Complete Solutions to Exercises 3.3

1. (a) We can construct a table to find the solution to $3x \equiv 1 \pmod 5$:

x	0	1	**2**	3	4
$3x \equiv 1 \pmod 5$	0	3	**1**	4	2

Hence $3x \equiv 1 \pmod 5$ has the solution $x \equiv 2 \pmod 5$.

(b) We need to solve $4x \equiv 2 \pmod 7$. Again we can construct a table:

x	0	1	2	3	**4**	5	6
$4x \pmod 7$	0	4	1	5	**2**	6	3

The solution to $4x \equiv 2 \pmod 7$ is $x \equiv 4 \pmod 7$.

(c) The given equation is $7x \equiv 0 \pmod 8$. *How can we solve this?*

Well an obvious solution to this linear congruence is $x \equiv 0 \pmod 8$.

(d) We need to solve $10x \equiv 5 \pmod{13}$. Modulo 13 is a bit too large to construct a table of values for. Remember $10x \equiv 5 \pmod{13}$ implies that $10x - 5$ is a multiple of 13 or $10x - 5 = 13k$. (This is a Diophantine equation $10x - 13k = 5$ because we are interested in integer solutions). Rearranging this to make x the subject gives

$$x = \frac{5 + 13k}{10}$$

Recall that x is an integer so we need a value for k which results in x being an integer. *Which value of k should we choose?*

Makes sense to try $k = 5$ because we already have a 5 on the numerator and we need to divide by 10:

$$x = \frac{5 + 13k}{10} = \frac{5 + 13(5)}{10} = \frac{70}{10} = 7$$

Hence the solution of $10x \equiv 5 \pmod{13}$ is $x \equiv 7 \pmod{13}$.

(e) We are given the linear congruence $8x \equiv 4 \pmod{15}$. To construct a table for modulo 15 we would need to evaluate $8x$ for each of the 15 numbers:

$$x = 0, 1, 2, 3, \cdots, 15$$

Requires too much work. Let us try the method of part (d).

The congruence $8x \equiv 4 \pmod{15}$ means that $8x - 4$ is a multiple of 15 which we can write as:

$$8x - 4 = 15k$$

$$x = \frac{15k + 4}{8} \quad \left[\text{Making } x \text{ the subject}\right]$$

We need to select a value for k such that x is an integer. Try $k = 4$:

$$x = \frac{15k + 4}{8} = \frac{15(4) + 4}{8} = \frac{64}{8} = 8$$

Therefore the solution of $8x \equiv 4 \pmod{15}$ is $x \equiv 8 \pmod{15}$.

(f) We need to solve the linear congruence $9x \equiv 10 \pmod{16}$. Again as 16 requires us to evaluate $9x$ modulo 16 for 16 numbers it is easier to use the method of parts (d) and (e). From $9x \equiv 10 \pmod{16}$ we have the Diophantine equation:

$$9x - 10 = 16k$$

$$x = \frac{16k + 10}{9}$$

Selecting $k = 5$ gives $x = \frac{16k + 10}{9} = \frac{16(5) + 10}{9} = \frac{90}{9} = 10$.

Hence $9x \equiv 10 \pmod{16}$ has the solution $x \equiv 10 \pmod{16}$.

2. (a) *How do we solve* $2x \equiv 25 \pmod{7}$ *?*

The easiest way to solve this is to reduce the 25 modulo 7 so that we have smaller numbers which makes the arithmetic easier. *What is the least non-negative residue of* $25 \pmod{7}$ *?*

$$25 \equiv 4 \pmod{7}$$

It is much easier to solve $2x \equiv 4 \pmod{7}$ rather than $2x \equiv 25 \pmod{7}$.

Since we know $2 \times 2 = 4$ so $x \equiv 2 \pmod{7}$ is the solution to $2x \equiv 25 \pmod{7}$.

A more systematic way is shown below in brackets.

[From $2x \equiv 4 \pmod{7}$ we have $2x - 4 = 7k$ and making x the subject gives

$$x = \frac{7k + 4}{2}$$

Remember x needs to be an integer so we choose k to be 0:

$$x = \frac{7k + 4}{2} = \frac{7(0) + 4}{2} = 2$$

The solution to $2x \equiv 25 \pmod 7$ is $x \equiv 2 \pmod 7$.]

(b) Similarly we can simplify $17x \equiv 3 \pmod 5$ before we solve because

$$17 \equiv 2 \pmod 5$$

Therefore we solve the equation $2x \equiv 3 \pmod 5$ rather than $17x \equiv 3 \pmod 5$.

Solving this $2x \equiv 3 \pmod 5$ by constructing a table:

x	0	1	2	3	**4**
$2x \pmod 5$	0	2	4	1	**3**

The solution of $2x \equiv 3 \pmod 5$ is $x \equiv 4 \pmod 5$. Of course this is also the solution to $17x \equiv 3 \pmod 5$ because $17x \equiv 2x \equiv 3 \pmod 5$.

(c) Similarly simplifying $27x \equiv 33 \pmod{10}$ we have

$$27x \equiv 7x \pmod{10} \quad \text{and} \quad 33 \equiv 3 \pmod{10}$$

Using these results, we have the equivalent equation $7x \equiv 3 \pmod{10}$.

Constructing a table:

x	0	1	2	3	4	5	6	7	8	**9**
$7x \pmod{10}$	0	7	4	1	8	5	2	9	6	**3**

Hence the solution to $7x \equiv 3 \pmod{10}$ is $x \equiv 9 \pmod{10}$ because $9 \times 7 \equiv 63 \equiv 3 \pmod{10}$. This is also the solution to $27x \equiv 33 \pmod{10}$.

(d) We are given the linear congruence $128x \equiv 1 \pmod 5$. We can reduce the 128 modulo 5 because $128 \equiv 3 \pmod 5$. It is much easier to solve

$$3x \equiv 1 \pmod 5 \text{ rather than } 128x \equiv 1 \pmod 5.$$

We solved this linear congruence $3x \equiv 1 \pmod 5$ in question 1(a) of this exercise. The solution to this is $x \equiv 2 \pmod 5$. Hence the solution of $128x \equiv 1 \pmod 5$ is $x \equiv 2 \pmod 5$.

(e) Simplifying $32x \equiv 23 \pmod{21}$ gives $11x \equiv 2 \pmod{21}$. Let us solve this equation $11x \equiv 2 \pmod{21}$. Since we have modulo 21 so establishing a table of

values is going to be tedious. From $11x \equiv 2 \pmod{21}$ we have the Diophantine equation

$$11x - 2 = 21k$$

Making x the subject of this formula gives

$$x = \frac{21k + 2}{11}$$

We need to choose a value for k which results in x being an integer. *What value?*

Well $k = 2$ works because $x = \dfrac{21k + 2}{11} = \dfrac{21(2) + 2}{11} = 4$.

Therefore the solution of $32x \equiv 23 \pmod{21}$ is $x \equiv 4 \pmod{21}$.

(f) We are given the linear congruence $54x \equiv 52 \pmod{53}$. Evaluating 54 and 52 modulo 53 gives

$$54 \equiv 1 \pmod{53} \quad \text{and} \quad 52 \equiv -1 \pmod{53}$$

Instead of solving $54x \equiv 52 \pmod{53}$ it is much easier to solve the equivalent

$$x \equiv -1 \pmod{53}$$

This $x \equiv -1 \pmod{53}$ is the solution but we do *not* have the least non-negative residue modulo 53. *What is* -1 *modulo 53 equal to?*

$$-1 \equiv 52 \pmod{53}$$

Therefore the solution to $54x \equiv 52 \pmod{53}$ is $x \equiv 52 \pmod{53}$.

3. (a) We are given the linear congruence $6x \equiv 2 \pmod{4}$. First we need to find the greatest common divisor of 6 and 4 which is 2. Also 2 divides 2 so we have two incongruent solutions of $6x \equiv 2 \pmod{4}$. Constructing a table:

x	0	**1**	2	**3**
$6x \pmod{4}$	0	**2**	0	**2**

The two solutions of $6x \equiv 2 \pmod{4}$ are $x \equiv 1 \pmod{4}$ and $x \equiv 3 \pmod{4}$.

(b) We need to solve $12x \equiv 6 \pmod{18}$. *How?*

First we need to find the greatest common divisor of 12 and 18; thus

$g = \gcd(12, \ 18) = 6$ and $6 \mid 6$ therefore there are 6 incongruent solutions. *How can we find one solution?*

Well $12x \equiv 6 \pmod{18}$ means that $12x - 6$ is a multiple of 18 or

$$12x - 6 = 18k$$

Making x the subject gives

$$x = \frac{18k + 6}{12}$$

Need to select an integer value for k so that x is an integer. Let $k = 1$ then

$$x = \frac{18k + 6}{12} = \frac{18(1) + 6}{12} = 2$$

One solution of $12x \equiv 6 \pmod{18}$ is $x \equiv 2 \pmod{18}$. *How do we find the other 5 solutions?*

In the text the solutions of $ax \equiv b \pmod{n}$ are given by:

(3.17) $x \equiv x_0,\ x_0 + \left(\frac{n}{g}\right),\ x_0 + 2\left(\frac{n}{g}\right),\ x_0 + 3\left(\frac{n}{g}\right), \cdots,\ x_0 + (g-1)\left(\frac{n}{g}\right) \pmod{n}$

Let x_0 be a particular solution of the linear congruence, so $x_0 = 2$. We have $n = 18$ and $g = 6$. Therefore $\frac{n}{g} = 3$. Substituting these values into the above formula yields

$$\begin{aligned} x &\equiv 2,\ 2+3,\ 2+2(3),\ 2+3(3), 2+4(3),\ 2+5(3) \\ &\equiv 2,\ 5,\ 8,\ 11, 14,\ 17 \pmod{18} \end{aligned}$$

Hence the six solutions of $12x \equiv 6 \pmod{18}$ are $x \equiv 2, 5, 8, 11, 14, 17 \pmod{18}$.

(c) We need to solve $15x \equiv 10 \pmod{25}$. First we find the gcd of 15 and 25.

Clearly $g = \gcd(15,\ 25) = 5$ and $5 \mid 10$ so we have 5 incongruent solutions of $15x \equiv 10 \pmod{25}$.

Let us find an initial solution. We simplify $15x \equiv 10 \pmod{25}$ by Proposition (3.10):

If $ac \equiv bc \pmod{n}$ then $a \equiv b \pmod{\frac{n}{g}}$ where $g = \gcd(c,\ n)$.

Using this on $15x \equiv 10 \pmod{25}$ with $g = 5$ we obtain

$$\frac{15}{5}x \equiv \frac{10}{5} \pmod{\frac{25}{5}} \quad \Leftrightarrow \quad 3x \equiv 2 \pmod{5}$$

Hence the solution to $3x \equiv 2 \pmod{5}$ is

$$x \equiv 4 \pmod 5$$

From $x \equiv 4 \pmod 5$ we obtain $x = 4 + 5t$ which gives

$$\begin{aligned} x &\equiv 4,\ 4+5,\ 4+2(5),\ 4+3(5),\ 4+4(5) \\ &\equiv 4,\ 9,\ 14,\ 19,\ 24 \pmod{25} \end{aligned}$$

Our five incongruent solutions are $x \equiv 4,\ 9,\ 14,\ 19,\ 24 \pmod{25}$.

(d) We are given the linear congruence $7x \equiv 21 \pmod{1001}$. First we find the greatest common divisor of 7 and 1001:

$$g = \gcd(7,\ 1001) = 7\,.$$

Also $7 \mid 21$ so there are seven incongruent solutions to $7x \equiv 21 \pmod{1001}$.

Dividing $7x \equiv 21 \pmod{1001}$ through by $g = \gcd(7,\ 1001) = 7$ gives

$$x \equiv 3 \pmod{143}$$

We can write this as the Diophantine equation

$$x = 143k + 3\,.$$

An obvious choice for k is 0 which gives $x = 3$. Substituting $k = 0, 1, 2, 3, \cdots, 6$ gives

$$\begin{aligned} x &\equiv 3,\ 3+(143),\ 3+2(143),\ 3+3(143),\ 3+4(143),\ 3+5(143),\ 3+6(143) \\ &\equiv 3,\ 146,\ 3+2(143),\ 3+3(143),\ 3+4(143),\ 3+5(143),\ 3+6(143) \\ &\equiv 3,\ 146,\ 289,\ 432,\ 575,\ 718,\ 861 \end{aligned}$$

Our seven *incongruent* solutions are

$$x \equiv 3,\ 146,\ 289,\ 432,\ 575,\ 718,\ 861 \pmod{1001}.$$

4. (a) We need to determine whether $12x \equiv 4 \pmod{18}$ has solutions. The greatest common divisor of 12 and 18 is 6 but $6 \nmid 4$ so there are *no* solutions to the given congruence.

(b) *Does* $13x \equiv 5 \pmod{65}$ *have any solutions?*

The greatest common divisor of 13 and 65 is 13 but $13 \nmid 5$ so there are *no* solutions.

(c) To establish whether $18x \equiv 1 \pmod{16}$ has solutions, we need to find the gcd of 18 and 16. The $\gcd(18,\ 16) = 2$ but $2 \nmid 1$ so there are *no* solutions.

(d) We are given the congruence $1001x \equiv 121 \pmod{11}$. We know 11 is prime.

Does 11 go into 1001?

Yes because $7 \times 11 \times 13 = 1001$ .Therefore $\gcd(11,\ \ 1001) = 11$ and $11 \mid 121$ so the given congruence has 11 incongruent solutions. *How do we find these?*

Since we have 11 incongruent solutions and we are working with modulo 11 so all the integers must be solutions, that is

$$x \equiv 0, 1, 2, \cdots, 10 \pmod{11}$$

Actually the given congruence can be simplified because

$$1001 \equiv 121 \equiv 0 \pmod{11}$$

Therefore the given equation $1001x \equiv 121 \pmod{11}$ is equivalent to

$$0x \equiv 0 \pmod{11}$$

Hence we have the solution $x \equiv 0, 1, 2, \cdots, 10 \pmod{11}$.

(e) We need to test if $15x \equiv 9 \pmod{27}$ has any solutions. First we find the gcd of 15 and 27. Hence $g = \gcd(15,\ \ 27) = 3$ and 3 divides 9 so there are 3 incongruent solutions to $15x \equiv 9 \pmod{27}$.

We simplify $15x \equiv 9 \pmod{27}$ by Proposition (3.10):

> If $ac \equiv bc \pmod{n}$ then $a \equiv b \pmod{\frac{n}{g}}$ where $g = \gcd(c,\ \ n)$.

Using this on $15x \equiv 9 \pmod{27}$ with $g = 3$ gives

$$\frac{15}{3}x \equiv \frac{9}{3} \pmod{\frac{27}{3}} \quad \Leftrightarrow \quad 5x \equiv 3 \pmod{9}.$$

It is much easier to work with modulo 9 rather than 27. We need to find a solution to $5x \equiv 3 \pmod{9}$. We can either create a table or try values of x between 0 and 9 and see which one satisfies $5x \equiv 3 \pmod{9}$. The x value which works is $x \equiv 6 \pmod{9}$. This $x \equiv 6 \pmod{9}$ which implies that x is 6 more than a multiple of 9, that is $x = 6 + 9t$ where t is an integer.

Remember we have 3 incongruent solutions to this equation $15x \equiv 9 \pmod{27}$.

Our 3 solutions can be found by substituting $t = 0, 1, 2$ into $x = 6 + 9t$:

$$x \equiv 6,\ 6+9,\ 6+2(9)$$
$$\equiv 6,\ 15,\ 24 \pmod{27}$$

Hence our solutions to $15x \equiv 9 \pmod{27}$ are $x \equiv 6,\ 15,\ 24 \pmod{27}$.

(f) We are given $407x \equiv 40 \pmod{666}$. Let us first try to find the factors 666.

$$666 = 2 \times 9 \times 37$$

Do any of these numbers, 2, 9 or 37 go into 407?

Clearly 2 and 9 don't. By using a calculator we can see that 37 does go into 407 and $407 = 11 \times 37$. This implies that

$$\gcd(407,\ 666) = \gcd(11 \times 37,\ 2 \times 9 \times 37) = 37.$$

However $37 \not| 40$ so there are *no* solutions to $407x \equiv 40 \pmod{666}$.

5. (a) We are given the linear congruence $10x \equiv 20 \pmod{15}$. First we need to find the greatest common divisor of 10 and 15 which is 5. Let

$$g = \gcd(10,\ 15) = 5.$$

Also $g = 5$ divides 20 so we have 5 incongruent solutions of $10x \equiv 20 \pmod{15}$. It is easier to work with smaller numbers. We have $20 \equiv 5 \pmod{15}$ and using this on the right - hand side gives

$$10x \equiv 20 \equiv 5 \pmod{15}$$

Simplifying $10x \equiv 5 \pmod{15}$ by Proposition (3.10):

If $ac \equiv bc \pmod{n}$ then $a \equiv b \left(\mod \frac{n}{g}\right)$ where $g = \gcd(c,\ n)$.

With $g = 5$ we have

$$10x \equiv 5 \pmod{15} \text{ implies } 2x \equiv 1 \pmod{3}.$$

Much easier to solve $2x \equiv 1 \pmod{3}$. We have

$$2x \equiv 1 \pmod{3} \text{ implies } x \equiv 2 \pmod{3}.$$

From this $x \equiv 2 \pmod{3}$ we have that x is 2 more than a multiple of 3;

$x = 2 + 3t$ where t is an integer. Hence the solutions are given by

$$x \equiv 2,\ 2+3,\ 2+2(3),\ 2+3(3),\ 2+4(3)$$
$$\equiv 2,\ 5,\ 8,\ 11,\ 14 \pmod{15}$$

(b) *How do we find the solutions of* $12x \equiv 18 \pmod{48}$ *?*

Well $\gcd(12,\ 48) = 12$ but $12 \not| 18$ so $12x \equiv 18 \pmod{48}$ has *no* solutions.

(c) We need to solve $12x \equiv 48 \pmod{18}$. First we find the gcd of 12 and 18:

$$g = \gcd(12,\ 18) = 6$$

Next we check if 6 divides 48 which it does so we have six incongruent solutions. We reduce $48 \pmod{18}$ so that we are dealing with smaller numbers:

$$48 \equiv 12 \pmod{18}$$

So we have the equation $12x \equiv 48 \equiv 12 \pmod{18}$. An obvious solution is $x \equiv 1 \pmod{18}$. The 5 other incongruent solutions are found by adding a multiple of $\dfrac{n}{g} = \dfrac{18}{6} = 3$:

$$\begin{aligned} x &\equiv 1, 1+3,\ 1+2(3),\ 1+3(3),\ 1+4(3),\ 1+5(3) \\ &\equiv 1, 4, 7, 10, 13, 16 \pmod{18} \end{aligned}$$

Our solutions are $x \equiv 1, 4, 7, 10, 13, 16 \pmod{18}$.

6. We need to find for which integers b the following congruence $15x \equiv b \pmod{25}$ has solutions. We first need to find the gcd of 15 and 25:

$$\gcd(15,\ 25) = 5$$

The linear congruence $15x \equiv b \pmod{25}$ has solutions $\Leftrightarrow\ 5 \mid b$ or b is a multiple of 5. The set of integers b for which $15x \equiv b \pmod{25}$ has solutions is when b is a multiple of 5. Also the given equation has 5 incongruent solutions.

7. The congruence $nx \equiv b \pmod{n^2}$ has solutions $\Leftrightarrow\ \gcd(n,\ n^2) = n$ and $n \mid b$ or equivalently b is a multiple of n. There are n incongruent solutions.

8. *What do we mean by the multiplicative inverse in modular arithmetic?*
The inverse of a modulo n is the integer $x \pmod{n}$ such that

$$ax \equiv 1 \pmod{n}$$

(a) We need to find the multiplicative inverse of $6 \pmod{13}$. Let x be the inverse of this, so we need to solve $6x \equiv 1 \pmod{13}$.

The $g = \gcd(6, \ 13) = 1$ and 1 divides 1 so have an inverse x. Creating a table:

x	0	1	2	3	4	5	6	7	8	9	10	**11**	12
$6x \pmod{13}$	0	6	12	5	11	4	10	3	9	2	8	**1**	7

Hence the inverse is $x \equiv 11 \pmod{13}$.

(b) Similarly we can find the multiplicative inverse of $5 \pmod{6}$. Let integer $x \pmod{6}$ be the inverse of $5 \pmod{6}$. Therefore we need to solve the linear congruence equation

$$5x \equiv 1 \pmod{6}$$

Since $g = \gcd(5, \ 6) = 1$ so $5 \pmod{6}$ has an inverse. It is much easier to use $5 \equiv -1 \pmod{6}$ because the congruence $5x \equiv 1 \pmod{6}$ is equivalent to

$$5x \equiv 1 \pmod{6} \quad \Leftrightarrow \quad -x \equiv 1 \pmod{6} \quad \Leftrightarrow \quad x \equiv -1 \equiv 5 \pmod{6}$$

Solving $5x \equiv 1 \pmod{6}$ gives $x \equiv 5 \pmod{6}$. Therefore the inverse of $5 \pmod{6}$ is $5 \pmod{6}$. In this case we have what is called **self – invertible**.

In general if $a = x$ and $ax \equiv 1 \pmod{n}$ with $\gcd(a, \ n) = 1$ then we say $a \pmod{n}$ is self invertible.

(c) We need to find x which satisfies $12x \equiv 1 \pmod{17}$. Since $g = \gcd(12, \ 17) = 1$ so $12 \pmod{17}$ does have an inverse. We have to solve the above equation

$$12x \equiv 1 \pmod{17}$$

From $12x \equiv 1 \pmod{17}$ we have the Diophantine equation $12x = 17k + 1$.

Making x the subject gives

$$x = \frac{17k + 1}{12}$$

We need to choose a k such that x is an integer. Let $k = 7$ then

$$x = \frac{17k+1}{12} = \frac{17\left(7\right)+1}{12} = 10$$

Our solution to $12x \equiv 1 \left(\text{mod } 17\right)$ is $x \equiv 10 \left(\text{mod } 17\right)$ so $12^{-1} \equiv 10 \left(\text{mod } 17\right)$.

(d) We need to solve

$$16x \equiv 1 \left(\text{mod } 17\right)$$

We have greatest common divisor of 16 and 17 is equal to 1 (we have already shown that two consecutive integers are relatively prime) so $16 \left(\text{mod } 17\right)$ has an inverse. We can write $16 \equiv -1 \left(\text{mod } 17\right)$ which makes solving $16x \equiv 1 \left(\text{mod } 17\right)$ a lot easier:

$$16x \equiv -x \equiv 1 \left(\text{mod } 17\right) \;\Leftrightarrow\; x \equiv 16 \equiv -1 \left(\text{mod } 17\right)$$

Hence the inverse of $16 \left(\text{mod } 17\right)$ is $16 \left(\text{mod } 17\right)$. This congruence $16 \left(\text{mod } 17\right)$ is self invertible.

(e) We need to find the multiplicative inverse of $9 \left(\text{mod } 101\right)$ which means we need to solve

$$9x \equiv 1 \left(\text{mod } 101\right)$$

This $9x \equiv 1 \left(\text{mod } 101\right)$ means that we are looking for x such that

$$9x - 1 = 101k$$

$$x = \frac{101k+1}{9} \qquad \left(*\right)$$

Recall the test for divisibility by 9 is that the sum of the digits are also divisible by 9. Therefore we look for k such that the sum of digits of $101k+1$ is a multiple of 9. The digits of $101k+1 = k0k+1$ are equal to a multiple of 9. Let us consider the simplest case where the sum of digits are equal to 9:

$$k + k + 1 = 2k + 1 = 9 \quad \Rightarrow\; k = 4$$

Substituting $k = 4$ into the above (*) gives

$$x = \frac{\left(101 \times 4\right)+1}{9} = 45$$

Hence the inverse of $9 \left(\text{mod } 101\right)$ is $45 \left(\text{mod } 101\right)$.

(f) We need to see if $\left(n+1\right)x \equiv 1 \left(\text{mod } n\right)$ has a unique solution. Since n and $n+1$ are relatively prime so the $\gcd\left(n,\;\; n+1\right) = 1$ (two consecutive integers

have no factor in common.) Therefore $\big(n+1\big)x \equiv 1\Big(\text{mod } n\Big)$ has a unique solution and $n+1 \equiv 1\Big(\text{mod } n\Big)$ so

$$\big(n+1\big)x \equiv 1x \equiv x \equiv 1\Big(\text{mod } n\Big)$$

Hence $\big(n+1\big)^{-1} \equiv 1\Big(\text{mod } n\Big)$.

9. (a) We need to find integers a such that the linear congruence $ax \equiv 1\Big(\text{mod } 12\Big)$ has a unique solution. Clearly it is those integers a which have a gcd of 1 with 12 and $1 \le a < 12$ (that is the integers between 1 and 12 that are relatively prime to 12):

$$a = 1,\ 5,\ 7 \text{ and } 11$$

(b) We are interested in integers a below 13 which are relatively prime to 13, that is $\gcd\Big(a,\ \ 13\Big) = 1$. Since 13 is a prime number so all the integers from 1 to 12 have a multiplicative inverse modulo 13.

(c) *Which integers below 15 are relatively prime to 15?*

1, 2, 4, 7, 8, 11, 13 and 14

10. Consider the linear congruence equation $12x \equiv 2\Big(\text{mod } 8\Big)$ then 2 divides 2, 8 and 12 but this equation has *no* solutions. *Why not?*

Because the $\gcd\Big(12,\ \ 8\Big) = 4$ and $4 \not| 2$ so there are no solutions.

11. We need to prove that a modulo p has its own inverse $\Leftrightarrow$ $a \equiv 1\Big(\text{mod } p\Big)$ or $a \equiv -1\Big(\text{mod } p\Big)$.

Proof.

$\Big(\Leftarrow\Big)$. Assume $a \equiv 1\Big(\text{mod } p\Big)$ then multiplying this by $a \equiv 1\Big(\text{mod } p\Big)$ gives

$$aa \equiv \big(1\big)\big(1\big)\Big(\text{mod } p\Big)$$

Simplifying this gives

$$a^2 \equiv 1\Big(\text{mod } p\Big) \quad \Rightarrow \quad a^{-1} \equiv a\Big(\text{mod } p\Big)$$

By carbon copy of the above argument we can show this for $a \equiv -1\Big(\text{mod } p\Big)$.

$\Big(\Rightarrow\Big)$. Assume a modulo p has its own inverse, so we have

$$a^2 \equiv 1 \left(\text{mod } p\right)$$

We can rewrite this as $a^2 \equiv 1^2 \left(\text{mod } p\right)$. By Proposition (3.14) (b):

$$a^2 \equiv b^2 \left(\text{mod } p\right) \Leftrightarrow a \equiv \pm b \left(\text{mod } p\right)$$

Applying this result to $a^2 \equiv 1^2 \left(\text{mod } p\right)$ gives $a \equiv \pm 1 \left(\text{mod } p\right)$.

This completes our proof.

■

12. We are asked to show that if $a^{-1} \equiv b\left(\text{mod } n\right)$ then $b^{-1} \equiv a\left(\text{mod } n\right)$.

Proof.

Suppose $a^{-1} \equiv b\left(\text{mod } n\right)$ then

$$ab \equiv 1\left(\text{mod } n\right) \Rightarrow b\left(a\right) \equiv 1\left(\text{mod } n\right) \Rightarrow b^{-1} \equiv a\left(\text{mod } n\right)$$

This completes our proof.

■

13. We need to show that $a \left(\text{mod } n\right)$ has an inverse $\Leftrightarrow$ a and n are relatively prime.

This is Proposition (3.21).

Proof.

$(\Rightarrow)$ Assume that $a \left(\text{mod } n\right)$ has an inverse, say $x \left(\text{mod } n\right)$. Therefore by the definition of inverse we have

$$ax \equiv 1\left(\text{mod } n\right)$$

By definition of congruence we have

$$ax - 1 = kn \quad \Rightarrow \quad ax - kn = 1$$

This is a Diophantine equation with the unknowns x and $-k$ because we can write the above equation as

$$ax - kn = 1 \Rightarrow ax + \left(-k\right)n = 1$$

This $ax + \left(-k\right)n = 1$ has a solution if the $\gcd\left(a, \quad n\right)$ divides the right-hand-side 1. The only positive factor of 1 is 1 so $\gcd\left(a, \quad n\right) = 1$. Hence a and n are relatively prime.

$(\Leftarrow)$ Now assume that a and n are relatively prime. Therefore we have $\gcd\left(a, \quad n\right) = 1$. Let us examine the linear congruence:

$$ax \equiv 1\left(\text{mod } n\right)$$

By Proposition (3.16):

$ax \equiv b \pmod{n}$ has exactly g solutions provided $g \mid b$ where $g = \gcd(a, \quad n)$.

Since $\gcd(a, \quad n) = 1$ divides 1 so $ax \equiv 1 \pmod{n}$ has a unique solution. Hence by the definition of inverse we have $a \pmod{n}$ has an inverse $x \pmod{n}$. This completes our proof.

■

14. We need to prove that the unique solution of $ax \equiv b \pmod{n}$ is $x \equiv a^{-1}b \pmod{n}$ where $\gcd(a, \quad n) = 1$.

Proof.

We are given that $\gcd(a, \quad n) = 1$ so the linear congruence $ax \equiv b \pmod{n}$ has a unique solution because $1 \mid b$. Since $\gcd(a, \quad n) = 1$ so the linear congruence $ax' \equiv 1 \pmod{n}$ has a unique solution $x' \equiv a^{-1} \pmod{n}$.

Multiplying both sides of $ax \equiv b \pmod{n}$ by $a^{-1} \pmod{n}$ gives

$$a^{-1}(ax) \equiv a^{-1}b \pmod{n}$$

Simplifying the left - hand side we have

$$\underbrace{(a^{-1}a)}_{\equiv 1 \pmod{n}} x \equiv x \equiv a^{-1}b \pmod{n}$$

Hence we have our solution $x \equiv a^{-1}b \pmod{n}$.

■

Let $x \equiv 9^{-1} \pmod{21}$ then we need to solve

$$9x \equiv 1 \pmod{21}$$

Since the $\gcd(9, \quad 21) = 3$ so this congruence $9x \equiv 1 \pmod{21}$ has *no* solution.

15. We are required to prove that for every integer a such that $1 \leq a < p$ where p is prime has a multiplicative inverse.

Proof.

Let a be any arbitrary integer such that $1 \leq a < p$. Since p is prime so $\gcd(a, \quad p) = 1$ because $1 \leq a < p$. This implies that the linear congruence

$ax \equiv 1 \pmod{n}$ has the unique solution $x \equiv a^{-1} \pmod{n}$. As a was arbitrary so every integer a such that $1 \leq a < p$ has a multiplicative inverse modulo p.

■

16. We are asked to show that *none* of the elements in $\{2, 3, \cdots, p-2\}$ modulo p are self-invertible.

Proof.

Let $a \in \{2, 3, \cdots, p-2\}$ and suppose at least one of *a's* is self-invertible. Therefore

$$a^2 \equiv 1 \pmod{p}$$

We can write this as $a^2 \equiv 1^2 \pmod{p}$. Applying Proposition (3.14)(b):

If $a^2 \equiv b^2 \pmod{p}$ then $a \equiv \pm b \pmod{p}$.

To $a^2 \equiv 1^2 \pmod{p}$ gives $a \equiv \pm 1 \pmod{p}$ which implies

$$a \equiv 1 \pmod{p} \quad \text{or} \quad a \equiv -1 \equiv p-1 \pmod{p}$$

However $a \in \{2, 3, \cdots, p-2\}$ which means 1 or $p-1$ are *not* in this set. We have a contradiction, so our supposition that at least one of the a's in $\{2, 3, \cdots, p-2\}$ is self-invertible is wrong. Hence none of the elements in $\{2, 3, \cdots, p-2\}$ modulo p *are* self-invertible.

■

17. We are required to prove that $n(a+b)x \equiv \left[a^2 - b^2\right] \left(\mathrm{mod}\ (a+b)\right)$ has solutions.

Proof.

First, we need to find the greatest common divisor of $n(a+b)$ and $a+b$. This is

$$g = \gcd\left(n(a+b),\ \ a+b\right) = |a+b|$$

Since $a^2 - b^2 = (a-b)(a+b)$ so $|a+b|$ divides $(a-b)(a+b)$. *Why?*

Because

$$|a+b| = \begin{cases} a+b & \text{if} \quad a+b \geq 0 \\ -(a+b) & \text{if} \quad a+b < 0 \end{cases}$$

This implies that $|a+b|$ divides $a+b$ so it divides $(a-b)(a+b) = a^2 - b^2$.

As $g = |a+b|$ divides $\left[a^2 - b^2\right]$ therefore the given equation

$$n(a+b)x \equiv \left[a^2 - b^2\right] \quad \left(\mathrm{mod}\ (a+b)\right)$$

has solutions and there are $g = |a + b|$ incongruent solutions to this equation.

■

18. We are required to prove that $\frac{a}{g}x \equiv b \left(\text{mod } \frac{n}{g}\right)$ has solutions.

Proof.

By Proposition (1.5) of Chapter 1:

$$\gcd(x, \quad y) = g \text{ implies } \gcd\left(\frac{x}{g}, \quad \frac{y}{g}\right) = 1$$

We have $\gcd\left(\frac{a}{g}, \quad \frac{n}{g}\right) = 1$ and 1 divides b so there is a *unique* solution to the linear congruence equation $\frac{a}{g}x \equiv b \left(\text{mod } \frac{n}{g}\right)$.

■

19. First we need to solve the Diophantine equation $15x - 6y = 3$.

Since $g = \gcd(15, \quad -6) = 3$ and 3 divides 3 so we have solutions to $15x - 6y = 3$.

Making x the subject of $15x - 6y = 3$ gives

$$x = \frac{3 + 6y}{15}$$

Substituting $y = 2$, because x and y are integers, gives

$$x = \frac{3 + 6y}{15} = \frac{3 + 6(2)}{15} = 1.$$

Hence one solution is $x = 1, \quad y = 2$. Using Proposition (1.18):

The equation $ax + by = c$ has solutions given by $x = x_0 + \left(\frac{b}{g}\right)t$ and $y = y_0 - \left(\frac{a}{g}\right)t$ where $\gcd(a, \quad b) = g$

With $x_0 = 1$, $b = -6$ and $g = 3$ gives

$$x = x_0 + \left(\frac{b}{g}\right)t = 1 + \left(\frac{-6}{3}\right)t = 1 - 2t.$$

Similarly for y with $a = 15$ we have

$$y = y_0 - \left(\frac{a}{g}\right)t = 2 - \left(\frac{15}{3}\right)t = 2 - 5t.$$

The solution to the given Diophantine equation is

$$x = 1 - 2t \text{ and } y = 2 - 5t.$$

How do we use these solutions to solve $15x \equiv 3 \pmod 6$ *?*

Remember the congruence $15x \equiv 3 \pmod 6$ implies that $15x - 3$ is a multiple of 6 or

$$15x - 3 = 6y$$

Re-arranging this we have $15x - 6y = 3$ which is the given Diophantine equation. The above solution for x is $x = 1 - 2t$. However we are now working with modulo 6 so

$$x \equiv 1 - 2t \pmod 6 \text{ where } 0 \le t \le g - 1$$

We have $g - 1 = 3 - 1 = 2$ so our incongruent solutions are

$$\begin{aligned} x &\equiv 1,\ 1-2,\ 1-4 \qquad \left[\text{Substituting } t = 0,\ 1 \text{ and } 2\right] \\ &\equiv 1, -1, -3 \equiv 1,\ 5,\ 3 \pmod 6 \end{aligned}$$

Our three incongruent solutions are $x \equiv 1,\ 3,\ 5 \pmod 6$.

20. (a) The equivalent congruence to the Diophantine equation $6x + 7y = 100$ is

$$6x \equiv 100 \pmod 7$$

Since $\gcd(6,\ 7) = 1$ we have a unique solution to this congruence.

How can we cut down on the arithmetic we have to do?

Tame 100 because $100 = 2 \pmod 7$ and then solve the equivalent equation

$$6x \equiv 2 \pmod 7 \qquad (*)$$

Also recall that $6 \equiv -1 \pmod 7$. Using this in (*) gives

$$-x \equiv 2 \pmod 7 \text{ implies } x \equiv -2 \equiv 5 \pmod 7$$

Our solution is $x \equiv 5 \pmod 7$. By the definition of congruence, x is 5 more than a multiple of 7; that is $x = 5 + 7t$.

Substituting this $x = 5 + 7t$ into the given Diophantine equation $6x + 7y = 100$ gives

$$6(5 + 7t) + 7y = 100$$

Re-arranging this to make y the subject gives

$$\begin{aligned} y &= \frac{100 - 6(5 + 7t)}{7} \\ &= \frac{100 - 30 - 42t}{7} = \frac{70 - 42t}{7} = 10 - 6t \end{aligned}$$

Hence the general solution of the given Diophantine equation is $x = 5 + 7t$ and $y = 10 - 6t$.

(b) We are given the Diophantine equation $1998x + 100y = 5192$. The equivalent congruence is $1998x \equiv 5192 \pmod{100}$. We need to solve this congruence equation. *How?*

We are working with modulo 100 so $1998x \equiv 5192 \pmod{100}$ simplifies to

$$98x \equiv 92 \pmod{100}$$

Recall that $98 \equiv -2 \pmod{100}$ and $92 \equiv -8 \pmod{100}$. Replacing 98 with -2 and 92 with -8 in the above equation gives

$$-2x \equiv -8 \pmod{100}$$

Multiplying by -1 gives $2x \equiv 8 \pmod{100}$. The $\gcd(2, \ 100) = 2$ so we can divide through by 2 and obtain

$$x \equiv 4 \pmod{50}$$

This gives us the solution $x \equiv 4 \pmod{50}$.

From $x \equiv 4 \pmod{50}$ we have $x = 4 + 50t$. Putting this $x = 4 + 50t$ into the given Diophantine equation $1998x + 100y = 5192$ yields

$$1998(4 + 50t) + 100y = 5192$$

Making y the subject gives

$$y = \frac{5192 - 1998(4 + 50t)}{100}$$
$$= \frac{-2800 - 99900t}{100} = -28 - 999t$$

Our solution to the Diophantine equation is $x = 4 + 50t$ and $y = -28 - 999t$.

21. We need to find $71^{-1} \pmod{771}$. This means we need to solve

$$71x \equiv 1 \pmod{771}$$

By the definition of congruence we have the Diophantine equation

$$71x - 771y = 1 \qquad (*)$$

To see if this has a solution we must find the gcd of 71 and 771. By Euclid's algorithm we have

$$771 = \big(10 \times 71\big) + 61$$
$$71 = \big(1 \times 61\big) + 10$$
$$61 = \big(10 \times 6\big) + 1$$

The gcd of 71 and 771 is 1 so (*) has integer solutions. Working backwards

$$\begin{aligned} 1 &= 61 - \big(10 \times 6\big) \\ &= 61 - \Big(\big[71 - 61\big] \times 6\Big) \\ &= 7\big(61\big) - 6\big(71\big) \\ &= 7\Big(771 - \big(10 \times 71\big)\Big) - 6\big(71\big) \\ &= 7\big(771\big) - 76\big(71\big) = 771\big(7\big) + 71\big(-76\big) \end{aligned}$$

We only need to find x in (*). From the last line we have

$$x \equiv -76 \equiv 695 \big(\text{mod } 771\big)$$

Hence $71^{-1} \equiv 695 \big(\text{mod } 771\big)$.

22. (a) It would have a unique solution if we had a linear congruence $ax \equiv b \left(\text{mod } n\right)$ where the $\gcd\big(a, \quad n\big) = 1$. However we do not have a linear congruence but a quantic equation or an equation of degree 5, $x^5 \equiv x \left(\text{mod } 5\right)$, so we cannot apply the results of linear congruence to these equations.

We need to solve $x^5 \equiv x \left(\text{mod } 5\right)$. We only have the following least non-negative residues of modulo 5:

$$a = 0, \ 1, \ 2, \ \ 3, \ 4, \ 5$$

By evaluating a^5 for each of these a's gives

$$0^5 \equiv 0 \left(\text{mod } 5\right)$$
$$1^5 \equiv 1 \left(\text{mod } 5\right)$$
$$2^5 \equiv 32 \equiv 2 \left(\text{mod } 5\right)$$
$$3^5 \equiv 243 \equiv 3 \left(\text{mod } 5\right)$$
$$4^5 \equiv 1024 \equiv 4 \left(\text{mod } 5\right)$$
$$5^5 \equiv 3125 \equiv 0 \left(\text{mod } 5\right)$$

Note that in the last case $5^5 \equiv 0 \equiv 5 \left(\text{mod } 5\right)$. Therefore each of these residues is a solution to $x^5 \equiv x \left(\text{mod } 5\right)$. We have

$$x \equiv 0, \ 1, \ 2, \ \ 3, \ 4 \ \left(\text{mod } 5\right) \text{ are solutions.}$$

(b) We need to solve $x^5+1\equiv 0\pmod 5$. Rearranging this

$$x^5\equiv -1\pmod 5$$

Clearly $x\equiv -1\equiv 4\pmod 5$ is a solution because $(-1)^5\equiv -1\pmod 5$. Clearly $x\equiv 0\pmod 5$ is not a solution because $0^5\equiv 0\pmod 5$. Trying the other residues gives

$$2^5\equiv 32\equiv 2\not\equiv -1\pmod 5$$

$$3^5\equiv 243\equiv 3\not\equiv -1\pmod 5$$

Therefore $x^5+1\equiv 0\pmod 5$ has the unique solution $x\equiv 4\pmod 5$.

23. (i) Clearly $p\times q=11\times 13=143$ and we are given $e=17$. Bob's public key numbers are 143, 17. We need to find the private key number d which satisfies

$$d=17^{-1}\pmod{(11-1)(13-1)}\equiv 17^{-1}\pmod{120}$$

We need to solve the equation, that is find $x\pmod{120}$ such that

$$17x\equiv 1\pmod{120}$$

By trial and error we have $17\times 7=119$ therefore

$$17\times 7\equiv 119\equiv -1\pmod{120}$$

Multiply both sides of this $17\times 7\equiv 119\equiv -1\pmod{120}$ by -1 gives

$$17\times(-7)\equiv 1\pmod{120}$$

Hence $x\equiv -7\equiv 113\pmod{120}$ or $17^{-1}\equiv 113\pmod{120}$. Therefore $d=113$. Our private key number is 113.

(ii) We are given that $M^e\equiv 12^{17}\equiv a\pmod{143}$. We need to find a modulo 143:

$$12^2\equiv 144\equiv 1\pmod{143}\qquad (*)$$

By using the division algorithm we have $17=(2\times 8)+1$ therefore

$$M^e\equiv 12^{17}\equiv 12^{(2\times 8)+1}\equiv\left(12^2\right)^8\times 12\equiv 1^8\times 12\equiv 12\pmod{143}$$

Therefore $a\equiv 12\pmod{143}$.

For Bob's decryption we need to show that

$$a^d\equiv M\equiv 12\pmod{pq}$$

Well we have $a\equiv 12\pmod{143}$ and $d=113$. Evaluating $a^d\equiv M\pmod{pq}$:

$$12^{113} \equiv M \left(\text{mod}\, 143\right)$$

From (*) we know $12^2 \equiv 1 \left(\text{mod } 143\right)$ so

$$12^{113} \equiv 12^{(56\times 2)+1} \equiv \left(12^2\right)^{56} \times 12 \equiv 1 \times 12 \equiv 12 \left(\text{mod}\, 143\right)$$

This confirms that in this case we have $M \equiv a^d \left(\text{mod}\, pq\right)$.

24. *How do we prove this result?*

We use Proposition (1.18) of chapter 1 which gives the solutions of the Diophantine equation:

If x_0, y_0 are particular solutions of the Diophantine equation

$$ax + by = c$$

and $g \mid c$ where $\gcd\left(a, \quad b\right) = g$ then *all* the other solutions of this equation are given by

$$x = x_0 + \left(\frac{b}{g}\right)t \quad \text{and} \quad y = y_0 - \left(\frac{a}{g}\right)t$$

Proof.

We do the proof in two parts. First we list the solutions and then we show there are exactly g incongruent solutions.

The given congruence $ax \equiv b \left(\text{mod } n\right)$ implies that there is an integer k such that

$$ax - b = kn \text{ which implies } ax - kn = ax + n\left(-k\right) = b$$

Let x_0 be a particular solution to this equation then by applying the above Proposition (1.17) to $ax + n\left(-k\right) = b$ gives the other solutions as

$$x = x_0 + \left(\frac{n}{g}\right)t \quad \text{where } t \text{ is an arbitrary integer and } g = \gcd\left(a, \quad n\right)$$

Substituting $t = 0, \ t = 1, \ t = 2, \ \cdots$ and $t = g - 1$ we have

$$x = x_0, \ x_0 + \left(\frac{n}{g}\right), \ x_0 + 2\left(\frac{n}{g}\right), \ x_0 + 3\left(\frac{n}{g}\right), \cdots, \ x_0 + \left(g-1\right)\left(\frac{n}{g}\right) \qquad (*)$$

Need to show that each of these are *not* congruent modulo n. *How?*

Use proof by contradiction.

Suppose any two numbers in the list (*) are congruent modulo n:

$$x_0 + t_2\left(\frac{n}{g}\right) \equiv x_0 + t_1\left(\frac{n}{g}\right) \left(\text{mod } n\right)$$

Where $0 \le t_1 < t_2 \le g - 1$. By using Definition (3.1):

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad a - b = kn$$

On $x_0 + t_2\left(\frac{n}{g}\right) \equiv x_0 + t_1\left(\frac{n}{g}\right) \pmod{n}$ implies there is an integer $k_1 \geq 1$ such that

$$x_0 + t_2\left(\frac{n}{g}\right) - \left[x_0 + t_1\left(\frac{n}{g}\right)\right] = k_1 n$$

$$\left(t_2 - t_1\right)\left(\frac{n}{g}\right) = k_1 n \qquad \text{[Simplifying and factorizing]}$$

$$t_2 - t_1 \underbrace{=}_{\text{Cancelling } n\text{'s}} k_1 g \quad \text{implies} \quad t_2 = t_1 + k_1 g$$

We have $t_2 = t_1 + k_1 g \geq t_1 + g \geq g$ (because $k_1 \geq 1$) and earlier we had $t_2 \leq g - 1$.

This is a contradiction because we have $t_2 \geq g$ and $t_2 \leq g - 1$.

Hence *none* of the congruences in the above list (*) are congruent to each other modulo n. This means that the list of numbers:

$$x = x_0,\ x_0 + \left(\frac{n}{g}\right),\ x_0 + 2\left(\frac{n}{g}\right),\ x_0 + 3\left(\frac{n}{g}\right), \cdots,\ x_0 + \left(g - 1\right)\left(\frac{n}{g}\right)$$

are *incongruent* modulo n.

Any other solution $x = x_0 + \left(\frac{n}{g}\right)t$ is congruent to one of these in the list modulo n.

Why?

We can show this by using the Division Algorithm on integers t and g.

The Division Algorithm (1.7) of chapter 1:

Let $a,\ b \geq 1$ be given. Then there are unique integers q and r such that

$$a = bq + r \qquad 0 \leq r < b$$

Applying this on the above integers t and g means there are integers q and r such that:

$$t = gq + r \qquad 0 \leq r < g \qquad (\dagger)$$

Substituting this $t = gq + r$ into $x = x_0 + \left(\frac{n}{g}\right)t$ gives

$$\begin{aligned} x \equiv x_0 + \left(\frac{n}{g}\right)t &\equiv x_0 + \left(\frac{n}{g}\right)\big(gq + r\big) \\ &\equiv x_0 + nq + r\left(\frac{n}{g}\right) \\ &\equiv x_0 + \underbrace{0}_{\substack{\text{Because} \\ nq \equiv 0 \,(\mathrm{mod}\ n)}} + r\left(\frac{n}{g}\right) \\ &\equiv x_0 + \left(\frac{n}{g}\right)r \pmod{n} \end{aligned}$$

From (†) we have $0 \le r < g$ which means $r = 0,\ 1,\ 2,\ 3,\ \cdots,\ g-1$ so this $x = x_0 + \left(\frac{n}{g}\right)t$ is in the above list (*) which is:

$$x = x_0,\ \ x_0 + \left(\frac{n}{g}\right),\ \ x_0 + 2\left(\frac{n}{g}\right),\ \ x_0 + 3\left(\frac{n}{g}\right), \cdots,\ \ x_0 + \big(g-1\big)\left(\frac{n}{g}\right)$$

Hence, we have *exactly* g incongruent solutions to $ax \equiv b \pmod{n}$.

■