Chapter 4.4
Solutions

1.

(a)

$$9 = 2 \cdot 4 + 1$$
$$4 = 5 \cdot 1 + 0$$

Therefore

$$1 = 9 - 2 \cdot 4$$
$$1 \equiv -2 \cdot 4 \pmod 9.$$

Therefore

$$\overline{4} \pmod 9 \equiv -2 \pmod 9 \equiv 7 \pmod 9$$

(by convention we take the value between 0 and $m - 1$).

(b)

$$141 = 7 \cdot 19 + 8$$
$$19 = 2 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Therefore

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) \\ &= -1 \cdot 8 + 3 \cdot 3 \\ &= -1 \cdot 8 + 3 \cdot (19 - 2 \cdot 8) \\ &= 3 \cdot 19 - 7 \cdot 8 \\ &= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19) \\ &= -7 \cdot 141 + 52 \cdot 19. \\ &\equiv 52 \cdot 19 \pmod{141}. \end{aligned}$$

Therefore

$$\overline{19} \pmod{141} \equiv 52 \pmod{141}.$$

(c)

$$\begin{aligned}
232 &= 2 \cdot 89 + 54 \\
89 &= 1 \cdot 54 + 35 \\
54 &= 1 \cdot 35 + 19 \\
35 &= 1 \cdot 19 + 16 \\
19 &= 1 \cdot 16 + 3 \\
16 &= 5 \cdot 3 + 1 \\
3 &= 3 \cdot 1 + 0
\end{aligned}$$

Therefore

$$\begin{aligned}
1 &= 16 - 5 \cdot 3 \\
&= 16 - 5 \cdot (19 - 1 \cdot 16) \\
&= -5 \cdot 19 + 6 \cdot 16 \\
&= -5 \cdot 19 + 6 \cdot (35 - 1 \cdot 19) \\
&= 6 \cdot 35 - 11 \cdot 19 \\
&= 6 \cdot 35 - 11 \cdot (54 - 1 \cdot 35) \\
&= -11 \cdot 54 + 17 \cdot 35 \\
&= -11 \cdot 54 + 17 \cdot (89 - 1 \cdot 54) \\
&= 17 \cdot 89 - 28 \cdot 54 \\
&= 17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89) \\
&= -28 \cdot 232 + 73 \cdot 89. \\
&\equiv 73 \cdot 89 \pmod{232}.
\end{aligned}$$

Therefore

$$\overline{89} \pmod{232} \equiv 73 \pmod{232}.$$

(d)

$$\begin{aligned}
1231 &= 6 \cdot 189 + 97 \\
189 &= 1 \cdot 97 + 92 \\
97 &= 1 \cdot 92 + 5 \\
92 &= 18 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Therefore

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (92 - 18 \cdot 5) \\
&= -2 \cdot 92 + 37 \cdot 5 \\
&= -2 \cdot 92 + 37 \cdot (97 - 1 \cdot 92) \\
&= 37 \cdot 97 - 39 \cdot 92 \\
&= 37 \cdot 97 - 39 \cdot (189 - 1 \cdot 97) \\
&= -39 \cdot 189 + 76 \cdot 97 \\
&= -39 \cdot 189 + 76 \cdot (1231 - 6 \cdot 189) \\
&= 76 \cdot 1231 - 495 \cdot 189 \\
&\equiv -495 \cdot 189 \pmod{1231}.
\end{aligned}$$

Therefore

$$\overline{189} \pmod{1231} \equiv -495 \pmod{1231} \equiv 736 \pmod{1231}.$$

(e)

$$\begin{aligned}
1232 &= 6 \cdot 189 + 98 \\
189 &= 1 \cdot 98 + 91 \\
98 &= 1 \cdot 91 + 7 \\
91 &= 13 \cdot 7 + 0.
\end{aligned}$$

By Euclid's algorithm, we find that $\gcd(1232, 189) = 7 \neq 1$. The theorem that we saw in class guarantees that an inverse exists if the two numbers are co-prime. Here, 1232 and 189 are not co-prime. Therefore the theorem does not apply !

What do we do ?

3.

This question is an excuse to make you practice more. Take for example $a = 1041$ and $b = 244$.

(a)

$$\begin{aligned}
1041 &= 4 \cdot 244 + 65 \\
244 &= 3 \cdot 65 + 49 \\
65 &= 1 \cdot 49 + 16 \\
49 &= 3 \cdot 16 + 1 \\
16 &= 16 \cdot 1 + 0
\end{aligned}$$

(b)

$$\begin{aligned}
1 &= 49 - 3 \cdot 16 \\
&= 49 - 3 \cdot (65 - 1 \cdot 49) \\
&= -3 \cdot 65 + 4 \cdot 49 \\
&= -3 \cdot 65 + 4 \cdot (244 - 3 \cdot 65) \\
&= 4 \cdot 244 - 15 \cdot 65 \\
&= 4 \cdot 244 - 15 \cdot (1041 - 4 \cdot 244) \\
&= -15 \cdot 1041 + 64 \cdot 244
\end{aligned}$$

(c) We therefore have

$$1 \equiv 64 \cdot 244 \pmod{1041},$$

therefore

$$\overline{244} \pmod{1041} \equiv 64 \pmod{1041}.$$

(d) We therefore have

$$1 \equiv -15 \cdot 1041 \pmod{244},$$

therefore

$$\overline{1041} \pmod{244} \equiv -15 \pmod{244} \equiv 229 \pmod{244}.$$

5.

(a) We have $x = 6a + 3$ for an integer a. Therefore

$$\begin{aligned}
6a + 3 &\equiv 4 \pmod{7} \\
6a &\equiv 1 \pmod{7} \\
6 \cdot 6a &\equiv 6 \cdot 1 \pmod{7} \\
36a &\equiv 6 \pmod{7} \\
a &\equiv 6 \pmod{7}
\end{aligned}$$

Therefore $a = 7b + 6$ for an integer b. We therefore find

$$x = 6(7b + 6) + 3 = 42b + 39 \equiv 39 \pmod{6 \cdot 7}.$$

(b) We start by simplifying the system. It's more simple if all the coefficients are "1"s. The system

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

becomes

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

so

$$\begin{aligned} 25x &\equiv 3 \pmod 6 \\ 8x &\equiv 1 \pmod 7, \end{aligned}$$

so

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

Therfore $x = 6a + 3$ for an integer a. Therefore

$$\begin{aligned} 6a + 3 &\equiv 1 \pmod 7 \\ 6a &\equiv 5 \pmod 7 \\ 6 \cdot 6a &\equiv 6 \cdot 5 \pmod 7 \\ 36a &\equiv 2 \pmod 7 \\ a &\equiv 2 \pmod 7. \end{aligned}$$

Therefore $a = 7b + 2$ for an integer b. We therefore find

$$x = 6a + 3 = 6(7b + 2) + 3 = 42b + 15 \equiv 15 \pmod{6 \cdot 7}.$$

(c) If we take $x = 1$, it works!

But the question asks to proceed by substitution, so here is how to do it.

We have $x = 5a + 1$ for an integer a. Therefore

$$\begin{aligned} 5a + 1 &\equiv 1 \pmod 4 \\ 5a &\equiv 0 \pmod 4 \\ a &\equiv 0 \pmod 4. \end{aligned}$$

Therefore $a = 4b$ for an integer b. So $x = 5a + 1 = 5(4b) + 1 = 20b + 1$. So

$$\begin{aligned} 20b + 1 &\equiv 1 \pmod 3 \\ 2b &\equiv 0 \pmod 3 \\ 2 \cdot 2b &\equiv 0 \pmod 3 \\ 4b &\equiv 0 \pmod 3 \\ b &\equiv 0 \pmod 3. \end{aligned}$$

So $b = 3c$ for an integer c. Therefore

$$x = 20b + 1 = 20(3c) + 1 = 60c + 1 \equiv 1 \pmod{5 \cdot 4 \cdot 3}.$$

(d) This one's a little harder.

We could try to simplify the system. It's simpler if all the coefficients are "1"s. But there's a problem : 2 has no inverse $\mathbb{Z}_4$. So we can't simplify $2x \equiv 2 \pmod 4$. We can simplify the first equation.

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

We'll now proceed by simplifying.
We have $x = 5a + 3$ for an integer a. We therefore have

$$\begin{aligned} 2(5a + 3) &\equiv 2 \pmod 4 \\ 10a &\equiv 0 \pmod 4 \\ 2a &\equiv 0 \pmod 4. \end{aligned}$$

What's the solution to the last congruence ? If $2a \equiv 0 \pmod 4$, then $2a$ is divisible by 4. If $2a$ is divisible by 4, then a is even. Otherwise said, $a \equiv 0 \pmod 2$. We then have $a = 2b$ for an integer b.
We find $x = 5a + 3 = 5(2b) + 3 = 10b + 3$. We therefore have

$$\begin{aligned} 10b + 3 &\equiv 1 \pmod 3 \\ 10b &\equiv 1 \pmod 3 \\ b &\equiv 1 \pmod 3. \end{aligned}$$

So $b = 3c + 1$ for an integer c. We find

$$x = 10b + 3 = 10(3c + 1) + 3 = 30c + 13 \equiv 13 \pmod{5 \cdot 2 \cdot 3}.$$

We use $\pmod{5 \cdot 2 \cdot 3}$ and not $\pmod{5 \cdot 4 \cdot 3}$ because, as we saw, the second congruence is equivalent to a congruence $\pmod 2$.

(e) Here as well, if we take $x = 1$, it works !

But the questions asks to proceed via substitution, so here's how to do it.

We have $x = 4a + 1$ for an integer a. So

$$\begin{aligned} 4a + 1 &\equiv 1 \pmod 9 \\ 4a &\equiv 0 \pmod 9 \\ 7 \cdot 4a &\equiv 7 \cdot 0 \pmod 9 \\ a &\equiv 0 \pmod 9 \end{aligned}$$

So $a = 9b$ for an integer b. Therefore $x = 4a + 1 = 4(9b) + 1 = 36b + 1$.
So

$$\begin{aligned} 36b + 1 &\equiv 1 \pmod{25} \\ 36b &\equiv 0 \pmod{25} \\ 16 \cdot 36b &\equiv 16 \cdot 0 \pmod{25} \\ b &\equiv 0 \pmod{25} \end{aligned}$$

So $b = 25c$ for an integer c. We therefore have

$$x = 36b + 1 = 36(25c) + 1 = 900c + 1 \equiv 1 \pmod{4 \cdot 9 \cdot 25}.$$

7.

(a) It suffices to take $x \equiv 0 \pmod{101 \cdot 103 \cdot 107}$.

(b) No method is imposed. Let's start by simplifying the system of congruences.

$$\begin{aligned} 2x &\equiv 1 \pmod{3} \\ 3x &\equiv 2 \pmod{4} \\ 4x &\equiv 3 \pmod{5} \end{aligned}$$

becomes

$$\begin{aligned} 2 \cdot 2x &\equiv 2 \cdot 1 \pmod{3} \\ 3 \cdot 3x &\equiv 3 \cdot 2 \pmod{4} \\ 4 \cdot 4x &\equiv 4 \cdot 3 \pmod{5} \end{aligned}$$

which becomes

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

It suffices to take $x \equiv 2 \pmod{3 \cdot 4 \cdot 5}$.

9.

(a) Note that $28 = 4 \cdot 7 \equiv 0 \pmod{7}$.

$$\begin{aligned} & 28^{1000000} \pmod{7} \\ & \equiv 0^{1000000} \pmod{7} \\ & \equiv 0 \pmod{7} \end{aligned}$$

(b)

$$\begin{aligned} & 6^{778} \pmod 7 \\ \equiv\ & (-1)^{778} \pmod 7 \\ \equiv\ & 1 \pmod 7 \end{aligned}$$

since 778 is even.

11.

(a)

$$2020! = 1 \cdot 2 \ldots 2019 \cdot 2020 \equiv 0 \pmod{10}$$

since 10 is a factor, so the last digit is 0.

(b)

$$1^1 + 2^2 + 3^3 + 4^4 + \ldots 2019^{2019} + 2020^{2020}$$

(c) We see that $3^4 = 81$ and $11^2 = 121$.

$$\begin{aligned} 3^{400} &= 3^{4 \cdot 100} \\ &\equiv 1^{100} \pmod{10} \\ 11^{400} &= 11^{2 \cdot 200} \\ &\equiv 1^{200} \pmod{10} \end{aligned}$$

So the last digit is $1 + 1 = 2$.

13. The statement is true. Here is a proof by contradiction.
Let $d = \gcd(a, m)$. By hypothesis, we have $d > 1$. We therefore have $a = d\,k$ for an integer k and $m = d\,\ell$ for an integer ℓ. Suppose that a admits a multiplicative inverse $\overline{a} \pmod m$. Then

$$\begin{aligned} m &\equiv 0 \pmod m \\ d\,\ell &\equiv 0 \pmod m \\ k\,d\,\ell &\equiv 0 \pmod m \\ a\,\ell &\equiv 0 \pmod m \\ \overline{a}\,a\,\ell &\equiv 0 \pmod m \\ 1\,\ell &\equiv 0 \pmod m \\ \ell &\equiv 0 \pmod m. \end{aligned}$$

So ℓ is divisible by m. But m is divisible by ℓ. So $m = \ell$. So $m = dm$, that is to say $d = 1$. This is a contradiction.

15. The statement is true. Here is a direct proof :
If $\gcd(a, p) \neq 1$, then $p|a$.

$$\begin{aligned} & a^{p-1} \pmod p \\ \equiv\ & 0^{p-1} \pmod p \\ \equiv\ & 0 \pmod p \\ \not\equiv\ & 1 \pmod p \end{aligned}$$