ then $p = 2$ and $1 \leq k \leq 5$ Thus some candidates for n are 17, 32, 34, 40, 48, 60. ◀

15. (a) Suppose that $d = \operatorname{ord}_m a$. Prove that if $a^n \equiv 1 \pmod{m}$ then $d \mid n$.

▶ **Solution.** By the division algorithm, $n = dq + r$ where $0 \leq r < d$. Then

$$1 \equiv a^n \equiv a^{dq+r} \equiv (a^d)^q a^r \equiv 1^q a^r \pmod{m}.$$

But $r < d$ and d is the smallest positive integer k with $a^k \equiv 1 \pmod{m}$. Thus, r cannot be positive so it must be 0 and hence $n = dq$. That is $d \mid n$. ◀

(b) Find (with justification) $\operatorname{ord}_m b$ if $b^8 \equiv -1 \pmod{m}$ with $m \geq 2$.

▶ **Solution.** $b^{16} = (b^8)^2 \equiv (-1)^2 \equiv 1 \pmod{m}$. Therefore, $d - \operatorname{ord}_m b \mid 16$ so $d = 1, 2, 4, 8$ or 16. If $d = 1, 2, 4,$ or 8 then $a^8 \equiv 1 \pmod{m}$. But $a^8 \equiv -1 \not\equiv 1 \pmod{m}$ since $m \geq 2$. Thus, $d = 16$. ◀

16. (a) What is the order of 3 modulo 23?

▶ **Solution.** From Fermat's theorem $3^{22} \equiv 1 \pmod{23}$. Thus $d = \operatorname{ord}_{23} 3 \mid 22$ so $d = 1, 2, 11,$ or 22. Calculating modulo 23, we have $3^2 \equiv 9$, $3^3 = 27 \equiv 4$, $3^4 \equiv 12$, $3^8 \equiv 12^2 \equiv 144 \equiv 6$, $3^{11} = 3^3 3^8 \equiv 4 \cdot 6 \equiv 24 \equiv 1$. Thus, $\operatorname{ord}_{23} 3 = 11$ since $3^{11} \equiv 1 \pmod{23}$ but $3^2 \not\equiv 1$. ◀

(b) If the order of b modulo m is 15, what is the order of b^6 modulo m.

▶ **Solution.** If $\operatorname{ord}_m b = 15$ then $\operatorname{ord}_m b^6 = 15/(15, 6) = 15/3 = 5$. ◀

17. Use the Chinese Remainder Theorem to solve the simultaneous congruences:

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 1 \pmod 6 \end{aligned}$$

▶ **Solution.** Let $M = 5 \cdot 7 \cdot 6 = 210$, $M_1 = 7 \cdot 6 = 42$, $M - 2 = 5 \cdot 6 = 30$, $M_3 = 5 \cdot 7 = 35$. Then solve the linear congruences:

$M_1 x_1 \equiv 1 \pmod 5 \implies 42 x_1 \equiv 1 \pmod 5 \implies 2x_1 \equiv 1 \pmod 5 \implies x_1 \equiv 3 \pmod 5$

$M_2 x_2 \equiv 1 \pmod 7 \implies 30 x_2 \equiv 1 \pmod 7 \implies 2x_2 \equiv 1 \pmod 7 \implies x_2 \equiv 4 \pmod 7$

$M_3 x_3 \equiv 1 \pmod 6 \implies 35 x_3 \equiv 1 \pmod 6 \implies (-1)x_3 \equiv 1 \pmod 6 \implies x_3 \equiv -1 \pmod 6$.

Then the solution of the simultaneous congruences is

$$\begin{aligned} x &\equiv a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 \pmod M \\ &\equiv 3 \cdot 42 \cdot 3 + 2 \cdot 30 \cdot 4 + 1 \cdot 35 \cdot (-1) \pmod{210} \\ &\equiv 583 \equiv 163 \pmod{210}. \end{aligned}$$

◀

18. (a) Use the Euclidean algorithm to compute the greatest common divisor (2517, 2370).

▶ **Solution.** Use the Euclidean Algorithm:

2517	2370		
1	0	2517	
0	1	2370	
1	−1	147	$= 2517 - 2370$
−16	17	18	$= 2370 - 16 \cdot 147$
129	−137	3	$= 147 - 8 \cdot 18$

Thus, $(2517, 2370) = 3 = 2517 \cdot 129 + 2370 \cdot (-137)$. ◀

(b) Find all integer solutions to the equation $2517x - 2370y = 69$, or explain why there are none.

▶ **Solution.** From part (a), $2517 \cdot 129 + 2370 \cdot (-137) = 3$ and multiplying by 23 gives

$$2517 \cdot 2967 - 2370 \cdot 3151 = 69.$$

That is, $x_0 = 2967$ and $y_0 = 3151$ is one solution to the linear equation. The remaining solutions are given by

$$x_k = x_0 + k\frac{2370}{3} = 2967 + k \cdot 790, \qquad y_k = y_0 + k\frac{2517}{3} = 3151 + k \cdot 839$$

where k is an arbitrary integer. ◀

(c) Solve the linear congruence $2370x \equiv 69 \pmod{2517}$ or explain why there are no solutions.

▶ **Solution.** From part (b), one solution to this linear congruence is $x = -3151 \pmod{2517}$ or $x \equiv 1883 \pmod{2517}$ is the least residue. Since $(2517, 2370) = 3$ there are 3 incongruent solutions modulo 2517:
$x_0 \equiv 1883$, $x_1 = 1883 + \frac{2517}{3} = 1883 + 839 = 2722 \equiv 205$, $x_2 = x_1 + 839 = 1044$ ◀

19. (a) For which odd primes p does the Legendre symbol $\left(\frac{2}{p}\right) = 1$?

▶ **Solution.** $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 8$. ◀

(b) For which distinct odd primes p, q does the Legendre symbol satisfy $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$?

▶ **Solution.** When p and q are both congruent to 3 modulo 4. ◀

(c) Evaluate the Legendre symbol $\left(\frac{431}{1097}\right)$.

▶ **Solution.** Since $1097 \equiv 1 \pmod 4$,

$$\begin{aligned}
\left(\frac{431}{1097}\right) &= \left(\frac{1097}{431}\right) = \left(\frac{2 \cdot 431 + 235}{431}\right) = \left(\frac{235}{431}\right) \\
&= \left(\frac{5}{431}\right)\left(\frac{47}{431}\right) = \left(\frac{431}{5}\right)\left(\frac{47}{431}\right) \\
&= \left(\frac{1}{5}\right)\left(\frac{47}{431}\right) = \left(\frac{47}{431}\right) \\
&= -\left(\frac{431}{47}\right) = -\left(\frac{431}{47}\right) = -\left(\frac{9 \cdot 47 + 8}{47}\right) \\
&= -\left(\frac{8}{47}\right) = -\left(\frac{2^2 \cdot 2}{47}\right) = -\left(\frac{2}{47}\right) = -1,
\end{aligned}$$

where the last equality is because $47 \equiv -1 \pmod 8$. ◀

20. Find a complete solution to the congruence $x^2 - 5x + 6 \equiv 0 \pmod{187}$. (Note that $187 = 11 \cdot 17$.)

▶ **Solution.** First solve $x^2 - 5x + 6 \equiv 0 \pmod{11}$ and $x^2 - 5x + 6 \equiv 0 \pmod{17}$. Since 11 and 17 are prime, each of these quadratic congruences has at most 2 incongruent solutions by Lagrange's theorem. Since $x^2 - 5x + 6 = (x-2)(x-3)$ it is clear that the first congruence has the solutions $x \equiv 2,\ 3 \pmod{11}$ and the second has the solutions $x \equiv 2,\ 3 \pmod{17}$. Thus, to solve the original congruence we need to solve the simultaneous systems

$$\begin{aligned} x &\equiv 2,\ 3 \pmod{11} \\ x &\equiv 2,\ 3 \pmod{17}. \end{aligned}$$

Since $17 \cdot 2 - 11 \cdot 3 = 1$ we get that $34 \equiv 1 \pmod{11}$; $34 \equiv 0 \pmod{17}$ while $-33 \equiv 0 \pmod{11}$; $-33 \equiv 1 \pmod{17}$. Thus, the solutions of the simultaneous congruences are given by

$$x \equiv \{2,\ 3\} \cdot 34 + \{2,\ 3\} \cdot (-33) \pmod{187}.$$

This gives the 4 incongruent solutions

$$\begin{aligned} x_1 &\equiv 2 \cdot 34 - 2 \cdot 33 \equiv 2 \pmod{187} \\ x_2 &\equiv 2 \cdot 34 - 3 \cdot 33 \equiv -31 \equiv 156 \pmod{187} \\ x_3 &\equiv 3 \cdot 34 - 2 \cdot 33 \equiv 36 \pmod{187} \\ x_4 &\equiv 3 \cdot 34 - 3 \cdot 33 \equiv 3 \pmod{187}. \end{aligned}$$

◀

21. Solve $x^2 + x + 2 \equiv 0 \pmod{121}$.

▶ **Solution.** First solve $x^2 + x + 2 \equiv 0 \pmod{11}$. The discriminant is $b^2 - 4ac = 1 - 8 = -7 \equiv 4 \pmod{11}$. The solutions of $y^2 \equiv 4 \pmod{11}$ are $y \equiv \pm 2 \pmod{11}$. Hence the solutions of the quadratic are $x_1 \equiv (-1+2)/2 \equiv 6 \pmod{11}$ and $x_2 \equiv (-1-2)?3 \equiv 8/2 \equiv 4 \pmod{11}$. Extend each of these to a solution of $f(x) = x^2 + x + 2$ modulo 121.

Case 1: $x_1 = 6$. Look for a solution modulo 121 of the form $x_1' = x_1 + 11y$ where y satisfies the linear congruence

$$\frac{f(x_1)}{11} + f'(x_1)y \equiv 0 \pmod{11}.$$

Since $f'(x) = 2x + 1$ this congruence becomes

$$\frac{f(x_1)}{11} + f'(x_1)y \equiv \frac{44}{11} + 13y \equiv 4 + 2y \pmod{11},$$

and hence $y \equiv -2 \equiv 9 \pmod{11}$. Thus, $x_1' = x_1 + 11y = 6 + 11 \cdot 9 \equiv 105 \equiv -16 \pmod{11}$.

Case 1: $x_2 = 4$. Look for a solution modulo 121 of the form $x_2' = x_2 + 11y$ where y satisfies the linear congruence

$$\frac{f(x_2)}{11} + f'(x_2)y \equiv 0 \pmod{11}.$$

Since $f'(x) = 2x + 1$ this congruence becomes

$$\frac{f(x_2)}{11} + f'(x_2)y \equiv \frac{22}{11} + 9y \equiv 2 - 2y \pmod{11},$$

and hence $y \equiv 1 \pmod{11}$. Thus, $x_2' = x_2 + 11y = 4 + 11 \cdot 1 \equiv 15 \pmod{11}$.

Therefore, the only solutions of the quadratic modulo 121 are $x \equiv 15,\ 105 \pmod{121}$. ◀

22. Determine if each of the following congruences have a solution.

(a) $x^2 \equiv 15 \pmod{41}$.

▶ **Solution.** It is necessary to determine if 15 is a quadratic residue modulo 41. For this, use the Legendre symbol.

$$\begin{aligned}
\left(\frac{15}{41}\right) &= \left(\frac{5}{41}\right)\left(\frac{3}{41}\right) \\
&= \left(\frac{41}{5}\right)\left(\frac{41}{3}\right) \text{ since } 41 \equiv 1 \pmod 4 \\
&= \left(\frac{5\cdot 8+1}{41}\right)\left(\frac{13\cdot 3+2}{41}\right) = \left(\frac{1}{5}\right)\left(\frac{2}{3}\right) \\
&= 1 \cdot (-1) = -1.
\end{aligned}$$

Thus, 15 is a quadratic non-residue modulo 41 so the equation $x^2 \equiv 15 \pmod{41}$ is no solvable. ◀

(b) $x^2 + 5x + 7 \equiv 0 \pmod{97}$.

▶ **Solution.** It is necessary to determine if the discriminant is a quadratic residue or non-residue modulo 97. The discriminant is $b^2 - 4ac = 25 - 28 = -3$. Thus compute the Legendre sysmbol

$$\begin{aligned}
\left(\frac{-3}{97}\right) &= \left(\frac{-1}{97}\right)\left(\frac{3}{97}\right) \\
&= 1 \cdot \left(\frac{3}{97}\right) \\
&= \left(\frac{97}{3}\right) = \left(\frac{1}{3}\right) = 1.
\end{aligned}$$

Thus, $x^2 + 5x + 7 \equiv 0 \pmod{97}$ is solvable. ◀

(c) $3x^2 + 4x + 5 \equiv 0 \pmod{51}$.

▶ **Solution.** Since $51 = 3 \cdot 17$, $3x^2 + 4x + 5 \equiv 0 \pmod{51}$ is solvable if and only if $3x^2 + 4x + 5 \equiv 0 \pmod 3$ and $3x^2 + 4x + 5 \equiv 0 \pmod{17}$ are both solvable. The first equation is $4x + 5 \equiv 0 \pmod 3$ which is solvable since $(4, 3) = 1$. For the second one, the congruence is solvable if and only if the discriminant is a quadratic residue modulo 17. The discriminant is $b^2 - 4ac = 16 - 60 = -44 \equiv 7 \pmod{17}$. Now use the Legendre symbol

$$\begin{aligned}
\left(\frac{7}{17}\right) &= \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) \\
&= -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.
\end{aligned}$$

Thus, the discriminant is a quadratic non-residue modulo 17 and hence $3x^2+4x+5 \equiv 0 \pmod{17}$ is not solvable. Therefore, $3x^2+4x+5 \equiv 0 \pmod{51}$ is not solvable. ◀

23. Circle True (T) or False (F). Reasons are not required.

T	F	(a) If $15 \mid a^2$ then $15 \mid a$.
T	F	(b) If $x^2 \equiv 1 \pmod{35}$ then $x \equiv \pm 1 \pmod{35}$.
T	F	(c) $\{21, -3, 13, -15, -4\}$ is a complete residue system modulo 5.
T	F	(d) $7^{753} \equiv 2 \pmod{11}$.
T	F	(e) $\{1, 3, -3, 9\}$ is a reduced residue system modulo 10.
T	F	(f) The Fibonacci numbers satisfy $f_{2n+3} - f_{2n+2} = f_{2n+1}$.
T	F	(g) $\underbrace{72727272727272727272}_{10 \text{ times}} \equiv 6 \pmod{11}$.
T	F	(h) If p is an odd prime then $2^p \equiv 2 \pmod{p}$.
T	F	(i) The composition $\tau(\tau(n))$ is a multiplicative function.
T	F	(j) If p is prime then $\phi(pm) = \phi(m)$.
T	F	(k) $\sum_{d \mid n} \phi(d) = n$.