## Complete Solutions to Exercises 1.2

1. Applying the division algorithm in each case gives:
   (a) $31 = 7\big(4\big) + 3$ so quotient is 7 and remainder is 3.
   (b) $-1001 = -84\big(12\big) + 7$. The quotient is $-84$ and remainder is 7.
   (c) $-10\,001 = -73\big(137\big) + 0$ therefore, the quotient is $-73$ and remainder is 0.

2. We need to prove that the square of any integer is of the form $4m$ or $4m+1$.
   We give two proofs.
   *Proof 1.*
   Let $a$ be an integer. Then $a$ is even or odd.
   If $a$ is even, then we write this as $a = 2k$ where $k$ is an integer. Squaring this yields

$$a^2 = \big(2k\big)^2 = 4k^2 = 4m \text{ where } m = k^2.$$

   If $a$ is odd then we can write this as $a = 2k+1$ where $k$ is an integer. Similarly we have

$$\begin{aligned} a^2 &= \big(2k+1\big)^2 \\ &= 4k^2 + 4k + 1 = 4\big(k^2 + k\big) + 1 = 4m + 1 \end{aligned}$$

   where $m = k^2 + k$.
   In both cases we have shown that the square of an integer is of the form $4m$ or $4m+1$.
   *Proof 2.*
   We use the Division Algorithm (1.7):

> Given any integers $a$ and $b \geq 1$ there exist *unique* integers $q$ and $r$ such that
> $$a = bq + r \qquad 0 \leq r < b$$

   Let $b = 4$ and $n$ be any integer then

$$n = 4q + r \qquad r = 0, 1, 2, 3$$

   Squaring this gives

$$\begin{aligned} n^2 = \left(4q + r\right)^2 &= 16q^2 + 8qr + r^2 \\ &= 4\left(4q^2 + 2qr\right) + r^2 \\ &= 4\left(4q^2 + 2qr\right) + 0^2,\ 4\left(4q^2 + 2qr\right) + 1^2,\ 4\left(4q^2 + 2qr\right) + 2^2,\ 4\left(4q^2 + 2qr\right) + 3^2 \\ &= 4k + 0,\ 4k + 1,\ 4k + 4 = 4\left(k + 1\right),\ 4m + 9 = 4\left(k + 2\right) + 1 \\ &= 4k,\ 4k + 1,\ 4\left(k + 1\right),\ 4\left(k + 2\right) + 1 \end{aligned}$$

Hence $n^2$ is of the form $4m$ or $4m + 1$.

■

3. By applying the Division Algorithm (1.7):

> Given any integers $a$ and $b \geq 1$ there exist *unique* integers $q$ and $r$ such that
> $$a = bq + r \qquad 0 \leq r < b$$

With $b = 8$:

$$n = 8q + r \qquad 0 \leq r < 8$$

Taking the fourth power of this using the binomial expansion with (I.37):

$$\left(a + b\right)^n = C_n a^n + C_{n-1} a^{n-1} b + C_{n-2} a^{n-2} b^2 + C_{n-3} a^{n-3} b^3 + \ldots + C_0 b^n$$

Recall the $C$'s are the coefficients obtained by Pascal's triangle. We have

$$n^4 = \left(8q + r\right)^4 \underset{\text{By binomial}}{=} \underbrace{\left(8q\right)^4 + 4\left(8q\right)^3 r + 6\left(8q\right)^2 r^2 + 4\left(8q\right) r^3}_{=8k} + r^4 = 8k + r^4$$

Since $0 \leq r < 8$ so

$$r = 0,\ 1,\ 2,\ 3,\ \cdots,\ 7$$

Finding the remainder $r'$ for each of these to the power 4;

$$0^4 = 0 = 0\left(8\right) + 0 \quad \text{gives} \quad r' = 0$$

$$1^4 = 1 = 0\left(8\right) + 1 \quad \text{gives} \quad r' = 1$$

$$2^4 = 16 = 2\left(8\right) + 0 \quad \text{gives} \quad r' = 0$$

$$3^4 = 81 = 10\left(8\right) + 1 \quad \text{gives} \quad r' = 1$$

$$4^4 = 256 = 32\left(8\right) + 0 \quad \text{gives} \quad r' = 0$$

$$5^4 = 625 = 78\left(8\right) + 1 \quad \text{gives} \quad r' = 1$$

$$6^4 = 1296 = 162\left(8\right) + 0 \quad \text{gives} \quad r' = 0$$

$$7^4 = 2401 = 300\left(8\right) + 1 \quad \text{gives} \quad r' = 1$$

$r^4$ can only take values 0 and 1 for the reminder after dividing by 8. Hence the fourth power of any integer has the form

$$n^4 = 8k + r^4 = 8k \quad \text{or} \quad 8k+1$$

[There is a simpler way of doing this problem:

Consider two cases of $n$ – is even and odd.

Let $n = 2m$ then

$$n^4 = \left(2m\right)^4 = 16m^4 = 8\left(2m^4\right) = 8k \quad \text{where } k = 2m^4$$

Let $n = 2m+1$ then

$$\begin{aligned}\left(2m+1\right)^4 &= \left(2m\right)^4 + 4\left(2m\right)^3 + 6\left(2m\right)^2 + 4\left(2m\right) + 1 \\ &= 8\left(2m^4\right) + 8\left(4m^3\right) + 8\left(3m^2\right) + 8m + 1 \\ &= 8\underbrace{\left[2m^4 + 4m^3 + 3m^2 + m\right]}_{=k} + 1 \\ &= 8k + 1\end{aligned}$$

Hence fourth power of any integer is of the form $8k$ or $8k+1$.]

4. We need to prove that $6 \mid \left(a^3 + 5a\right)$.

*Proof.*

Let $a$ be any integer. By the Division Algorithm (1.7) :

> Given any integers $a$ and $b \geq 1$ there exist *unique* integers $q$ and $r$ such that
> $$a = bq + r \qquad 0 \leq r < b$$

With $b = 6$ we have

$$a = 6q + r \qquad 0 \leq r < 6$$

Now substituting this $a = 6q + r$ into $a^3 + 5a$ gives

$$a^3 + 5a = \left(6q + r\right)^3 + 5\left(6q + r\right)$$

We expand $\left(6q + r\right)^3$ by the binomial expansion using Pascal's triangle (I.37):

$$\left(a+b\right)^n = C_n a^n + C_{n-1}a^{n-1}b + C_{n-2}a^{n-2}b^2 + C_{n-3}a^{n-3}b^3 + \ldots + C_0 b^n$$

We have

$$\begin{aligned} a^3+5a &= \left(6q+r\right)^3+5\left(6q+r\right) \\ &= \left(6q\right)^3+3\left(6q\right)^2 r+3\left(6q\right)r^2+r^3+5\left(6q\right)+5r \\ &= \underbrace{\left(6q\right)^3+3\left(6q\right)^2 r+3\left(6q\right)r^2+5\left(6q\right)}_{\text{multiple of 6}}+r^3+5r \\ &= 6k+r^3+5r \end{aligned}$$

Clearly $6 \mid 6k$. We need to show that $6 \mid \left(r^3+5r\right)$. Substituting possible values of $r$ which are $r=0,\ 1,\ 2,\ 3,\ 4,\ 5$ because $0 \le r < 6$. No point substituting $r=0$ because $a^3+5a=6k+r^3+5r=6k$. Substituting the remaining values of $r$ gives

$$\begin{aligned} 1^3+\left(5\times 1\right)=6 &\quad\Rightarrow\quad 6 \mid 6 \\ 2^3+\left(5\times 2\right)=18 &\quad\Rightarrow\quad 6 \mid 18 \\ 3^3+\left(5\times 3\right)=42 &\quad\Rightarrow\quad 6 \mid 42 \\ 4^3+\left(5\times 4\right)=84 &\quad\Rightarrow\quad 6 \mid 84 \\ 5^3+\left(5\times 5\right)=150 &\quad\Rightarrow\quad 6 \mid 150 \end{aligned}$$

Hence $6 \mid \left(r^3+5r\right)$ for every remainder value. Therefore $6 \mid \left(a^3+5a\right)$ for any integer $a$. This finishes our proof.

■

5. (i) We are asked to prove that $7 \mid \left(a^6-1\right)$ where $\gcd\left(a,\ \ 7\right)=1$.

*Proof.*

Let $a$ be an integer such that $\gcd\left(a,\ \ 7\right)=1$. We write $a$ by using the Division Algorithm (1.7):

> Given any integers $a$ and $b \ge 1$ there exist *unique* integers $q$ and $r$ such that
> $$a=bq+r \qquad 0 \le r < b$$

With $b=7$ and $r>0$ because we are given $\gcd\left(a,\ \ 7\right)=1$ (with $r=0$ we have $a=7q$ and so $\gcd\left(a,\ \ 7\right)=7$):

$$a=7q+r \qquad 0<r<7$$

Substituting this $a=7q+r$ into $a^6-1$ gives

$$\begin{aligned} a^6-1 &= \left(7q+r\right)^6-1 \\ &= 7k+r^6-1 \qquad \left[\text{where } k \text{ is an integer}\right] \end{aligned}$$

We know that $7 \mid 7k$ so we only need to show that $7 \mid \left(r^6 - 1\right)$. Substituting possible $r$ values, $r = 1, 2, 3, 4, 5$ and $6$ into $r^6 - 1$ gives

$$\begin{aligned} 1^6 - 1 = 0 &\Rightarrow 7 \mid 0 \\ 2^6 - 1 = 63 &\Rightarrow 7 \mid 63 \\ 3^6 - 1 = 728 &\Rightarrow 7 \mid 728 \\ 4^6 - 1 = 4095 &\Rightarrow 7 \mid 4095 \\ 5^6 - 1 = 15624 &\Rightarrow 7 \mid 15624 \\ 6^6 - 1 = 46655 &\Rightarrow 7 \mid 46655 \end{aligned}$$

Hence $7 \mid \left(r^6 - 1\right)$. Since $7 \mid 7k$ and $7 \mid \left(r^6 - 1\right)$ so

$$7 \mid \underbrace{\left(7k + r^6 - 1\right)}_{= a^6 - 1} \text{ which implies } 7 \mid \left(a^6 - 1\right)$$

This completes our proof. ■

(ii) This time we need to prove $7 \mid \left(a^7 - a\right)$.

We consider two cases; $\gcd\left(a, \ 7\right) = 1$ and $\gcd\left(a, \ 7\right) \neq 1$ [Not equal to 1]

*Proof.*

Case I: $\gcd\left(a, \ 7\right) = 1$.

We have

$$7 \mid \left(a^7 - a\right) \ \Leftrightarrow \ 7 \mid a\left(a^6 - 1\right)$$

From part (i) we have that $7 \mid \left(a^6 - 1\right)$ provided $\gcd\left(a, \ 7\right) = 1$. Therefore

$$7 \mid a\left(a^6 - 1\right) \ \text{[Because if } x \mid y \text{ then } x \mid yz \text{]}$$

Case II: $\gcd\left(a, \ 7\right) \neq 1$

The only factors of 7 are 1 and 7 and since $\gcd\left(a, \ 7\right) \neq 1$ so

$$\gcd\left(a, \ 7\right) = 7$$

This implies that $7 \mid a$ which gives $7 \mid a\left(a^6 - 1\right)$.

In either case we have

$$7 \mid a\left(a^6 - 1\right) \text{ which implies } 7 \mid \left(a^7 - a\right)$$

This completes our proof.

■

6. We need to prove $11 \mid \left(a^{11} - a\right)$. *How?*

We apply the division algorithm to an arbitrary integer $a$ with $b = 11$.

*Proof.*

Let $a$ be an arbitrary integer then by Division Algorithm (1.7):

> Given any integers $a$ and $b \geq 1$ there exist *unique* integers $q$ and $r$ such that
> $$a = bq + r \qquad 0 \leq r < b$$

With $b = 11$ we have

$$a = 11q + r \qquad 0 \leq r < 11$$

Substituting this $a = 11q + r$ into $a^{11} - a$ gives

$$\begin{aligned} a^{11} - a &= \left(11q + r\right)^{11} - \left(11q + r\right) \\ &= 11k + r^{11} - r \quad \left[\text{where } k \text{ is some integer}\right] \end{aligned}$$

Clearly $11 \mid 11k$ and we only need to prove that $11 \mid \left(r^{11} - r\right)$ where the integer $r$ satisfies $r = 0,\ 1,\ 2,\ \cdots,\ ,\ 9,\ 10$. Evaluating each of these $r^{11} - r$ values gives

$$\begin{aligned} 0^{11} - 0 = 0 &\ \Rightarrow\ 11 \mid 0 \\ 1^{7} - 1 = 0 &\ \Rightarrow\ 11 \mid 0 \\ 2^{11} - 2 = 2046 &\ \Rightarrow\ 11 \mid 2046 \\ 3^{11} - 3 = 177144 &\ \Rightarrow\ 11 \mid 177144 \\ 4^{11} - 4 = 4194300 &\ \Rightarrow\ 11 \mid 4194300 \\ \vdots \qquad\qquad \vdots &\qquad\qquad \vdots \\ 10^{11} - 10 = 99999999990 &\ \Rightarrow\ 11 \mid 99999999990 \end{aligned}$$

Hence for each remainder $r$ we have $11 \mid \left(r^{11} - r\right)$. Therefore

$$11 \mid \left(a^{11} - a\right)$$

This completes our proof.

■

7. *Proof*

If $b$ is positive then we are done because we have the result by the Division Algorithm. If $b$ is negative, $b < 0$, then we consider $|b| > 0$. Applying the Division Algorithm to $a$ and $|b| > 0$ we have

$$a = |b|q + r \qquad 0 \le r < |b|$$

Remember

$$|b| = \begin{cases} b & \text{if } b \ge 0 \\ -b & \text{if } b < 0 \end{cases}$$

In the case where $|b| = -b$ we can write the above expression

$$a = |b|q + r = -bq + r \underbrace{=}_{\text{Let } q' = -q} bq' + r \qquad 0 \le r < |b|$$

This completes our proof.

■