Complete Solutions to Exercise 3.2

1. (a) We are given $5\times 4 \equiv 5\times 7 \pmod 3$ and this implies $4 \equiv 7 \pmod 3$ is true because

$$4 \equiv 7 \equiv 1 \pmod 3$$

(b) In this case we have $9\times 12 \equiv 9\times 8 \pmod 6$ but is $12 \equiv 8 \pmod 6$?

No because $8 \equiv 2 \pmod 6$ and $12 \equiv 0 \pmod 6$ so $12 \not\equiv 8 \pmod 6$.

(c) Starting with $6\times 11 \equiv 6\times 7 \pmod 8$ and cancelling out the 6 gives $11 \equiv 7 \pmod 8$ but this last congruence is false because

$$11 \equiv 3 \pmod 8 \text{ but } 7 \equiv 7 \pmod 8.$$

Hence $11 \not\equiv 7 \pmod 8$.

(d) We have $13\times 21 \equiv 13\times 7 \pmod{26}$ but clearly $21 \not\equiv 7 \pmod{26}$. We do not have $ac \equiv bc \pmod n \;\Rightarrow\; a \equiv b \pmod n$.

(e) We are given $13\times 31 \equiv 13\times 5 \pmod{26}$. Cancelling out the 13's gives

$$31 \equiv 5 \pmod{26}$$

Is this congruent true?

Yes.

(f) If we cancel out the 101's in the congruence $101\times 35 \equiv 101\times 66 \pmod{31}$ we get $35 \equiv 66 \pmod{31}$. *Is this congruence* $35 \equiv 66 \pmod{31}$ *true?*

Yes because $35 \equiv 4 \pmod{31}$ and $66 \equiv 4 \pmod{31}$.

2. In each case we use Proposition (3.10):

$$ac \equiv bc \pmod n \;\Rightarrow\; a \equiv b \left(\bmod \frac{n}{g}\right) \text{ where } g = \gcd(c,\ n)$$

(a) We need to find x in the following $2x \equiv 2\times 1 \pmod 5$. The $g = \gcd(2,\ 5) = 1$ so

$$x \equiv 1 \pmod 5$$

This $x \equiv 1 \pmod 5$ implies $x-1$ is a multiple of 5 or $x-1=5t$ where t is any integer. Therefore, for any integer t we have $x=1+5t$.

(b) We are given the linear congruence $7x \equiv 7\times 3 \pmod{14}$. We first find the greatest common divisor g of 7 and 14 which is $g=\gcd(7,\ 14)=7$. Applying the above proposition with $g=7$ gives

$$x \equiv 3 \pmod{\frac{14}{7}} \equiv 3 \equiv 1 \pmod 2$$

This congruent $x \equiv 1 \pmod 2$ implies $x-1$ is a multiple of 2 or

$$x-1=2t \ \Rightarrow\ x=1+2t$$

Our solution is $x=1+2t$ for any integer t.

(c) *How do we solve the linear congruence* $10x \equiv 10\times 12 \pmod 6$ *?*

First we need to find the greatest common divisor of 10 and 6; $\gcd(10,\ 6)=2$.

Using Proposition (3.10):

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

gives

$$10x \equiv 10\times 12 \pmod 6 \ \text{ implies } \ x \equiv 12 \pmod{\frac{6}{2}} \equiv 12 \pmod 3 \equiv 0 \pmod 3$$

What does $x \equiv 0 \pmod 3$ *mean?*

It means x is a multiple of 3. Therefore $x=3t$.

An easier way to solve this would be to reduce the congruent from the beginning because $10 \equiv 4 \pmod 6$. Using this we have the equation

$$4x \equiv 4\times 12 \equiv 48 \equiv 0 \pmod 6$$

We have $x \equiv 0 \pmod 6$ which means $x=6s=3(2s)=3t$ where $t=2s$.

Of course, we end up with the same result $x \equiv 0 \pmod 3$ which gives $x=3t$.

(d) We are given the linear congruence $8x \equiv 8\times 5 \pmod{48}$. The

$$g=\gcd(8,\ 48)=8.$$

Applying Proposition (3.10) with $g=8$ we obtain

$$8x \equiv 8\times 5 \pmod{48} \ \Rightarrow\ x \equiv 5 \pmod{\frac{48}{8}} \equiv 5 \pmod 6$$

Therefore $x-5=6t \;\Rightarrow\; x=5+6t$. Our solution is $x=5+6t$.

(e) We can rewrite the given congruence as

$$3\left(-x\right)\equiv 3\times 5\left(\text{mod } 21\right)$$

Since $\gcd\left(3,\;\;21\right)=3$, therefore we have

$$3\left(-x\right)\equiv 3\times 5\left(\text{mod } 21\right) \;\Rightarrow\; -x\equiv 5\left(\text{mod } \frac{21}{3}\right)\equiv 5\left(\text{mod } 7\right)$$

From this $-x\equiv 5\left(\text{mod } 7\right)$ we can multiply both sides by -1 to give

$$x\equiv -5\equiv 2\left(\text{mod } 7\right)$$

Our solution is $x-2=7t$ or $x=2+7t$.

(f) We are given $-12x\equiv 12\times 7\left(\text{mod } 108\right)$. The greatest common divisor of 12 and 108 is 12, this means that $g=\gcd\left(12,\;\;108\right)=12$. Applying Proposition (3.10) gives

$$-12x\equiv 12\times 7\left(\text{mod } 108\right) \;\Rightarrow\; -x\equiv 7\left(\text{mod } \frac{108}{12}\right)\equiv 7\left(\text{mod } 9\right)$$

We have $-x\equiv 7\left(\text{mod } 9\right)$ which is equivalent to $x\equiv -7\equiv 2\left(\text{mod } 9\right)$. Our solution is given by $x=2+9t$.

(g) We need to solve $15x\equiv 0\left(\text{mod } 8\right)$. Note that $\gcd\left(8,\;\;15\right)=1$ and

$$15\equiv 7\equiv -1\left(\text{mod } 8\right)$$

Easier to solve $15x\equiv -x\equiv 0\left(\text{mod } 8\right)$ and multiplying both sides by -1 gives

$$x\equiv 0\left(\text{mod } 8\right)$$

Hence our solution is $x=8t$ which means the integers x which satisfy $15x\equiv 0\left(\text{mod } 8\right)$ are multiples of 8.

3. You should be able to find these examples by trial and error.

(a) $4\times 3\equiv 0\left(\text{mod } 12\right)$ but $4\not\equiv 0\left(\text{mod } 12\right)$ and $3\not\equiv 0\left(\text{mod } 12\right)$.

(b) $7\times 5\equiv 0\left(\text{mod } 35\right)$ but $7\not\equiv 0\left(\text{mod } 35\right)$ and $5\not\equiv 0\left(\text{mod } 35\right)$.

(c) $12\times 15\equiv 0\left(\text{mod } 30\right)$ but $12\not\equiv 0\left(\text{mod } 30\right)$ and $15\not\equiv 0\left(\text{mod } 30\right)$.

4. Similarly for the following result:

$$a\times b\equiv 0\left(\text{mod } n\right) \text{ implies } a\equiv 0\left(\text{mod } n\right) \text{ or } b\equiv 0\left(\text{mod } n\right)$$

We have:

(a) $5\times 12\equiv 0\pmod 6$ implies that $12\equiv 0\pmod 6$.

(b) $6\times 105\equiv 0\pmod{35}$ implies that $105\equiv 0\pmod{35}$.

(c) $84\times 147\equiv 0\pmod 7$ implies that $84\equiv 0\pmod 7$ or $147\equiv 0\pmod 7$.

5. Consider the following:

(a) $10\times 5\equiv 0\pmod 5$ then $10\equiv 5\equiv 0\pmod 5$.

(b) $78\times 91\equiv 0\pmod{13}$ then $78\equiv 91\equiv 0\pmod{13}$.

(c) $85\times 153\equiv 0\pmod{17}$ then $85\equiv 153\equiv 0\pmod{17}$.

6. We need to prove $x^2\equiv 0\pmod p$ gives $p\mid x$.

Proof.

Applying Proposition (3.14):

> If $a\times b\equiv 0\pmod p$ where p is prime then $a\equiv 0\pmod p$ or $b\equiv 0\pmod p$.

To $x^2\equiv 0\pmod p$ gives $x\equiv 0\pmod p$. From the definition of congruence $x\equiv 0\pmod p$ we have $p\mid x$.

■

7. We are required to prove $a^2\equiv b^2\pmod p \Leftrightarrow a\equiv \pm b\pmod p$

How do we prove this result?

Again we use Proposition (3.14):

> If $x\times y\equiv 0\pmod p$ where p is prime then $x\equiv 0\pmod p$ or $y\equiv 0\pmod p$.

Proof.

$(\Leftarrow)$. Assume $a\equiv \pm b\pmod p$ and squaring this gives

$$a^2\equiv b^2\pmod p$$

$(\Rightarrow)$. From the given congruence $a^2\equiv b^2\pmod p$ we have

$$a^2-b^2\equiv 0\pmod p$$

Factorizing the left - hand side gives

$$(a-b)(a+b)\equiv 0\pmod p$$

Applying the above Proposition (3.14) with $x=a-b$ and $y=a+b$ we have

$$a-b\equiv 0\left(\text{mod } p\right) \quad \Leftrightarrow \quad a\equiv b\left(\text{mod } p\right) \text{ or}$$
$$a+b\equiv 0\left(\text{mod } p\right) \quad \Leftrightarrow \quad a\equiv -b\left(\text{mod } p\right)$$

Also by the definition of congruence $a-b\equiv 0\left(\text{mod } p\right)$ and $a+b\equiv 0\left(\text{mod } p\right)$ we have

$$p\,\Big|\,\left(a-b\right) \text{ or } p\,\Big|\,\left(a+b\right).$$

This completes our proof.

■

8. (a) We can write $25=5^2$ and so

$$x^2\equiv 25\equiv 5^2\equiv 2^2\equiv 1\left(\text{mod } 3\right) \text{ or } x^2-1^2\equiv 0\left(\text{mod } 3\right)$$

Applying Proposition (3.14) (b) to $x^2\equiv 1\left(\text{mod } 3\right)$ gives

$$x\equiv 1,\ -1\equiv 1,\ 2\left(\text{mod } 3\right)$$

From this $x\equiv 1\left(\text{mod } 3\right)$ we have $x-1=3t$ for any integer t. Similarly $x\equiv 2\left(\text{mod } 3\right)$ gives $x-2=3s$ for any integer s. Our general solution is

$$x=1+3t \text{ or } x=3s+2.$$

where s and t are any integers.

(b) Similarly for $x^2\equiv 100\left(\text{mod } 11\right)$ we can write $100=10^2$ so

$$x^2\equiv 10^2 \underset{\substack{\text{Because } 10\equiv -1\left(\text{mod } 11\right)\\ \circlearrowleft}}{\equiv} \left(-1\right)^2\equiv 1\left(\text{mod } 11\right)$$

Applying Proposition (3.14) (b) to $x^2\equiv 1\left(\text{mod } 11\right)$ yields

$$x\equiv 1,\ -1\equiv 1,\ 10\left(\text{mod } 11\right)$$

Let s and t be any integers then the general solution is given by:

$$x\equiv 1\left(\text{mod } 11\right) \text{ implies } \ x=1+11s$$
$$x\equiv 10\left(\text{mod } 11\right) \text{ implies } \ x=10+11t$$

Our general solution is $x=1+11s$ or $x=10+11t$ for any integers s and t.

9. (i) We need to disprove that if $\gcd\left(x,\ \ n\right)=1$ and $x^2\equiv 1\left(\text{mod } n\right)$ then $x\equiv \pm 1\left(\text{mod } n\right)$. *How?*

By producing a counter example:

Let $x=4,\ \ n=15$ then $\gcd\left(4,\ \ 15\right)=1$ but

$$4^2 \equiv 16 \equiv 1 \pmod{15} \text{ and } 4 \not\equiv \pm 1 \pmod{15}$$

(ii) The following is a counter example to $\gcd(x, \ n) = 1$ and $x^2 \equiv a \pmod{n}$ then $x \equiv \pm a \pmod{n}$:

$$x^2 \equiv 10 \pmod{39} \quad \Rightarrow \quad x \equiv 7, 19, 20, 32 \pmod{39}$$

You may be wondering how we got these solutions. Brute force.

10. We are asked to show that if $a^n \equiv 0 \pmod{p}$ where p is prime then $a \equiv 0 \pmod{p}$. *How do we prove this result?*

By mathematical induction.

Proof.

Clearly the result holds for $n = 1$ because we are given $a^n \equiv 0 \pmod{p}$ so

$$a^1 \equiv a \equiv 0 \pmod{p}$$

Assume the result is true for $n = k$, that is

$$a^k \equiv 0 \pmod{p} \text{ implies } a \equiv 0 \pmod{p} \qquad (*)$$

Required to prove the result for $n = k+1$ which means we have to show

$$a^{k+1} \equiv 0 \pmod{p} \text{ implies } a \equiv 0 \pmod{p}.$$

Consider $a^{k+1} \equiv 0 \pmod{p}$. By the rules of indices we have

$$a^{k+1} \equiv a^k \times a \equiv 0 \pmod{p}$$

Applying Proposition (3.14) (a):

$$a \times b \equiv 0 \pmod{p} \quad \Rightarrow \quad a \equiv 0 \pmod{p} \text{ or } b \equiv 0 \pmod{p}$$

To $a^{k+1} \equiv a^k \times a \equiv 0 \pmod{p}$ gives

$$a^k \equiv 0 \pmod{p} \text{ or } a \equiv 0 \pmod{p}$$

If $a \equiv 0 \pmod{p}$ then we are done. If $a^k \equiv 0 \pmod{p}$ then by (*) we have

$$a \equiv 0 \pmod{p}$$

By mathematical induction we have $a^n \equiv 0 \pmod{p}$ implies $a \equiv 0 \pmod{p}$.

This completes our proof.

■