Do the following exercises from the text:
Section 5.2: 2, 5, 6 (d), 14

2. Find the integer s such that $-2310 \leq x \leq 2310$, and

$$\begin{aligned} x &\equiv 1 \pmod{21} \\ x &\equiv 2 \pmod{20} \\ x &\equiv 3 \pmod{11}. \end{aligned}$$

▶ **Solution.** Since $(21, 20) = (21, 11) = (20, 11) = 1$, the Chinese Remainder Theorem applies. First, solve the linear congruences:

$$\begin{aligned} 20 \cdot 11x &\equiv 1 \pmod{21} \\ 21 \cdot 11x &\equiv 1 \pmod{21} \\ 21 \cdot 20x &\equiv 1 \pmod{11} \end{aligned}$$

For the first one, apply the Euclidean Algorithm to the pair $20 \cdot 11 = 220$ and 21 to get $220 \cdot (-2) + 21 \cdot 21 = 1$ so $x_1 = -2$ solves the first congruence. For the second apply the Euclidean Algorithm to $21 \cdot 11 = 231$ and 20 to get $231 \cdot (-9) + 104 \cdot 20 = 1$ so $x_2 = -9$ is a solution of the second linear congruence. Similarly $21 \cdot 20 = 420$ and the Euclidean Algorithm gives $420 \cdot (-5) + 191 \cdot 11 = 1$ so $x_3 = -5$ is the solution to the third linear congruence. Then a solution to the simultaneous congruences is

$$x = 220 \cdot (-2) \cdot 1 + 231 \cdot (-4) \cdot 2 + 420 \cdot (-5) \cdot 3 = -10,898.$$

and the solution is unique modulo $21 \cdot 20 \cdot 11 = 4620$. Thus, the general solution is $x = -10,898 + 4620k$ where k is any integer. Taking $k = 2$ gives the only solution $-10,898 + 4620 \cdot 2 = -1658$ in the required range. ◀

5. Solve the system

$$\begin{aligned} 2x &\equiv 5 \pmod{7} \\ 4x &\equiv 2 \pmod{6} \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

There will be two incongruence solutions modulo $210 = [7, 6, 5]$; find both of them.

▶ **Solution.** First solve each of the linear congruences separately, and then use the Chinese Remainder Theorem to solve simultaneously. Since $4 \cdot 2 = 8 \equiv 1 \pmod{7}$, the first linear congruence has the solution $x \equiv 4 \cdot 5 \equiv -1 \pmod{7}$. The third one is already given in solved form. For the second, since the greatest common divisor $(4, 6) = 2$ and $2 \mid 2$, there are two incongruence solutions to this congruence. Dividing by 2 gives the congruence $2x \equiv 1 \pmod{3}$ which has the unique solution $x = -1$

modulo 3. The other solution modulo 6 are $-1 + (6/2)k$ modulo 6. Hence there are two solutions -1 and $-1 + 3 = 2$ modulo 6. Thus, there are 2 sets of simultaneous congruences to solve:

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

To solve these, first solve the three linear congruences

$$\begin{aligned} 30x &\equiv 1 \pmod 7 \\ 35x &\equiv 1 \pmod 6 \\ 42x &\equiv 1 \pmod 5 \end{aligned}$$

Reducing moduolo 7, the first congruence becomes $2x \equiv 1 \pmod 7$, which has the solution $x \equiv 4 \pmod 7$. The second has the solution $x \equiv -1 \pmod 6$, and the third, after reducing moduolo 5, is $2x \equiv 1 \pmod 5$, which has the solution $x \equiv 3 \pmod 5$. Then the first set of simultaneous congruences has the solution

$$\begin{aligned} x_1 &= 30 \cdot 4 \cdot (-1) + 35 \cdot (-2) \cdot 2 + 42 \cdot 3 \cdot 3 \\ &= -120 + 35 + 378 = 293 \\ &\equiv 83 \pmod{210}, \end{aligned}$$

and the second set has the solution

$$\begin{aligned} x_2 &= 30 \cdot 4 \cdot (-1) + 35 \cdot (-1) \cdot 2 + 42 \cdot 3 \cdot 3 \\ &= -120 - 70 + 378 \\ &\equiv 188 \pmod{210}. \end{aligned}$$

Thus, the two solutions of the original system of linear congruences are 83 and 188 (mod 210). ◀

6. Solve the following congruences using the method of Theorem 5.3.

(d) $606x \equiv 138 \pmod{1710}$

▶ **Solution.** The prime factorization of 1710 is $1710 = 2 \cdot 3^2 \cdot 5 \cdot 19$. Thus, the congruence $606x \equiv 138 \pmod{1710}$ is equivalent to the simultaneous system of congruences

$$\begin{aligned} 606x &\equiv 138 \pmod 2 \\ 606x &\equiv 138 \pmod 5 \\ 606x &\equiv 138 \pmod 9 \\ 606x &\equiv 138 \pmod{19} \end{aligned}$$

Reducing each of these congruences by the respective modulus gives:

$$\begin{aligned} 0 \cdot x &\equiv 0 \pmod{2} \\ x &\equiv 3 \pmod{5} \\ 3x &\equiv 3 \pmod{9} \\ 17x &\equiv 5 \pmod{19} \end{aligned}$$

Solving these congruences gives:

$$\begin{aligned} &x \equiv 0,\ 1 \pmod{2} \\ &x \equiv 3 \pmod{5} \\ &x \equiv 1,\ 4,\ 7 \pmod{9} \\ &x \equiv 7 \pmod{19}. \end{aligned}$$

To solve these simultaneous congruences, we need to first solve the following linear congruences:

$$\begin{aligned} 5 \cdot 9 \cdot 19x = 855x &\equiv 1 \pmod{2} \\ 2 \cdot 9 \cdot 19x = 342x &\equiv 1 \pmod{5} \\ 2 \cdot 5 \cdot 19x = 190x &\equiv 1 \pmod{9} \\ 2 \cdot 5 \cdot 9x = 90x &\equiv 1 \pmod{19} \end{aligned}$$

Reducing each of these congruences modulo the respective modulus gives

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ 2x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{9} \\ 14x &\equiv 1 \pmod{19} \end{aligned}$$

The solutions of these are, respectively, $x \equiv 1 \pmod{2}$, $x \equiv 3 \pmod{5}$, $x \equiv 1 \pmod{9}$, and $x \equiv -4 \pmod{19}$. To find all the solutions of the simultaneous congruences, compute:

$$x \equiv 855 \cdot 1 \cdot (0 \text{ or } 1) + 342 \cdot 3 \cdot 3 + 190 \cdot 1 \cdot (1 \text{ or } 4 \text{ or } 7) + 90 \cdot (-4) \cdot 7 \pmod{1710}.$$

Do the calculations for each of the 6 choices (0 or 1 in one place and 1 or 4 or 7 in another) to get:

$$x \equiv 178,\ 463,\ 748,\ 1033,\ 1318,\ 1603 \pmod{1710}$$

◀

14. Find all solutions to the system

$$\begin{aligned} 3x^2 + 6x + 5 &\equiv 0 \pmod{7} \\ 7x + 4 &\equiv 0 \pmod{13} \end{aligned}$$

which are incongruence modulo 91.

▶ **Solution.** By direct calculation, we determine that 1 and -3 are solutions of the quadratic congruence. Since the solutions are unique modulo 7 the solutions of the system are of the form $1+7y$ and $-3+7z$ where $7(1+7y)+4 \equiv 0 \pmod{13}$ and $7(-3+7z)+4 \equiv 0 \pmod{13}$. These yield $y=8$ and $z=3$ and hence the solutios 57 and 18 which are unique modulo 91. ◀

Section 5.3: 1, 2, 4

1. Solve:

(a) $5x^3 - 2x + 1 \equiv 0 \pmod{343}$

▶ **Solution.** Since $343 = 7^3$, start by solving $f(x) = 5x^3 - 2s + 1 \equiv 0 \pmod 7$. This will be done by direct calculation:

x	-3	-2	-1	0	1	2	3
$f(x)$	-128	-35	-6	1	4	37	127

The only value of $f(x)$ that is divisible by 7 is -35. Thus, the unique solution of $f(x) \equiv 0 \pmod 7$ is $x_1 \equiv -2 \pmod 7$. Now apply Theorem 5.7 to find a solution (if it exists) of $f(x) \equiv 0 \pmod{49}$. Any such solution will have the form $x_2 = x_1 + 7y$ where y is a solution of the linear congruence

$$\frac{f(x_1)}{7} + yf'(x_1) \equiv 0 \pmod 7.$$

Since $f'(x) = 15x^2 - 2$, $f'(x_1) = f'(-2) = 58 \equiv 2 \pmod 7$, so the linear congruence for y is

$$\frac{-35}{7} + 2y \equiv 0 \pmod 7.$$

This is $-5 + 2y \equiv 0 \pmod 7$ which has the unique solution $y \equiv -1 \pmod 7$, which gives $x_2 = -2 - 7 = -9$ as the unique solution of $f(x) \equiv 0 \pmod{49}$. Now apply Theorem 5.7 again to find a solution of $f(x) \equiv 0 \pmod{343}$. Such a solution will have the form $x_3 = x_2 + 49y$ where y is a solution of the linear congruence

$$\frac{f(x_2)}{49} + yf'(x_2) \equiv 0 \pmod 7.$$

Calculate that $f(-9) = -3626 = (-74)(49)$ and $f'(-9) = 15(-9)^2 - 2$. Since we only need $f'(-9)$ modulo 7, we get that $f'(-9) \equiv 1 \cdot (-2)^2 - 2 \equiv 2 \pmod 7$. Thus, the linear congruence for finding x_3 is $\frac{f(-9)}{49} + yf'(-9) \equiv 0 \pmod 7$ or $-74 + 2y \equiv 0 \pmod 7$ which has the unique solution $y \equiv 2 \pmod 7$. Hence, $x_3 = -9 + 2 \cdot 49 = 89 \pmod{343}$ is the unique solution of $f(x) \equiv 0 \pmod{343}$. ◀

(b) $5x^3 - 2x + 1 \equiv 0 \pmod{25}$

▶ **Solution.** Proceed as in part (a). From the calculations of $f(x)$ in part (a) we see that $x_1 = -2$ is the unique solution of $f(x) \equiv 0 \pmod 5$. A solution modulo 25 is obtained as $x_2 = x_1 + 5y$ where y is a solution of the linear congruence

$$\frac{f(x_1)}{5} + yf'(x_1) \equiv 0 \pmod 5.$$

From calculations done is part (a), this linear congruence for y becomes $-7+3y \equiv 0 \pmod 5$, which has the unique solution $y \equiv -1 \pmod 5$. Thus, the unique solution of $f(x) \equiv 0 \pmod{25}$ is $x_2 = -2 + 5 \cdot (-1) = -7 \equiv 18 \pmod{25}$. ◀

(c) $5x^3 - 2x + 1 \equiv 0 \pmod{8575}$

▶ **Solution.** Since $8575 = 343 \cdot 25$ the solutions of $f(x) \equiv 0 \pmod{8575}$ are the solutions of the simultaneous system

$$\begin{aligned} f(x) &\equiv 0 \pmod{343} \\ f(x) &\equiv 0 \pmod{25} \end{aligned}$$

These two prime power congruences were solved in parts (a) and (b). Thus, it is simply necessary to solve the simultaneous congruences

$$\begin{aligned} x &\equiv 89 \pmod{343} \\ x &\equiv 18 \pmod{25} \end{aligned}$$

This is done via the Chinese Remainder Theorem. Apply the Euclidean Algorithm to the relative prime integers 343 and 25 to get $7 \cdot 343 - 96 \cdot 25 = 1$. Then the solution of the simultaneous congruence is

$$x = 18 \cdot 7 \cdot 343 - 96 \cdot 25 \cdot 89 = -170,382 \equiv 1118 \pmod{8575}.$$

◀

2. Solve $2x^9 + 2x^6 - x^5 - 2x^2 - x \equiv 0 \pmod 5$.

▶ **Solution.** Since $2x^9 + 2x^6 - x^5 - 2x^2 - x = (x^5 - x)(2x^4 + 2x + 1)$ and since $x^5 \equiv x \pmod 5$ for any integer x by Fermat's theorem, it follows that every integer value of x is a solution of the given equation. ◀

4. Solve the system

$$\begin{aligned} 5x^2 + 4x - 3 &\equiv 0 \pmod 6 \\ 3x^2 + 10 &\equiv 0 \pmod{17}. \end{aligned}$$

▶ **Solution.** We solve each congruence separately, and then solve the system using the Chinese Remainder Theorem. For the first congruence, we have

$$\begin{aligned} 5x^2 + 4x - 3 &\equiv 0 \pmod 6 \\ -x^2 + 4x - 3 &\equiv 0 \pmod 6 \\ x^2 - 4x + 3 &\equiv 0 \pmod 6 \\ (x-3)(x-1) &\equiv 0 \pmod 6 \\ x &\equiv 1 \text{ or } 3 \pmod 6. \end{aligned}$$

Similarly,

$$\begin{aligned} 3x^2 + 10 &\equiv 10 \pmod{17} \\ 3x^2 &\equiv 7 \pmod{17} \\ x^2 \equiv 18x^2 \equiv 42 &\equiv 25 \pmod{17} \\ x &\equiv \pm 5 \pmod{17}. \end{aligned}$$

Thus, we must solve the four systems:

$$\begin{aligned} x &\equiv 1 \pmod 6 \\ x &\equiv 5 \pmod{17} \end{aligned} \qquad \begin{aligned} x &\equiv 1 \pmod 6 \\ x &\equiv -5 \pmod{17} \end{aligned}$$

$$\begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv 5 \pmod{17} \end{aligned} \qquad \begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv -5 \pmod{17} \end{aligned}$$

Using the Chinese Remainder Theorem, we find that the solutions are 39, 63, 73 and 97 modulo $102 = 17 \cdot 6$. ◀

Section 5.4: 1, 3, 13

1. Prove the converse of Wilson's Theorem.

▶ **Solution.** Wilson's Theorem says that if p is a prime, then $(p-1)! \equiv -1 \pmod p$. The converse is if $(n-1)! \equiv -1 \pmod n$, then n is prime. Thus, suppose that $(n-1)! \equiv -1 \pmod n$. We show that the assumption n is composite leads to a contradiction. If n is composite, then $n = rs$ for $1 < r < n$ and $1 < s < n$. Thus, $r \mid (n-1)!$, and our assumption is that $(n-1)! = -1 + qn$. Since $r \mid n$, it follows that $r \mid 1$, which is a contradiction since $r > 1$. Thus, n cannot have any factors less than n, except for 1. Thus, n is prime. ◀

3. If p is an odd prime, show that $x^2 \equiv 1 \pmod p$ has precisely 2 incongruent solutions modulo p.

▶ **Solution.** Both 1 and $p-1 \equiv -1 \pmod{p}$ are solutions and $1 \not\equiv p-1 \pmod{p}$ since p is odd. If there were more than two solutions, it would contradict Lagrange's theorem. ◀

13. If p is an odd prime, use Fermat's theorem to show that $x^2 \equiv -1 \pmod{p}$ has a solution only if $p \equiv 1 \pmod{4}$.

▶ **Solution.** Suppose $a^2 \equiv -1 \pmod{p}$. Therefore, $p \nmid a$ and by Fermat's theorem $1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}$. Since p is an odd prime, $1 \not\equiv -1 \pmod{p}$, so $1 \equiv (-1)^{(p-1)/2} \pmod{p}$ can only occur if $(p-1)/2$ is even. That is $(p-1)/2 = 2k$ for some positive integer k, so that $p = 4k+1$. That is $p \equiv 1 \pmod{4}$. ◀