Book Elementary Number Theory by Burton Exercises

Jason Sass

May 31, 2025

Chapter 1 Preliminaries

Chapter 1.1 Mathematical Induction

Example 1. For all $n \in \mathbb{Z}^+$, $\sum_{k=0}^{n-1} 2^k = 2^n - 1$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : \sum_{k=0}^{n-1} 2^k = 2^n - 1\}$.

Basis:

Since $1 \in \mathbb{Z}^+$ and $\sum_{k=0}^{1-1} 2^k = \sum_{k=0}^{0} 2^k = 1 = 2^1 - 1$, then $1 \in S$.

Induction:

Let $m \in \mathbb{Z}^+$ such that $m \in S$.

Then $\sum_{k=0}^{m-1} 2^k = 2^m - 1$.

Since $m \in \mathbb{Z}^+$, then $m + 1 \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned}
\sum_{k=0}^{(m+1)-1} 2^k &= \sum_{k=0}^{m} 2^k \\
&= \sum_{k=0}^{m-1} 2^k + 2^m \\
&= (2^m - 1) + 2^m \\
&= 2 \cdot 2^m - 1 \\
&= 2^{m+1} - 1.
\end{aligned}$$

Since $m + 1 \in \mathbb{Z}^+$ and $\sum_{k=0}^{(m+1)-1} 2^k = 2^{m+1} - 1$, then $m + 1 \in S$.

Hence, $m \in S$ implies $m + 1 \in S$ for all $m \in \mathbb{Z}^+$.

Since $1 \in S$ and $m \in S$ implies $m + 1 \in S$ for all $m \in \mathbb{Z}^+$, then by induction, $S = \mathbb{Z}^+$, so $\sum_{k=0}^{n-1} 2^k = 2^n - 1$ for all $n \in \mathbb{Z}^+$. □

Example 2. If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + 2^3 + ... + 2^n = 2^{n+1} - 1$.

Proof. Suppose $n \in \mathbb{N}$.

Let S_n be the number

$$S_n = 2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} + 2^n \tag{1}$$

We must show that $S_n = 2^{n+1} - 1$.

Multiply both sides of Equation 1 by 2 to get

$$2S_n = 2^1 + 2^2 + 2^3 + \cdots + 2^n + 2^{n+1} \tag{2}$$

Now subtract 1 from both sides of Equation 2 to get

$$2S_n - 1 = 2^1 + 2^2 + 2^3 + \cdots + 2^n + 2^{n+1} - 1 \tag{3}$$

From Equation 1 we know that $S_n - 1 = 2^1 + 2^2 + 2^3 + \cdots + 2^n$ so we can substitute this fact into Equation 3 to get

$$2S_n - 1 = (S_n - 1) + 2^{n+1} - 1 \tag{4}$$

Now add 1 to both sides of Equation 4 to get

$$2S_n = S_n + 2^{n+1} - 1 \tag{5}$$

Now subtract S_n from both sides of Equation 5 to get

$$S_n = 2^{n+1} - 1$$

□

Example 3. Let (a_n) be the Lucas sequence defined by $a_1 = 1$ and $a_2 = 3$ and $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$.

Then $a_n < (\dfrac{7}{4})^n$ for all $n \in \mathbb{Z}^+$.

Proof. Let $p(n)$ be the predicate $a_n < (\dfrac{7}{4})^n$ defined over $\mathbb{Z}^+$.

We prove $p(n)$ is true for all positive integers n by strong induction on n.

Basis:

Since $a_1 = 1 < \frac{7}{4} = (\frac{7}{4})^1$, then $p(1)$ is true.

Since $a_2 = 3 < \frac{49}{16} = (\frac{7}{4})^2$, then $p(2)$ is true.

Induction:

For any integer $k \geq 3$, assume $p(n)$ is true for $n = 1, 2, ..., k-1$.

In particular, $p(k-2)$ and $p(k-1)$ are true, so $a_{k-2} < (\dfrac{7}{4})^{k-2}$ and $a_{k-1} < (\dfrac{7}{4})^{k-1}$.

Observe that

$$\begin{aligned}
a_k &= a_{k-1} + a_{k-2} \\
&< (\frac{7}{4})^{k-1} + (\frac{7}{4})^{k-2} \\
&= (\frac{7}{4})^{k-2}(\frac{7}{4} + 1) \\
&= (\frac{7}{4})^{k-2}(\frac{11}{4}) \\
&< (\frac{7}{4})^{k-2}(\frac{49}{16}) \\
&= (\frac{7}{4})^{k-2}(\frac{7}{4})^2 \\
&= (\frac{7}{4})^k.
\end{aligned}$$

Thus, $a_k < (\frac{7}{4})^k$, so $p(k)$ is true.

Hence, for any integer $k \geq 3$ such that $p(1), p(2), ..., p(k-1)$ is true, then $p(k)$ is true.

Since $p(1)$ is true and $p(2)$ is true, and for any integer $k \geq 3$ such that $p(1), p(2), ..., p(k-1)$ is true, then $p(k)$ is true, then by strong induction, $p(n)$ is true for all $n \in \mathbb{Z}^+$.

Therefore, $a_n < (\frac{7}{4})^n$ for all $n \in \mathbb{Z}^+$. ☐

Chapter 1.1 Problems

Exercise 4. sum of the first n products of pairs of consecutive integers

For all $n \in \mathbb{Z}^+$, $\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : \sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}\}$.

Basis:

Since $1 \in \mathbb{Z}^+$ and $1 \cdot 2 = 2 = \frac{1 \cdot 2 \cdot 3}{3}$, then $1 \in S$.

Induction:

Let $m \in \mathbb{Z}^+$ such that $m \in S$.

Then $\sum_{k=1}^{m} k(k+1) = \frac{m(m+1)(m+2)}{3}$.

Thus,

$$\begin{aligned}
\sum_{k=1}^{m+1} k(k+1) &= \sum_{k=1}^{m} k(k+1) + (m+1)(m+2) \\
&= \frac{m(m+1)(m+2)}{3} + (m+1)(m+2) \\
&= (m+1)(m+2)(\frac{m}{3}+1) \\
&= \frac{(m+1)(m+2)(m+3)}{3}.
\end{aligned}$$

Since $m+1 \in \mathbb{Z}^+$ and $\sum_{k=1}^{m+1} k(k+1) = \dfrac{(m+1)(m+2)(m+3)}{3}$, then $m+1 \in S$.

Therefore, $m \in S$ implies $m+1 \in S$ for all $m \in \mathbb{Z}^+$.

Since $1 \in S$ and $m \in S$ implies $m+1 \in S$ for all $m \in \mathbb{Z}^+$, then by induction, $S = \mathbb{Z}^+$, so $\sum_{k=1}^{n} k(k+1) = \dfrac{n(n+1)(n+2)}{3}$ for all $n \in \mathbb{Z}^+$, as desired. □

Exercise 5. The sum of the squares of the first n odd positive integers is $\dfrac{n(4n^2-1)}{3}$.

Proof. We must prove $\sum_{k=1}^{n}(2k-1)^2 = \dfrac{n(4n^2-1)}{3}$ for all $n \in \mathbb{Z}^+$.

Let $n \in \mathbb{Z}^+$.

Then

$$\begin{aligned}
\sum_{k=1}^{n}(2k-1)^2 &= \sum_{k=1}^{n}(4k^2-4k+1) \\
&= \sum_{k=1}^{n} 4k^2 - \sum_{k=1}^{n} 4k + \sum_{k=1}^{n} 1 \\
&= 4\sum_{k=1}^{n} k^2 - 4\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1 \\
&= 4 \cdot \frac{n(n+1)(2n+1)}{6} - 4 \cdot \frac{n(n+1)}{2} + n \\
&= \frac{2n(n+1)(2n+1)}{3} - 2n(n+1) + n \\
&= \frac{n}{3}[2(n+1)(2n+1) - 6(n+1) + 3] \\
&= \frac{n}{3}[2(2n^2+3n+1) - 6(n+1) + 3] \\
&= \frac{n}{3}(4n^2+6n+2-6n-6+3) \\
&= \frac{n}{3}(4n^2-1).
\end{aligned}$$

Therefore, $\sum_{k=1}^{n}(2k-1)^2 = \dfrac{n(4n^2-1)}{3}$. $\square$

Exercise 6. The cube of any positive integer can be written as the difference of two squares.

Proof. We prove for every $n \in \mathbb{Z}^+$, there exist integers k and m such that $n^3 = k^2 - m^2$.

Let $n \in \mathbb{Z}^+$.

Let $k = \dfrac{n(n+1)}{2}$.

Let $m = \dfrac{(n-1)n}{2}$.

Since n and $n+1$ are consecutive integers, then the product $n(n+1)$ is even, so k is an integer.

Since $n-1$ and n are consecutive integers, then the product $(n-1)n$ is even, so m is an integer.

Observe that

$$\begin{aligned}
n^3 &= n^3 + 0 \\
&= n^3 + [1^3 + 2^3 + ... + (n-1)^3] - [1^3 + 2^3 + ... + (n-1)^3] \\
&= [1^3 + 2^3 + ... + (n-1)^3 + n^3] - [1^3 + 2^3 + ... + (n-1)^3] \\
&= \sum_{k=1}^{n} k^3 - \sum_{k=1}^{n-1} k^3 \\
&= (\frac{n(n+1)}{2})^2 - (\frac{(n-1)n}{2})^2 \\
&= k^2 - m^2.
\end{aligned}$$

$\square$

Exercise 7. Let $m, n \in \mathbb{Z}^+$.

Is $(mn)! = m!n!$?

Is $(m+n)! = m! + n!$?

Proof. Let $m = 4$ and $n = 5$.

Then $(mn)! = (4 * 5)! = 20! = 2432902008176640000 \neq 22880 = 24 * 120 = (4!)(5!) = m!n!$, so $(mn)! \neq m!n!$.

Let $m = 3$ and $n = 7$.

Then $(m+n)! = (3+7)! = 10! = 3628800 \neq 5046 = 6 + 5040 = 3! + 7! = m! + n!$, so $(m+n)! \neq m! + n!$. $\square$

Exercise 8. For all integers $n \geq 4$, $n! > n^2$.

Proof. We prove $n! > n^2$ for all $n \in \mathbb{Z}^+$ with $n \geq 4$ by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : n! > n^2\}$.

Basis:

Since $4 \in \mathbb{Z}^+$ and $4! = 24 > 16 = 4^2$, then $4 \in S$.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 4$ such that $k \in S$.

Then $k! > k^2$.

Since $k \in \mathbb{Z}^+$, then $k + 1 \in \mathbb{Z}^+$.

Since $k + 1 > k$ and $k \geq 4$ and $4 > 0$, then $k + 1 > 4$ and $k + 1 > 0$.

Since $k \geq 4 > 1$, then $k > 1$.

Since $k \geq 4$, then $k - 1 \geq 3$.

Since $k - 1 \geq 3 > 1$, then $k - 1 > 1$.

Since $k > 1$ and $k - 1 > 1$, then $k(k - 1) > 1$, so $k^2 - k > 1$.

Hence, $k^2 > k + 1$.

Observe that

$$\begin{aligned}
(k+1)! &= (k+1)k! \\
&> (k+1)k^2 \\
&> (k+1)(k+1) \\
&= (k+1)^2.
\end{aligned}$$

Since $k + 1 \in \mathbb{Z}^+$ and $k + 1 > 4$ and $(k + 1)! > (k + 1)^2$, then $k + 1 \in S$.

Hence, $k \in S$ implies $k + 1 \in S$ for all integers $k \geq 4$.

Since $4 \in S$ and $k \in S$ implies $k + 1 \in S$ for all integers $k \geq 4$, then by induction $n! > n^2$ for all integers $n \geq 4$. $\square$

Exercise 9. For all integers $n \geq 6$, $n! > n^3$.

Proof. We prove $n! > n^3$ for all $n \in \mathbb{Z}^+$ with $n \geq 6$ by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : n! > n^3\}$.

Basis:

Since $6 \in \mathbb{Z}^+$ and $6! = 720 > 216 = 6^3$, then $6 \in S$.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 6$ such that $k \in S$.

Then $k! > k^3$.

Since $k \in \mathbb{Z}^+$, then $k > 0$ and $k + 1 \in \mathbb{Z}^+$, so $k + 1 > 0$.

Since $k + 1 > k \geq 6$, then $k + 1 > 6$.

Since $k \geq 6$, then $k^3 \geq 6^3 = 216 > 3$, so $k^3 > 3$.

Hence, $\frac{k^3}{3} > 1$.

Since $k \geq 6$, then $k^2 \geq 6^2 = 36 > 6$, so $k^2 > 6$.

Since $k > 0$, then $k^3 > 6k$, so $\frac{k^3}{3} > 2k$.

Since $k \geq 6 > 3$, then $k > 3$.

Since $k > 0$, then $k^2 > 0$, so $k^3 > 3k^2$.

Hence, $\frac{k^3}{3} > k^2$.

Since $\frac{k^3}{3} > k^2$ and $\frac{k^3}{3} > 2k$ and $\frac{k^3}{3} > 1$, then $k^3 = \frac{k^3}{3}+\frac{k^3}{3}+\frac{k^3}{3} > k^2+2k+1 = (k+1)^2$, so $k^3 > (k+1)^2$.

Observe that

$$\begin{aligned}(k+1)! &= (k+1)k! \\ &> (k+1)k^3 \\ &> (k+1)\cdot(k+1)^2 \\ &= (k+1)^3.\end{aligned}$$

Since $k+1 \in \mathbb{Z}^+$ and $(k+1)! > (k+1)^3$, then $k+1 \in S$.

Hence, $k \in S$ implies $k+1 \in S$ for all integers $k \geq 6$.

Since $6 \in S$ and $k \in S$ implies $k+1 \in S$ for all integers $k \geq 6$, then by induction, $n! > n^3$ for all integers $n \geq 6$. ☐

Exercise 10. Let (a_n) be the sequence defined by $a_1 = 1$ and $a_n = a_{n-1} + nn!$ for all positive integers $n > 1$.

Then $a_n = (n+1)! - 1$ for all $n \in \mathbb{Z}^+$.

Proof. We prove $(\forall n \in \mathbb{Z}^+)(a_n = (n+1)! - 1)$ by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : a_n = (n+1)! - 1\}$.

Basis:

Since $1 \in \mathbb{Z}^+$ and $a_1 = 1 = 2 - 1 = (1+1)! - 1$, then $1 \in S$.

Induction:

Let $k \in \mathbb{Z}^+$ such that $k \in S$.

Then $a_k = (k+1)! - 1$.

Since $k \in \mathbb{Z}^+$, then $k > 0$ and $k+1 \in \mathbb{Z}^+$.

Since $k > 0$, then $k+1 > 1$.

Observe that

$$\begin{aligned}a_{k+1} &= a_k + (k+1)(k+1)! \\ &= [(k+1)! - 1] + (k+1)(k+1)! \\ &= (k+1)! - 1 + (k+1)(k+1)! \\ &= (k+1)! + (k+1)(k+1)! - 1 \\ &= (k+2)(k+1)! - 1 \\ &= (k+2)! - 1 \\ &= [(k+1)+1]! - 1.\end{aligned}$$

Since $k+1 \in \mathbb{Z}^+$ and $a_{k+1} = [(k+1)+1]! - 1$, then $k+1 \in S$.

Hence, $k \in S$ implies $k+1 \in S$ for all $k \in \mathbb{Z}^+$.

Since $1 \in S$ and $k \in S$ implies $k+1 \in S$ for all $k \in \mathbb{Z}^+$, then by induction, $S = \mathbb{Z}^+$.

Therefore, $a_n = (n+1)! - 1$ for all $n \in \mathbb{Z}^+$. ☐

Chapter 1.2 Mathematical Induction

Chapter 1.2 Problems

Exercise 11. Let $k \in \mathbb{Z}$.

Then $\binom{n}{k} < \binom{n}{k+1}$ iff $0 \leq k < \frac{n-1}{2}$ for all $n \in \mathbb{Z}^+$.

Proof. Let $n \in \mathbb{Z}^+$.

We first prove if $\binom{n}{k} < \binom{n}{k+1}$, then $0 \leq k < \frac{n-1}{2}$.

Suppose $\binom{n}{k} < \binom{n}{k+1}$.

Then $\frac{n!}{k!(n-k)!} < \frac{n!}{(k+1)!(n-k-1)!}$.

Since $k!$ exists, then $k \geq 0$, by definition of factorial.

By definition of factorial function, the factorial of an integer is positive, so $n! > 0$ and $(k+1)! > 0$ and $(n-k)! > 0$.

Since $\frac{n!}{k!(n-k)!} < \frac{n!}{(k+1)!(n-k-1)!}$ and $n! > 0$, then $\frac{1}{k!(n-k)!} < \frac{1}{(k+1)!(n-k-1)!}$.

Since $k!$ and $(n-k-1)!$ are all in the denominator, then $k! \neq 0$ and $(n-k-1)! \neq 0$.

Since $\frac{1}{k!(n-k)!} < \frac{1}{(k+1)!(n-k-1)!}$ and $(k+1)! > 0$, then $\frac{(k+1)!}{k!(n-k)!} < \frac{1}{(n-k-1)!}$.

Thus, $\frac{(k+1)k!}{k!(n-k)!} < \frac{1}{(n-k-1)!}$, so $\frac{k+1}{(n-k)!} < \frac{1}{(n-k-1)!}$.

Since $\frac{k+1}{(n-k)!} < \frac{1}{(n-k-1)!}$ and $(n-k)! > 0$, then $k+1 < \frac{(n-k)!}{(n-k-1)!}$.

Hence, $k+1 < \frac{(n-k)(n-k-1)!}{(n-k-1)!}$, so $k+1 < n-k$.

Thus, $2k < n-1$, so $k < \frac{n-1}{2}$.

Since $0 \leq k$ and $k < \frac{n-1}{2}$, then $0 \leq k < \frac{n-1}{2}$. $\square$

Proof. Conversely, we prove if $0 \leq k < \frac{n-1}{2}$, then $\binom{n}{k} < \binom{n}{k+1}$.

Suppose $0 \leq k < \frac{n-1}{2}$.

Then $0 \leq k$ and $k < \frac{n-1}{2}$.

Since $k < \frac{n-1}{2}$, then $2k < n-1$, so $k+k < n-1$.

Thus, $k+1 < n-k$.

By definition of factorial function, the factorial of an integer is positive.

Thus, $(n-k-1)! > 0$ and $k! > 0$ and $(n-k)! > 0$ and $(k+1)! > 0$ and $n! > 0$.

Since $k+1 < n-k$ and $(n-k-1)! > 0$, then $k+1 < \frac{(n-k)(n-k-1)!}{(n-k-1)!}$, so $k+1 < \frac{(n-k)!}{(n-k-1)!}$.

Since $k! > 0$, then $\frac{(k+1)k!}{k!} < \frac{(n-k)!}{(n-k-1)!}$, so $\frac{(k+1)!}{k!} < \frac{(n-k)!}{(n-k-1)!}$.

Since $(n-k)! > 0$, then $\frac{(k+1)!}{k!(n-k)!} < \frac{1}{(n-k-1)!}$.

Since $(k+1)! > 0$, then $\frac{1}{k!(n-k)!} < \frac{1}{(k+1)!(n-k-1)!}$.

Since $n! > 0$, then $\frac{n!}{k!(n-k)!} < \frac{n!}{(k+1)!(n-k-1)!}$, so $\binom{n}{k} < \binom{n}{k+1}$. $\square$

Exercise 12. Let $n, k \in \mathbb{Z}$ and $0 \leq k \leq n$.

Then $\binom{n}{k} = \binom{n}{k+1}$ iff $k = \frac{n-1}{2}$.

Proof. We prove if $\binom{n}{k} = \binom{n}{k+1}$, then $k = \frac{n-1}{2}$.

Suppose $\binom{n}{k} = \binom{n}{k+1}$.

Observe that

$$\begin{aligned}
k+1 &= 1\cdot(k+1)\\
&= 1\cdot 1\cdot 1\cdot(k+1)\\
&= \frac{n!}{n!}\cdot\frac{(n-k)!}{(n-k)!}\cdot\frac{k!}{k!}\cdot(k+1)\\
&= \frac{n!}{n!}\cdot\frac{(n-k)!}{(n-k)!}\cdot\frac{(k+1)!}{k!}\\
&= \frac{n!}{k!}\cdot\frac{(n-k)!}{(n-k)!}\cdot\frac{(k+1)!}{n!}\\
&= \frac{n!}{k!(n-k)!}\cdot\frac{(n-k)!(k+1)!}{n!}\\
&= \binom{n}{k}\cdot\frac{(n-k)!(k+1)!}{n!}\\
&= \binom{n}{k+1}\cdot\frac{(n-k)!(k+1)!}{n!}\\
&= \frac{n!}{(k+1)!(n-k-1)!}\cdot\frac{(n-k)!(k+1)!}{n!}\\
&= \frac{(n-k)!}{(n-k-1)!}\cdot\frac{n!}{n!}\cdot\frac{(k+1)!}{(k+1)!}\\
&= \frac{(n-k)!}{(n-k-1)!}\\
&= \frac{(n-k)(n-k-1)!}{(n-k-1)!}\\
&= n-k.
\end{aligned}$$

Hence, $k+1=n-k$, so $2k+1=n$.
Therefore, $2k=n-1$, so $k=\frac{n-1}{2}$. ☐

Proof. Conversely, we prove if $k=\frac{n-1}{2}$, then $\binom{n}{k}=\binom{n}{k+1}$.

Suppose $k=\frac{n-1}{2}$.
Then $n-1=2k=k+k$, so $n-1=k+k$.
Hence, $n-k=k+1$, so $k=n-k-1$.

Observe that

$$\begin{aligned}
\binom{n}{k} &= \frac{n!}{k!(n-k)!} \\
&= \frac{n!}{(n-k)!k!} \\
&= \frac{n!}{(k+1)!k!} \\
&= \frac{n!}{(k+1)!(n-k-1)!} \\
&= \frac{n!}{(k+1)!(n-k-1)!} \\
&= \binom{n}{k+1}.
\end{aligned}$$

Therefore, $\binom{n}{k} = \binom{n}{k+1}$. ∎

Exercise 13. If $k \in \mathbb{Z}$ and $2 \leq k \leq n-2$, then $\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$ for all $n \in \mathbb{Z}^+$ and $n \geq 4$.

Proof. We define the predicate $p(n)$ over $\mathbb{Z}^+$ by 'if $k \in \mathbb{Z}$ and $2 \leq k \leq n-2$, then $\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$'.

We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ with $n \geq 4$ by induction on n.

Basis:

Let $n = 4$.

Suppose $k \in \mathbb{Z}$ and $2 \leq k \leq n-2$.

Then $k \in \mathbb{Z}$ and $2 \leq k \leq 4-2 = 2$, so $2 \leq k \leq 2$.

Since $k \in \mathbb{Z}$ and $2 \leq k \leq 2$, then $k = 2$.

Observe that

$$\begin{aligned}
\binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k} &= \binom{4-2}{2-2} + 2\binom{4-2}{2-1} + \binom{4-2}{2} \\
&= \binom{2}{0} + 2\binom{2}{1} + \binom{2}{2} \\
&= 1 + 2 \cdot 2 + 1 \\
&= 6 \\
&= \binom{4}{2} \\
&= \binom{n}{k}.
\end{aligned}$$

Therefore, $p(4)$ is true.

Induction:

Let $n \in \mathbb{Z}^+$ with $n \geq 4$ such that $p(n)$ is true.

Then $k \in \mathbb{Z}$ and $2 \leq k \leq n-2$ implies $\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$.

Suppose $k \in \mathbb{Z}$ and $2 \leq k \leq n-1$.

Then $2 \leq k$ and $k \leq n-1$.

Since $k \leq n-1$, then either $k < n-1$ or $k = n-1$, so either $k \leq n-2$ or $k = n-1$.

We consider each case separately.

Case 1: Suppose $k = n-1$.

Then $k+2 = (n-1)+2 = n+1$, so $k+2 = n+1$.

Observe that

$$\begin{aligned}
\binom{n-1}{k-2} + 2\binom{n-1}{k-1} + \binom{n-1}{k} &= \binom{k}{k-2} + 2\binom{k}{k-1} + \binom{k}{k} \\
&= \binom{k}{k-2} + [\binom{k}{k-1} + \binom{k}{k-1}] + \binom{k}{k} \\
&= [\binom{k}{k-2} + \binom{k}{k-1}] + [\binom{k}{k-1} + \binom{k}{k}] \\
&= \binom{k+1}{k-1} + \binom{k+1}{k} \\
&= \binom{k+2}{k} \\
&= \binom{n+1}{k}.
\end{aligned}$$

Case 2: Suppose $k \leq n-2$.

Since $2 \leq k$ and $k \leq n-2$, then $2 \leq k \leq n-2$.

Since $k \in \mathbb{Z}$ and $2 \leq k \leq n-2$, then $\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$, by the induction hypothesis.

Observe that

$$\begin{aligned}
\binom{n+1}{k} &= \binom{n}{k-1} + \binom{n}{k} \\
&= \binom{n}{k-1} + [\binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}] \\
&= \binom{n}{k-1} + \binom{n-2}{k-2} + \binom{n-2}{k-1} + \binom{n-2}{k-1} + \binom{n-2}{k} \\
&= \binom{n}{k-1} + [\binom{n-2}{k-2} + \binom{n-2}{k-1}] + [\binom{n-2}{k-1} + \binom{n-2}{k}] \\
&= \binom{n}{k-1} + \binom{n-1}{k-1} + \binom{n-1}{k} \\
&= [\binom{n-1}{k-2} + \binom{n-1}{k-1}] + \binom{n-1}{k-1} + \binom{n-1}{k} \\
&= \binom{n-1}{k-2} + 2\binom{n-1}{k-1} + \binom{n-1}{k}.
\end{aligned}$$

Therefore, $p(n+1)$ is true.

Hence, $p(n)$ implies $p(n+1)$ for all integers $n \geq 4$.

Since $p(4)$ is true and $p(n)$ implies $p(n+1)$ for all integers $n \geq 4$, then by induction, $p(n)$ is true for all integers $n \geq 4$.

Therefore, if $k \in \mathbb{Z}$ and $2 \leq k \leq n-2$, then $\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$ for all integers $n \geq 4$. $\square$

Lemma 14. *For every* $n \in \mathbb{Z}^+$, $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$.

Proof. Let $n \in \mathbb{Z}^+$.

Then

$$\begin{aligned}
\sum_{k=0}^{n}(-1)^k\binom{n}{k} &= \sum_{k=0}^{n}\binom{n}{k}\cdot(-1)^k \\
&= \sum_{k=0}^{n}\binom{n}{k}\cdot 1\cdot(-1)^k \\
&= \sum_{k=0}^{n}\binom{n}{k}\cdot 1^{n-k}\cdot(-1)^k \\
&= [1+(-1)]^n \\
&= 0^n \\
&= 0.
\end{aligned}$$

$\square$

Exercise 15. For every $n \in \mathbb{Z}^+$, $\sum_{k=0}^{\infty} \binom{n}{2k} = \sum_{k=0}^{\infty} \binom{n}{2k+1} = 2^{n-1}$.

Proof. Let $n \in \mathbb{Z}^+$.

Let $S = \sum_{k=0}^{\infty} \binom{n}{2k}$.

Let $T = \sum_{k=0}^{\infty} \binom{n}{2k+1}$.

Since $n \in \mathbb{Z}^+$, then $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Observe that

$$\begin{aligned}
S + T &= \sum_{k=0}^{\infty} \binom{n}{2k} + \sum_{k=0}^{\infty} \binom{n}{2k+1} \\
&= [\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + ...] + [\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + ...] \\
&= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5} + ... \\
&= \sum_{k=0}^{\infty} \binom{n}{k} \\
&= \sum_{k=0}^{n} \binom{n}{k} + \sum_{k=n+1}^{\infty} \binom{n}{k} \\
&= 2^n + [\binom{n}{n+1} + \binom{n}{n+2} + \binom{n}{n+3} + ...] \\
&= 2^n + 0 \\
&= 2^n.
\end{aligned}$$

Therefore, $S + T = 2^n$.

Since $n \in \mathbb{Z}^+$, then $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$, by lemma 14.

Observe that

$$
\begin{aligned}
S - T &= \sum_{k=0}^{\infty} \binom{n}{2k} - \sum_{k=0}^{\infty} \binom{n}{2k+1} \\
&= [\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + ...] - [\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + ...] \\
&= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \binom{n}{4} - \binom{n}{5} + ... \\
&= \sum_{k=0}^{\infty} \binom{n}{k} (-1)^k \\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k + \sum_{k=n+1}^{\infty} \binom{n}{k} (-1)^k \\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k + [\binom{n}{n+1} (-1)^{n+1} + \binom{n}{n+2} (-1)^{n+2} + \binom{n}{n+3} (-1)^{n+3} + ...] \\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k + 0 \\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k \\
&= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \\
&= 0.
\end{aligned}
$$

Therefore, $S - T = 0$, so $S = T$.
Hence, $2^n = S + T = S + S = 2S$, so $2^n = 2S$.
Thus, $2^{n-1} = S = T$, so $\sum_{k=0}^{\infty} \binom{n}{2k} = \sum_{k=0}^{\infty} \binom{n}{2k+1} = 2^{n-1}$. $\square$

Exercise 16. Show that $\sum_{k=1}^{n} k \binom{n}{k} = n \cdot 2^{n-1}$ for all $n \in \mathbb{Z}^+$.

Proof. We prove the statement $\sum_{k=1}^{n} k \binom{n}{k} = n2^{n-1}$ for all $n \in \mathbb{Z}^+$ by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : \sum_{k=1}^{n} k \binom{n}{k} = n2^{n-1}\}$.

Basis:
Since $1 \in \mathbb{Z}^+$ and $\sum_{k=1}^{1} k \binom{1}{k} = 1\binom{1}{1} = 1 = (1)2^{1-1}$, then $1 \in S$.

Induction:
Suppose $m \in S$.
Then $m \in \mathbb{Z}^+$ and $\sum_{k=1}^{m} k \binom{m}{k} = m2^{m-1}$.

We must prove $\sum_{k=1}^{m+1} k\binom{m+1}{k} = (m+1)2^m$.

TODO

We may need to abandon using proof by induction and use binomial theorem instead. Try to get it into a form so that we can use the binomial theorem.

Hence, $m \in S$ implies $m+1 \in S$.

Therefore, by PMI, $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$ for all $n \in \mathbb{Z}^+$. $\square$

Exercise 17. Show that $\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$ for all $n \in \mathbb{Z}^+$.

Proof. Let $n \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned}
\sum_{k=0}^{n} 2^k \binom{n}{k} &= 2^0\binom{n}{0} + 2^1\binom{n}{1} + ... + 2^{n-2}\binom{n}{n-2} + 2^{n-1}\binom{n}{n-1} + 2^n\binom{n}{n} \\
&= \binom{n}{0}2^0 + \binom{n}{1}2^1 + ... + \binom{n}{n-2}2^{n-2} + \binom{n}{n-1}2^{n-1} + \binom{n}{n}2^n \\
&= \binom{n}{n}2^0 + \binom{n}{n-1}2^1 + ... + \binom{n}{2}2^{n-2} + \binom{n}{1}2^{n-1} + \binom{n}{0}2^n \\
&= \binom{n}{0}2^n + \binom{n}{1}2^{n-1} + \binom{n}{2}2^{n-2} + ... + \binom{n}{n-1}2^1 + \binom{n}{n}2^0 \\
&= \binom{n}{0}2^{n-0} + \binom{n}{1}2^{n-1} + \binom{n}{2}2^{n-2} + ... + \binom{n}{n-1}2^{n-(n-1)} + \binom{n}{n}2^{n-n} \\
&= \sum_{k=0}^{n}\binom{n}{k}2^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}2^{n-k} \cdot 1 \\
&= \sum_{k=0}^{n}\binom{n}{k}2^{n-k} \cdot 1^k \\
&= (2+1)^n \\
&= 3^n.
\end{aligned}$$

$\square$

Lemma 18. *Let $n \in \mathbb{Z}$ and $n \geq 2$.*

Then $\sum_{k=2}^{n} \binom{k}{2} = \binom{n+1}{3}$.

Proof. Define predicate $p(n)$ over $\mathbb{Z}^+$ by '$\sum_{k=2}^{n} \binom{k}{2} = \binom{n+1}{3}$'.

We prove $p(n)$ is true for all integers $n \geq 2$ by induction on n.

Basis:

Let $n = 2$.

Then $\sum_{k=2}^{2}\binom{k}{2} = \binom{2}{2} = 1 = \binom{3}{3} = \binom{2+1}{3}$.
Therefore, $p(2)$ is true.
Induction:
Let $m \in \mathbb{Z}^+$ with $m \geq 2$ such that $p(m)$ is true.
Then $\sum_{k=2}^{m}\binom{k}{2} = \binom{m+1}{3}$.

Observe that

$$\begin{aligned}
\sum_{k=2}^{m+1}\binom{k}{2} &= \sum_{k=2}^{m}\binom{k}{2} + \binom{m+1}{2} \\
&= \binom{m+1}{3} + \binom{m+1}{2} \\
&= \binom{m+2}{3} \\
&= \binom{(m+1)+1}{3}.
\end{aligned}$$

Thus, $p(m+1)$ is true, so $p(m)$ implies $p(m+1)$ for all integers $m \geq 2$.

Since $p(2)$ is true and $p(m)$ implies $p(m+1)$ for all integers $m \geq 2$, then by induction, $p(n)$ is true for all integers $n \geq 2$.
Therefore, $\sum_{k=2}^{n}\binom{k}{2} = \binom{n+1}{3}$ for all integers $n \geq 2$. $\square$

Exercise 19. If $n \in \mathbb{Z}^+$, then $n^2 = 2\binom{n}{2} + \binom{n}{1}$.

Proof. Let $n \in \mathbb{Z}^+$.
Since $n \in \mathbb{Z}^+$, then $n \geq 1$, so either $n > 1$ or $n = 1$.
We consider each case separately.
Case 1: Suppose $n = 1$.
Then $2\binom{1}{2} + \binom{1}{1} = 2 \cdot 0 + 1 = 1 = 1^2$.
Case 2: Suppose $n > 1$.
Then $2\binom{n}{2} + \binom{n}{1} = 2 \cdot \frac{n(n-1)}{2} + n = n(n-1) + n = n^2 - n + n = n^2$.
Both cases show $n^2 = 2\binom{n}{2} + \binom{n}{1}$. $\square$

Lemma 20. *Let $n \in \mathbb{Z}$ and $n \geq 2$.*
Then $2\binom{n}{2} + n = n^2$.

Proof. Define predicate $p(n)$ over $\mathbb{Z}^+$ by '$2\binom{n}{2} + n = n^2$'.

We prove $p(n)$ is true for all integers $n \geq 2$ by induction on n.

Basis:

Let $n = 2$.

Then $2\binom{2}{2} + 2 = 2 \cdot 1 + 2 = 4 = 2^2$, so $p(2)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 2$ such that $p(k)$ is true.

Then $2\binom{k}{2} + k = k^2$, so $2\binom{k}{2} = k^2 - k = k(k-1)$.

Observe that

$$\begin{aligned}
2 \cdot \binom{k+1}{2} + (k+1) &= 2 \cdot \frac{(k+1)!}{2!(k-1)!} + (k+1) \\
&= 2 \cdot \frac{(k+1)k!}{2!(k-1)!} + (k+1) \\
&= 2 \cdot \frac{(k+1)k!}{2!(k-1)(k-2)!} + (k+1) \\
&= 2 \cdot \frac{k!}{2!(k-2)!} \cdot \frac{k+1}{k-1} + (k+1) \\
&= 2 \cdot \binom{k}{2} \cdot \frac{k+1}{k-1} + (k+1) \\
&= k(k-1) \cdot \frac{k+1}{k-1} + (k+1) \\
&= k(k+1) + (k+1) \\
&= (k+1)(k+1) \\
&= (k+1)^2.
\end{aligned}$$

Thus, $p(k+1)$ is true, so $p(k)$ implies $p(k+1)$ for all integers $k \geq 2$.

Since $p(2)$ is true and $p(k)$ implies $p(k+1)$ for all integers $k \geq 2$, then by induction, $p(n)$ is true for all integers $n \geq 2$.

Therefore, $2\binom{n}{2} + n = n^2$ for all integers $n \geq 2$. □

Exercise 21. Let $n \in \mathbb{Z}^+$.

Prove $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ using lemmas 18 and 20.

Proof. Since $n \in \mathbb{Z}^+$, then $n \geq 1$, so either $n > 1$ or $n = 1$.

We consider these cases separately.

Case 1: Suppose $n = 1$.

Since $\sum_{k=1}^{1} k^2 = 1^2 = 1 = \frac{6}{6} = \frac{1 \cdot 2 \cdot 3}{6} = \frac{1(1+1)(2 \cdot 1 + 1)}{6}$, then the formula holds for $n = 1$.

Case 2: Suppose $n > 1$.

Since $n \in \mathbb{Z}$ and $n > 1$, then $n \geq 2$.

Since $n \in \mathbb{Z}$ and $n \geq 2$, then $\sum_{k=2}^{n} \binom{k}{2} = \binom{n+1}{3}$, by lemma 18.

Since $n \in \mathbb{Z}$ and $n \geq 2$, then $2\binom{n}{2} + n = n^2$, by lemma 20.

Observe that

$$\begin{aligned}
\sum_{k=1}^{n} k^2 &= \sum_{k=1}^{1} k^2 + \sum_{k=2}^{n} k^2 \\
&= 1^2 + \sum_{k=2}^{n} k^2 \\
&= 1 + \sum_{k=2}^{n} k^2 \\
&= 1 + \sum_{k=2}^{n} [2\binom{k}{2} + k] \\
&= 1 + \sum_{k=2}^{n} 2\binom{k}{2} + \sum_{k=2}^{n} k \\
&= 1 + 2 \cdot \sum_{k=2}^{n} \binom{k}{2} + [\sum_{k=1}^{n} k - \sum_{k=1}^{1} k] \\
&= 1 + 2 \cdot \binom{n+1}{3} + \frac{n(n+1)}{2} - 1 \\
&= 2 \cdot \binom{n+1}{3} + \frac{n(n+1)}{2} \\
&= \frac{2(n+1)n(n-1)(n-2)!}{(n-2)!3!} + \frac{n(n+1)}{2} \\
&= \frac{2n(n+1)(n-1)}{3!} + \frac{n(n+1)}{2} \\
&= \frac{2n(n+1)(n-1)}{6} + \frac{3n(n+1)}{6} \\
&= \frac{2n(n+1)(n-1) + 3n(n+1)}{6} \\
&= \frac{n(n+1)[2(n-1)+3]}{6} \\
&= \frac{n(n+1)(2n+1)}{6}.
\end{aligned}$$

Therefore, $\sum_{k=1}^{n} k^2 = \dfrac{n(n+1)(2n+1)}{6}$ for all $n \in \mathbb{Z}^+$. $\square$

Chapter 1.3 Early Number Theory

Chapter 1.3 Problems

Exercise 22. The positive integer n is triangular iff $8n+1$ is a perfect square.

Proof. We prove 'if the positive integer n is triangular, then $8n+1$ is a perfect square'.

Suppose the positive integer n is triangular.

Then $n \in \mathbb{Z}^+$ and n is triangular, so n is of the form $\dfrac{a(a+1)}{2}$ for some $a \in \mathbb{Z}^+$.

Hence, $n = \dfrac{a(a+1)}{2}$, so $8n = 4a(a+1)$.

Let $b = 2a+1$.

Since $a \in \mathbb{Z}$, then $2a+1 \in \mathbb{Z}$, so $b \in \mathbb{Z}$.

Observe that

$$\begin{aligned} b^2 &= (2a+1)^2 \\ &= 4a^2+4a+1 \\ &= 4a(a+1)+1 \\ &= 8n+1. \end{aligned}$$

Since $b \in \mathbb{Z}$ and $b^2 = 8n+1$, then $8n+1$ is a perfect square. $\square$

Proof. Conversely, we prove 'if n is a positive integer and $8n+1$ is a perfect square, then n is triangular'.

Suppose n is a positive integer and $8n+1$ is a perfect square.

Then $n \in \mathbb{Z}^+$ and $8n+1 = b^2$ for some integer b.

Let $a = \dfrac{b-1}{2}$.

Then $2a = b-1$, so $b = 2a+1$.

Observe that

$$\begin{aligned} 8n &= b^2-1 \\ &= (2a+1)^2-1 \\ &= 4a^2+4a+1-1 \\ &= 4a^2+4a \\ &= 4a(a+1). \end{aligned}$$

Thus, $8n = 4a(a+1)$, so $2n = a(a+1)$.
Hence, $n = \frac{a(a+1)}{2}$.

Suppose for the sake of contradiction b is even.
Then $b-1$ is odd and $b+1$ is odd, so the product $(b-1)(b+1) = b^2 - 1$ is odd.
Hence, $8n = b^2 - 1$ is odd, so $8n$ is odd.
But, $8n = 2(4n)$, so $8n$ is even.
Since a number cannot be both even and odd, then we must conclude b is not even.

Therefore, b is odd.
Since b is odd, then $b-1$ is even, so $\frac{b-1}{2}$ is even.
Thus, $\frac{b-1}{2} = 2c$ for some integer c, so $b-1 = 4c$.
Hence, $a = \frac{b-1}{2} = \frac{4c}{2} = 2c$.
Since $2 \in \mathbb{Z}$ and $c \in \mathbb{Z}$, then $2c \in \mathbb{Z}$, so $a \in \mathbb{Z}$.
Since $a \in \mathbb{Z}$ and $n = \frac{a(a+1)}{2}$, then n is triangular. $\square$

Exercise 23. The sum of any two consecutive triangular numbers is a perfect square.

Proof. Let a and b be any two consecutive triangular numbers.
Then $a = \frac{n(n+1)}{2}$ and $b = \frac{(n+1)(n+2)}{2}$ for some positive integer n.

Observe that

$$\begin{aligned} a+b &= \frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2} \\ &= \frac{n(n+1)+(n+1)(n+2)}{2} \\ &= \frac{(n+1)[n+(n+2)]}{2} \\ &= \frac{(n+1)(2n+2)}{2} \\ &= \frac{2(n+1)(n+1)}{2} \\ &= (n+1)(n+1) \\ &= (n+1)^2. \end{aligned}$$

Thus, $a+b = (n+1)^2$.
Let $t = n+1$.
Then $a+b = t^2$.

Since $n \in \mathbb{Z}$, then $n+1 \in \mathbb{Z}$, so $t \in \mathbb{Z}$.
Therefore, $a+b=t^2$ for some integer t, as desired. $\square$

Exercise 24. If n is a triangular number, then so are $9n+1$, $25n+3$, and $49n+6$.

Proof. Let n be a triangular number.
Then $n \in \mathbb{Z}^+$ and $n = \frac{a(a+1)}{2}$ for some $a \in \mathbb{Z}^+$.

We prove $9n+1$ is triangular.
Since $n \in \mathbb{Z}^+$, then $9n+1 \in \mathbb{Z}^+$.
Let $b = 3a+1$.
Since $a \in \mathbb{Z}^+$, then $3a+1 \in \mathbb{Z}^+$, so $b \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned} 9n+1 &= \frac{9a(a+1)}{2} + 1 \\ &= \frac{9a(a+1)+2}{2} \\ &= \frac{9a^2+9a+2}{2} \\ &= \frac{(3a+1)(3a+2)}{2} \\ &= \frac{b(b+1)}{2}. \end{aligned}$$

Thus, $9n+1 = \frac{b(b+1)}{2}$.
Since $9n+1 \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $9n+1 = \frac{b(b+1)}{2}$, then $9n+1$ is triangular. $\square$

Proof. Let n be a triangular number.
Then $n \in \mathbb{Z}^+$ and $n = \frac{a(a+1)}{2}$ for some $a \in \mathbb{Z}^+$.

We prove $25n+3$ is triangular.
Since $n \in \mathbb{Z}^+$, then $25n+3 \in \mathbb{Z}^+$.
Let $b = 5a+2$.
Since $a \in \mathbb{Z}^+$, then $5a+2 \in \mathbb{Z}^+$, so $b \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned} 25n+3 &= \frac{25a(a+1)}{2}+3 \\ &= \frac{25a(a+1)+6}{2} \\ &= \frac{25a^2+25a+6}{2} \\ &= \frac{(5a+2)(5a+3)}{2} \\ &= \frac{b(b+1)}{2}. \end{aligned}$$

Thus, $25n+3 = \frac{b(b+1)}{2}$.

Since $25n+3 \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $25n+3 = \frac{b(b+1)}{2}$, then $25n+3$ is triangular. $\square$

Proof. Let n be a triangular number.

Then $n \in \mathbb{Z}^+$ and $n = \frac{a(a+1)}{2}$ for some $a \in \mathbb{Z}^+$.

We prove $49n+6$ is triangular.

Since $n \in \mathbb{Z}^+$, then $49n+6 \in \mathbb{Z}^+$.

Let $b = 7a+3$.

Since $a \in \mathbb{Z}^+$, then $7a+3 \in \mathbb{Z}^+$, so $b \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned} 49n+6 &= \frac{49a(a+1)}{2}+6 \\ &= \frac{49a(a+1)+12}{2} \\ &= \frac{49a^2+49a+12}{2} \\ &= \frac{(7a+3)(7a+4)}{2} \\ &= \frac{b(b+1)}{2}. \end{aligned}$$

Thus, $49n+6 = \frac{b(b+1)}{2}$.

Since $49n+6 \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $49n+6 = \frac{b(b+1)}{2}$, then $49n+6$ is triangular. $\square$

Exercise 25. The sum of the first n triangular numbers is $t_1+t_2+t_3+...+t_n = \frac{n(n+1)(n+2)}{6}$ for all $n \in \mathbb{Z}^+$.

Proof. Let $n \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned}
t_1 + t_2 + t_3 + ... + t_n &= \sum_{k=1}^{n} \frac{k(k+1)}{2} \\
&= \frac{1}{2}\sum_{k=1}^{n} k(k+1) \\
&= \frac{1}{2}\sum_{k=1}^{n} (k^2+k) \\
&= \frac{1}{2}[\sum_{k=1}^{n} k^2 + \sum_{k=1}^{n} k] \\
&= \frac{1}{2}[\frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2}] \\
&= \frac{1}{2}[\frac{n(n+1)(2n+1)}{6} + \frac{3n(n+1)}{6}] \\
&= \frac{1}{2}[\frac{n(n+1)(2n+1)+3n(n+1)}{6}] \\
&= \frac{1}{2}[\frac{n(n+1)[(2n+1)+3)]}{6}] \\
&= \frac{1}{2}[\frac{n(n+1)(2n+4)}{6}] \\
&= \frac{2}{2}[\frac{n(n+1)(n+2)}{6}] \\
&= \frac{n(n+1)(n+2)}{6}.
\end{aligned}$$

□

Exercise 26. The square of any odd multiple of 3 is the difference of two triangular numbers.

Specifically, $9(2n+1)^2 = t_{9n+4} - t_{3n+1}$ for any integer $n \geq 0$.

Proof. Let n be any integer with $n \geq 0$.

Let a be any odd multiple of 3.

Then a is odd and a is a multiple of 3, so $a = 3(2n+1)$.

Observe that

$$\begin{aligned}
t_{9n+4} - t_{3n+1} &= \frac{(9n+4)(9n+5)}{2} - \frac{(3n+1)(3n+2)}{2} \\
&= \frac{81n^2+81n+20}{2} - \frac{9n^2+9n+2}{2} \\
&= \frac{81n^2+81n+20-(9n^2+9n+2)}{2} \\
&= \frac{81n^2+81n+20-9n^2-9n-2}{2} \\
&= \frac{72n^2+72n+18}{2} \\
&= \frac{18(4n^2+4n+1)}{2} \\
&= 9(4n^2+4n+1) \\
&= 3^2(2n+1)^2 \\
&= [3(2n+1)]^2 \\
&= a^2.
\end{aligned}$$

□

Exercise 27. Find two triangular numbers whose sum and difference are also triangular numbers.

Solution. Let $a = 21$ and $b = 15$.

Observe that a and b are triangular and $a + b = 21 + 15 = 36$ is triangular and $a - b = 21 - 15 = 6$ is triangular. □

Exercise 28. Find three successive triangular numbers whose product is a perfect square.

Solution. Let $a = 6$ and $b = 10$ and $c = 15$.

Then a, b, and c are successive triangular numbers and the product $abc = 6 \cdot 10 \cdot 15 = 900 = 30^2$ is a perfect square. □

Exercise 29. Find three successive triangular numbers whose sum is a perfect square.

Solution. Let $a = 15$ and $b = 21$ and $c = 28$.

Then a, b, and c are successive triangular numbers and the sum $a + b + c = 15 + 21 + 28 = 64 = 8^2$ is a perfect square. □

Exercise 30. Let $n \in \mathbb{Z}^+$.

If $2n^2 + 1$ is a perfect square, say $2n^2 + 1 = m^2$, then $(nm)^2$ is a triangular number.

Proof. Suppose $2n^2 + 1$ is a perfect square.

Then $2n^2 + 1 = m^2$ for some $m \in \mathbb{Z}^+$.

Hence, $2n^2 = m^2 - 1$.

Let $k = m^2 - 1$.
Then $k + 1 = m^2$.
Observe that

$$\begin{aligned}\frac{k(k+1)}{2} &= \frac{(m^2-1)m^2}{2} \\ &= \frac{(2n^2)m^2}{2} \\ &= n^2m^2 \\ &= (nm)^2.\end{aligned}$$

Since $m \in \mathbb{Z}$, then $m^2 - 1 \in \mathbb{Z}$, so $k \in \mathbb{Z}$.
Since $n \in \mathbb{Z}^+$, then $n \in \mathbb{Z}$ and $n > 0$.
Since $m \in \mathbb{Z}^+$, then $m \geq 1$, so either $m > 1$ or $m = 1$.

Suppose $m = 1$.
Then $1 = 1^2 = m^2 = 2n^2 + 1$, so $1 = 2n^2 + 1$.
Hence, $2n^2 = 0$, so $n^2 = 0$.
Thus, $n = 0$.
But, this contradicts $n > 0$.
Therefore, $m \neq 1$.

Since $m \geq 1$ and $m \neq 1$, then $m > 1$.
Since $m > 1$, then $m^2 > 1$, so $m^2 - 1 > 0$.
Since $k = m^2 - 1$ and $m^2 - 1 > 0$, then $k > 0$.
Since $k \in \mathbb{Z}$ and $k > 0$, then $k \in \mathbb{Z}^+$.

Therefore, there exists $k \in \mathbb{Z}^+$ such that $\frac{k(k+1)}{2} = (nm)^2$, so $(nm)^2$ is triangular. $\square$

Exercise 31. Let $n \in \mathbb{Z}^+$.
If $2n^2 - 1$ is a perfect square, say $2n^2 - 1 = m^2$, then $(nm)^2$ is a triangular number.

Proof. Suppose $2n^2 - 1$ is a perfect square.
Then $2n^2 - 1 = m^2$ for some $m \in \mathbb{Z}^+$.
Hence, $2n^2 = m^2 + 1$.

Let $k = m^2 + 1$.
Then $k - 1 = m^2$.

Observe that

$$\begin{aligned}
\frac{(k-1)k}{2} &= \frac{m^2(m^2+1)}{2} \\
&= \frac{m^2(2n^2)}{2} \\
&= m^2n^2 \\
&= (mn)^2 \\
&= (nm)^2.
\end{aligned}$$

Since $m \in \mathbb{Z}$, then $m^2+1 \in \mathbb{Z}$, so $k \in \mathbb{Z}$.
Hence, $k-1 \in \mathbb{Z}$.
Since $m \in \mathbb{Z}^+$, then $m \geq 1$, so $m^2 \geq 1$.
Hence, $k = m^2+1 \geq 1+1 = 2 > 1$, so $k > 1$.
Thus, $k-1 > 0$.
Since $k-1 \in \mathbb{Z}$ and $k-1 > 0$, then $k-1 \in \mathbb{Z}^+$.

Therefore, there exists $k-1 \in \mathbb{Z}^+$ such that $\frac{(k-1)k}{2} = (nm)^2$, so $(nm)^2$ is triangular. $\square$

Exercise 32. Find five examples of squares which are also triangular numbers.

Solution. Observe that $1 = 1^2 = \frac{1 \cdot 2}{2}$ is a square and is triangular.
Observe that $36 = 6^2 = \frac{8 \cdot 9}{2}$ is a square and is triangular.
Observe that $1225 = 35^2 = \frac{49 \cdot 50}{2}$ is a square and is triangular.
Observe that $41616 = 204^2 = \frac{288 \cdot 289}{2}$ is a square and is triangular.
Observe that $1413721 = 1189^2 = \frac{1681 \cdot 1682}{2}$ is a square and is triangular.
$\square$

Chapter 2 Divisibility

Chapter 2.1 The Division Algorithm

Example 33. Use the division algorithm to compute 1 divided by -7.

Solution. Since $1 = 7 \cdot 0 + 1$, then $1 = (-7) \cdot 0 + 1$. $\square$

Example 34. Use the division algorithm to compute -2 divided by -7.

Solution. Since $2 = 7 \cdot 0 + 2$, then $-2 = -(7 \cdot 0 + 2) = -(0+2) = -2 = -2 + 0 = -2 + 7 - 7 = 5 - 7 = -7 + 5 = (-7)1 + 5$.
Therefore, $-2 = (-7)1 + 5$. $\square$

Example 35. Use the division algorithm to compute 61 divided by -7.

Solution. Since $61 = 7 \cdot 8 + 5$, then $61 = (-7)(-8) + 5$. $\square$

Example 36. Use the division algorithm to compute -59 divided by -7.

Solution.
Observe that

$$\begin{aligned} -59 &= -(7 \cdot 8 + 3) \\ &= -7 \cdot 8 - 3 \\ &= -7 \cdot 8 - 3 + 7 - 7 \\ &= -7 \cdot 8 + 4 - 7 \\ &= -7 \cdot 9 + 4. \end{aligned}$$

Therefore, $-59 = (-7)9 + 4$. $\square$

Example 37. Every perfect square is of the form $4k$ or $4k+1$ for some integer k.
The square of an integer leaves remainder 0 or 1 when divided by 4.

Proof. Let $a \in \mathbb{Z}$.
By the division algorithm, when a is divided by 2, there exist unique integers q and r such that $a = 2q + r$ and $0 \leq r < 2$.
Since $r \in \mathbb{Z}$ and $0 \leq r < 2$, then either $r = 0$ or $r = 1$, so either $a = 2q$ or $a = 2q + 1$.
We consider these cases separately.
Case 1: Suppose $a = 2q$.
Then $a^2 = (2q)^2 = 4q^2 = 4(q^2) + 0$.
Hence, by the division algorithm, when a^2 is divided by 4, the remainder is 0.
Case 1: Suppose $a = 2q + 1$.
Then $a^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$.
Hence, by the division algorithm, when a^2 is divided by 4, the remainder is 1.

Therefore, in all cases, when a^2 is divided by 4, the remainder is either 0 or 1. $\square$

Let $a \in \mathbb{Z}$.
Then a^2 leaves remainder 0 or 1 when divided by 4.
Hence, $a^2 = 4k$ or $a^2 = 4k + 1$ for some integer k.
Therefore, every perfect square is of the form $4k$ or $4k + 1$ for some integer k.

Example 38. The square of any odd integer is of the form $8k + 1$ for some integer k.

Proof. Let n be any odd integer.

Then $n \in \mathbb{Z}$ and n is odd.

When n is divided by 4, by the division algorithm, there are unique integers q and r such that $n = 4q + r$ and $0 \leq r < 4$.

Since $r \in \mathbb{Z}$ and $0 \leq r < 4$, then $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$.

Hence, $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$.

Since $4q = 2(2q)$ and $4q + 2 = 2(2q + 1)$ are both even and n is odd, then n cannot be $4q$ or $4q + 2$.

Thus, either $n = 4q + 1$ or $n = 4q + 3$.

We consider these cases separately.

Case 1: Suppose $n = 4q + 1$.

Observe that

$$\begin{aligned} n^2 &= (4q+1)^2 \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1. \end{aligned}$$

Let $k = 2q^2 + q$.

Then $n^2 = 8k + 1$ and $k \in \mathbb{Z}$.

Case 2: Suppose $n = 4q + 3$.

Observe that

$$\begin{aligned} n^2 &= (4q+3)^2 \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + 8 + 1 \\ &= 8(2q^2 + 3q + 1) + 1. \end{aligned}$$

Let $k = 2q^2 + 3q + 1$.

Then $n^2 = 8k + 1$ and $k \in \mathbb{Z}$.

Therefore, in all cases, $n^2 = 8k + 1$ for some integer k. □

Chapter 2.1 Problems

Exercise 39. Let $a, b \in \mathbb{Z}$ with $b > 0$.

Then there exist unique integers q and r such that $a = bq + r$ with $2b \leq r < 3b$.

Proof. Since $a, b \in \mathbb{Z}$ and $b > 0$, then by the division algorithm, when a is divided by b, there exist unique integers q' and r' such that $a = bq' + r'$ with $0 \leq r' < b$.

Let $q = q' - 2$ and $r = 2b + r'$.
Since q' is a unique integer and $q = q' - 2$, then q is a unique integer.
Since r' is a unique integer and $r = 2b + r'$, then r is a unique integer.
Since $q = q' - 2$, then $q' = q + 2$.
Since $r = 2b + r'$, then $r' = r - 2b$.
Observe that

$$\begin{aligned} a &= bq' + r' \\ &= b(q+2) + (r - 2b) \\ &= bq + 2b + r - 2b \\ &= bq + r. \end{aligned}$$

Since $0 \leq r' < b$, then we add $2b$ to the inequality to obtain $2b+0 \leq 2b+r' < 2b + b$, so $2b \leq r < 3b$.

Therefore, there are unique integers q and r such that $a = bq + r$ and $2b \leq r < 3b$. ☐

Exercise 40. Any integer of the form $6k+5$ is also of the form $3k+2$, but not conversely.

Proof. We prove any integer of the form $6k + 5$ is of the form $3k + 2$.

Let a be any integer of the form $6k + 5$.
Then $a \in \mathbb{Z}$ and $a = 6k + 5$ for some integer k.
Observe that

$$\begin{aligned} a &= 6k + 5 \\ &= 6k + (3 + 2) \\ &= (6k + 3) + 2 \\ &= 3(2k + 1) + 2. \end{aligned}$$

Let $m = 2k + 1$.
Then $m \in \mathbb{Z}$ and $a = 3m + 2$.
Therefore, a is of the form $3m + 2$ for some integer m. ☐

Proof. Conversely, we prove not every integer of the form $3k + 2$ is of the form $6k + 5$.

Thus, we prove there is some integer of the form $3k+2$, but not of the form $6k + 5$.

Consider the integer 14.
Since $14 = 3 \cdot 4 + 2$, then 14 is of the form $3k + 2$ with integer $k = 4$.

Suppose $14 = 6k + 5$ for some integer k.
Then $6k = 14 - 5 = 9$, so $6k = 9$.
Hence, $k = \frac{9}{6} = \frac{3}{2}$.
But, $k = \frac{3}{2}$ is not an integer.
This contradicts that k is an integer.
Therefore, there is no integer k such that $14 = 6k + 5$.

Since 14 is of the form $3k+2$, but there is no integer k such that $14 = 6k+5$, then 14 is an integer of the form $3k + 2$, but not of the form $6k + 5$. $\square$

Exercise 41. Every odd integer is either of the form $4k + 1$ or of the form $4k + 3$ for some integer k.

Proof. Let a be an odd integer.
Then $a = 2b + 1$ for some integer b.
Either b is even or b is not even.
We consider these cases separately.
Case 1: Suppose b is even.
Then $b = 2k$ for some integer k.
Thus, $a = 2b + 1 = 2(2k) + 1 = 4k + 1$.
Therefore, $a = 4k + 1$ for some integer k.
Case 2: Suppose b is not even.
Then b is odd, so $b = 2m + 1$ for some integer m.
Thus, $a = 2b + 1 = 2(2m + 1) + 1 = 4m + 2 + 1 = 4m + 3$.
Therefore, $a = 4m + 3$ for some integer m. $\square$

Proof. Let a be an odd integer.
By the division algorithm, when a is divided by 4, there are unique integers q and r such that $a = 4q + r$ and $0 \leq r < 4$.
Since $0 \leq r < 4$, then either $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$.
Thus, either $a = 4q$ or $a = 4q + 1$ or $a = 4q + 2$ or $a = 4q + 3$.

Since $4q = 2(2q)$ and $4q + 2 = 2(2q + 1)$ are both even and a is odd, then a cannot be $4q$ or $4q + 2$.
Thus, a is either $4q + 1$ or $4q + 3$, so either $a = 4q + 1$ or $a = 4q + 3$.

Therefore, either $a = 4q + 1$ or $a = 4q + 3$ for some integer q, so a is either of the form $4q + 1$ or $4q + 3$ for some integer q. $\square$

Exercise 42. The square of any integer is either of the form $3k$ or of the form $3k + 1$ for some integer k.

Proof. Let $a \in \mathbb{Z}$.
By the division algorithm, when a is divided by 3, there exist unique integers q and r such that $a = 3q + r$ with $0 \leq r < 3$.
Since r is an integer and $0 \leq r < 3$, then either $r = 0$ or $r = 1$ or $r = 2$.
Hence, either $a = 3q$ or $a = 3q + 1$ or $a = 3q + 2$.

We consider these cases separately.
Case 1: Suppose $a = 3q$.
Then $a^2 = (3q)^2 = 3^2q^2 = 3(3q^2)$.
Let $k = 3q^2$.
Then k is an integer and $a^2 = 3k$.
Case 2: Suppose $a = 3q + 1$.
Then $a^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3q(3q + 2) + 1$.
Let $k = q(3q + 2)$.
Then k is an integer and $a^2 = 3k + 1$.
Case 3: Suppose $a = 3q + 2$.
Then $a^2 = (3q+2)^2 = 9q^2+12q+4 = 9q^2+12q+3+1 = 3(3q^2+4q+1)+1$.
Let $k = 3q^2 + 4q + 1$.
Then k is an integer and $a^2 = 3k + 1$. □

Exercise 43. The cube of any integer is either of the form $9k$, $9k+1$, or $9k+8$.

Proof. Let $a \in \mathbb{Z}$.

By the division algorithm, when a is divided by 3, there exist unique integers q and r such that $a = 3q + r$ with $0 \leq r < 3$.

Thus, either $a = 3q$ or $a = 3q + 1$ or $a = 3q + 2$.
We consider these cases separately.
Case 1: Suppose $a = 3q$.
Then $a^3 = (3q)^3 = 27q^3 = 9(3q^3) = 9k$ for integer $k = 3q^3$.
Case 2: Suppose $a = 3q + 1$.
Then $a^3 = (3q + 1)^3 = 27q^3 + 27q^2 + 9q + 1 = 9q(3q^2 + 3q + 1) + 1 = 9k + 1$ for integer $k = q(3q^2 + 3q + 1)$.
Case 3: Suppose $a = 3q + 2$.
Then $a^3 = (3q + 2)^3 = 27q^3 + 54q^2 + 36q + 8 = 9q(3q^2 + 6q + 4) + 8 = 9k + 8$ for integer $k = q(3q^2 + 6q + 4)$. □

Exercise 44. For every $n \in \mathbb{Z}^+$, $6|n(n + 1)(2n + 1)$.

Proof. Define predicate $p(n) : 6|n(n + 1)(2n + 1)$ over $\mathbb{Z}^+$.
We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Let $n = 1$.
Since $1(1 + 1)(2 * 1 + 1) = 6$ and $6|6$, then $p(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then $6|k(k + 1)(2k + 1)$.
Observe that

$$\begin{aligned}(k + 1)(k + 2)(2k + 3) &= 2k^3 + 9k^2 + 13k + 6 \\ &= k(k + 1)(2k + 1) + 6(k + 1)^2.\end{aligned}$$

Since $6|6$, then 6 divides any multiple of 6, so 6 divides $6(k + 1)^2$.

Since 6 divides $k(k + 1)(2k + 1)$ and 6 divides $6(k + 1)^2$, then 6 divides the sum $k(k + 1)(2k + 1) + 6(k + 1)^2$, so 6 divides $(k + 1)(k + 2)(2k + 3)$.

Hence, $p(k + 1)$ is true, so $p(k)$ implies $p(k + 1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction, $p(n)$ is true for all $n \in \mathbb{Z}^+$, so $6|n(n+1)(2n+1)$ for all $n \in \mathbb{Z}^+$. $\square$

Exercise 45. For all $n \in \mathbb{Z}^+$, $6|n(n+1)(2n+1)$.

Proof. By the division algorithm, when n is divided by 6, there exist unique integers q, r such that $n = 6q + r$ with $0 \leq r < 6$, so either $n = 6q$ or $n = 6q + 1$ or $n = 6q + 2$ or $n = 6q + 3$ or $n = 6q + 4$ or $n = 6q + 5$.

We consider each case separately.

Case 1: Suppose $n = 6q$.

Then $6|n$, so 6 divides any multiple of n.

Therefore, $6|n(n+1)(2n+1)$.

Case 2: Suppose $n = 6q + 1$.

Then $n+1 = 6q+2 = 2(3q+1)$ and $2n+1 = 2(6q+1)+1 = 12q+3 = 3(4q+1)$, so $(n+1)(2n+1) = 6(3q+1)(4q+1)$.

Hence, $6|(n+1)(2n+1)$, so 6 divides any multiple of $(n+1)(2n+1)$.

Therefore, $6|n(n+1)(2n+1)$.

Case 3: Suppose $n = 6q + 2$.

Then $n = 2(3q+1)$ and $n+1 = 6q+3 = 3(2q+1)$, so $n(n+1) = 6(3q+1)(2q+1)$.

Hence, $6|n(n+1)$, so 6 divides any multiple of $n(n+1)$.

Therefore, $6|n(n+1)(2n+1)$.

Case 4: Suppose $n = 6q + 3$.

The $n = 3(2q+1)$ and $n+1 = 6q+4 = 2(3q+2)$, so $n(n+1) = 6(2q+1)(3q+2)$.

Hence, $6|n(n+1)$, so 6 divides any multiple of $n(n+1)$.

Therefore, $6|n(n+1)(2n+1)$.

Case 5: Suppose $n = 6q + 4$.

Then $n = 2(3q+2)$ and $2n+1 = 2(6q+4)+1 = 12q+9 = 3(4q+3)$, so $n(2n+1) = 6(3q+2)(4q+3)$.

Hence, $6|n(2n+1)$, so 6 divides any multiple of $n(2n+1)$.

Therefore, $6|n(n+1)(2n+1)$.

Case 6: Suppose $n = 6q + 5$.

Then $n+1 = 6q+6 = 6(q+1)$, so $6|(n+1)$.

Hence, 6 divides any multiple of $n+1$.

Therefore, $6|n(n+1)(2n+1)$. $\square$

Exercise 46. If a positive integer is both a square and a cube, then it must be either of the form $7k$ or $7k+1$.

Solution. We prove:

1. Every square is of the form $7k, 7k+1, 7k+2, 7k+4$.
2. Every cube is of the form $7k, 7k+1, 7k+6$.

So, this would imply any integer that is both a square and a cube must be of a form that it common to both squares and cubes.

We observe that if n is a square and a cube, then $n = a^6$ for $a \in \mathbb{Z}^+$. $\square$

Proof. We first prove every square is of the form $7k, 7k+1, 7k+2$ or $7k+4$ for some integer k.

Let $n \in \mathbb{Z}$.

Suppose n is a square.

Then $n = a^2$ for some integer a.

By the division algorithm, there exist unique integers q and r such that $a = 7q + r$ with $0 \leq r < 7$.

Thus, either $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$ or $r = 4$ or $r = 5$ or $r = 6$.

We consider these cases separately.

Case 1: Suppose $r = 0$.

Then $a = 7q$.

Therefore, $n = (7q)^2 = 7^2q^2 = 7(7q^2) = 7k$ for integer $k = 7q^2$.

Case 2: Suppose $r = 1$.

Then $a = 7q + 1$.

Therefore, $n = (7q+1)^2 = 49q^2 + 14q + 1 = 7q(7q+2) + 1 = 7k + 1$ for integer $k = q(7q+2)$.

Case 3: Suppose $r = 2$.

Then $a = 7q + 2$.

Therefore, $n = (7q+2)^2 = 49q^2 + 28q + 4 = 7q(7q+4) + 4 = 7k + 4$ for integer $k = q(7q+4)$.

Case 4: Suppose $r = 3$.

Then $a = 7q + 3$.

Therefore, $n = (7q+3)^2 = 49q^2 + 42q + 9 = 7(7q^2) + 7(6q) + (7*1+2) = 7(7q^2 + 6q + 1) + 2 = 7k + 2$ for integer $k = 7q^2 + 6q + 1$.

Case 5: Suppose $r = 4$.

Then $a = 7q + 4$.

Therefore, $n = (7q+4)^2 = 49q^2 + 56q + 16 = 7(7q^2) + 7*8q + (7*2+2) = 7(7q^2 + 8q + 2) + 2 = 7k + 2$ for integer $k = 7q^2 + 8q + 2$.

Case 6: Suppose $r = 5$.

Then $a = 7q + 5$.

Therefore, $n = (7q+5)^2 = 49q^2 + 70q + 25 = 7(7q^2) + 7*10q + (7*3+4) = 7(7q^2 + 10q + 3) + 4 = 7k + 4$ for integer $k = 7q^2 + 10q + 3$.

Case 7: Suppose $r = 6$.

Then $a = 7q + 6$.

Therefore, $n = (7q+6)^2 = 49q^2 + 84q + 36 = 7(7q^2) + 7*12q + (7*5+1) = 7(7q^2 + 12q + 5) + 1 = 7k + 1$ for integer $k = 7q^2 + 12q + 5$.

Therefore, in all cases, either $n = 7k$ or $n = 7k+1$ or $n = 7k+2$ or $n = 7k+4$ for some integer k. □

Proof. We next prove every cube is of the form $7k, 7k+1$, or $7k+6$ for some integer k.

Let $n \in \mathbb{Z}$.

Suppose n is a cube.

Then $n = a^3$ for some integer a.

We must prove either $n = 7k$ or $n = 7k + 1$ or $n = 7k + 6$.

By the division algorithm, there exist unique integers q and r such that $a = 7q + r$ with $0 \le r < 7$.

Thus, either $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$ or $r = 4$ or $r = 5$ or $r = 6$.

We consider these cases separately.

Case 1: Suppose $r = 0$.

Then $a = 7q$.

Therefore, $n = (7q)^3 = 7^3q^3 = 7(7^2q^3) = 7(49q^3) = 7k$ for integer $k = 49q^3$.

Case 2: Suppose $r = 1$.

Then $a = 7q + 1$.

Observe that

$$\begin{aligned}
n &= (7q+1)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k} \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2 + \binom{3}{2}(7q) + \binom{3}{3} \\
&= (7q)^3 + 3(7q)^2 + 3(7q) + 1 \\
&= (7^3q^3) + 3(7^2q^2) + 3(7q) + 1 \\
&= 7(7^2q^3 + 3 * 7q^2 + 3q) + 1 \\
&= 7(49q^3 + 21q^2 + 3q) + 1.
\end{aligned}$$

Therefore, $n = 7k + 1$ for integer $k = 49q^3 + 21q^2 + 3q$.

Case 3: Suppose $r = 2$.

Then $a = 7q + 2$.

Observe that

$$\begin{aligned}
n &= (7q+2)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k}(2^k) \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2(2^1) + \binom{3}{2}(7q)(2^2) + \binom{3}{3}(2^3) \\
&= (7q)^3 + 3(7q)^2(2) + 3(7q)(2^2) + 8 \\
&= (7^3q^3) + (3)(2)(7^2q^2) + (3)(2^2)(7q) + (7 * 1 + 1) \\
&= 7(7^2q^3 + (3)(2) * 7q^2 + (3)(2^2)q + 1) + 1 \\
&= 7(49q^3 + 42q^2 + 12q + 1) + 1.
\end{aligned}$$

Therefore, $n = 7k + 1$ for integer $k = 49q^3 + 42q^2 + 12q + 1$.

Case 4: Suppose $r = 3$.

Then $a = 7q + 3$.

Observe that

$$
\begin{aligned}
n &= (7q+3)^3 \\
&= \sum_{k=0}^{3}\binom{3}{k}(7q)^{3-k}(3^k) \\
&= \binom{3}{0}(7q)^3+\binom{3}{1}(7q)^2(3^1)+\binom{3}{2}(7q)(3^2)+\binom{3}{3}(3^3) \\
&= (7q)^3+3(7q)^2(3)+3(7q)(3^2)+27 \\
&= (7^3q^3)+(3)(3)(7^2q^2)+(3)(3^2)(7q)+(7*3+6) \\
&= 7(7^2q^3+(3)(3)*7q^2+(3)(3^2)q+3)+6 \\
&= 7(49q^3+63q^2+27q+3)+6.
\end{aligned}
$$

Therefore, $n = 7k+6$ for integer $k = 49q^3+63q^2+27q+3$.
Case 5: Suppose $r = 4$.
Then $a = 7q+4$.
Observe that

$$
\begin{aligned}
n &= (7q+4)^3 \\
&= \sum_{k=0}^{3}\binom{3}{k}(7q)^{3-k}(4^k) \\
&= \binom{3}{0}(7q)^3+\binom{3}{1}(7q)^2(4^1)+\binom{3}{2}(7q)(4^2)+\binom{3}{3}(4^3) \\
&= (7q)^3+3(7q)^2(4)+3(7q)(4^2)+64 \\
&= (7^3q^3)+(3)(4)(7^2q^2)+(3)(4^2)(7q)+(7*9+1) \\
&= 7(7^2q^3+(3)(4)*7q^2+(3)(4^2)q+9)+1 \\
&= 7(49q^3+84q^2+48q+9)+1.
\end{aligned}
$$

Therefore, $n = 7k+1$ for integer $k = 49q^3+84q^2+48q+9$.
Case 6: Suppose $r = 5$.
Then $a = 7q+5$.
Observe that

$$\begin{aligned}
n &= (7q+5)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k}(5^k) \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2(5^1) + \binom{3}{2}(7q)(5^2) + \binom{3}{3}(5^3) \\
&= (7q)^3 + 3(7q)^2(5) + 3(7q)(5^2) + 125 \\
&= (7^3q^3) + (3)(5)(7^2q^2) + (3)(5^2)(7q) + (7*17+6) \\
&= 7(7^2q^3 + (3)(5)*7q^2 + (3)(5^2)q + 17) + 6 \\
&= 7(49q^3 + 105q^2 + 75q + 17) + 6.
\end{aligned}$$

Therefore, $n = 7k + 6$ for integer $k = 49q^3 + 105q^2 + 75q + 17$.
Case 7: Suppose $r = 6$.
Then $a = 7q + 6$.
Observe that

$$\begin{aligned}
n &= (7q+6)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} (7q)^{3-k}(6^k) \\
&= \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2(6^1) + \binom{3}{2}(7q)(6^2) + \binom{3}{3}(6^3) \\
&= (7q)^3 + 3(7q)^2(6) + 3(7q)(6^2) + 216 \\
&= (7^3q^3) + (3)(6)(7^2q^2) + (3)(6^2)(7q) + (7*30+6) \\
&= 7(7^2q^3 + (3)(6)*7q^2 + (3)(6^2)q + 30) + 6 \\
&= 7(49q^3 + 126q^2 + 108q + 30) + 6.
\end{aligned}$$

Therefore, $n = 7k + 6$ for integer $k = 49q^3 + 126q^2 + 108q + 30$.

Therefore, in all cases, either $n = 7k$ or $n = 7k + 1$ or $n = 7k + 6$ for some integer k. ☐

Proof. Let $n \in \mathbb{Z}$.

Suppose n is a square and a cube.

Then n is a square and n is a cube.

Since every square is of the form $7k, 7k+1, 7k+2, 7k+4$ for some integer k and n is a square, then n is of the form $7k, 7k+1, 7k+2, 7k+4$ for some integer k.

Since every cube is of the form $7m, 7m+1, 7m+6$ for some integer m and n is a cube, then n is of the form $7k, 7k+1, 7k+6$.

Since n is both a square and a cube, then this implies n is of the form that is common to both a square and a cube, so n is of the form $7k$ or $7k+1$. ☐

Exercise 47. another version of the division algorithm

Let $a, b \in \mathbb{Z}$ and $b \neq 0$.

Then there exist unique integers q and r such that $a = bq + r$ and $\frac{-|b|}{2} < r \leq \frac{|b|}{2}$.

Proof. Since $b \in \mathbb{Z}$ and $b \neq 0$, then either $b > 0$ or $b < 0$.

We consider these cases separately.

Case 1: Suppose $b > 0$.

By the division algorithm, when a is divided by b, there are unique integers q' and r' such that $a = bq' + r'$ and $0 \leq r' < b$.

Since $0 \leq r' < b$, then either $0 \leq r' \leq \frac{b}{2}$ or $\frac{b}{2} < r' < b$.

Case 1a: Suppose $\frac{b}{2} < r' < b$.

Let $r = r' - b$ and $q = q' + 1$.

Then $r' = r + b$ and $q' = q - 1$.

Since q' is a unique integer and $q = q' + 1$, then q is a unique integer.

Since r' is a unique integer and $r = r' - b$, then r is a unique integer.

Since $b > 0$, then $|b| = b$ and $\frac{b}{2} > 0$.

Observe that

$$\begin{aligned} a &= bq' + r' \\ &= b(q-1) + (r+b) \\ &= bq - b + r + b \\ &= bq + r. \end{aligned}$$

Observe that

$$\begin{aligned} \frac{b}{2} < r' < b &\Leftrightarrow \frac{b}{2} - b < r' - b < b - b \\ &\Leftrightarrow \frac{-b}{2} < r < 0 \\ &\Rightarrow \frac{-b}{2} < r < 0 < \frac{b}{2} \\ &\Rightarrow \frac{-b}{2} < r < \frac{b}{2} \\ &\Rightarrow \frac{-|b|}{2} < r < \frac{|b|}{2}. \end{aligned}$$

Therefore, there are unique integers q and r such that $a = bq + r$ and $\frac{-|b|}{2} < r < \frac{|b|}{2}$.

Case 1b: Suppose $0 \leq r' \leq \frac{b}{2}$.

Let $r = r'$ and $q = q'$.
Since q' is a unique integer and $q = q'$, then q is a unique integer.
Since r' is a unique integer and $r = r'$, then r is a unique integer.
Since $b > 0$, then $|b| = b$ and $\frac{b}{2} > 0$, so $\dfrac{-b}{2} < 0$.
Observe that

$$\begin{aligned} a &= bq' + r' \\ &= bq + r. \end{aligned}$$

Since $\dfrac{-b}{2} < 0$ and $0 \leq r' \leq \dfrac{b}{2}$, then $\dfrac{-b}{2} < 0 \leq r' \leq \dfrac{b}{2}$, so $\dfrac{-b}{2} < r' \leq \dfrac{b}{2}$.
Observe that

$$\begin{aligned} \frac{-b}{2} < r' \leq \frac{b}{2} &\Leftrightarrow \frac{-b}{2} < r \leq \frac{b}{2} \\ &\Leftrightarrow \frac{-|b|}{2} < r \leq \frac{|b|}{2}. \end{aligned}$$

Therefore, there are unique integers q and r such that $a = bq + r$ and $\dfrac{-|b|}{2} < r \leq \dfrac{|b|}{2}$.
Case 2: Suppose $b < 0$.
Then $b \neq 0$.
Hence, by the extended version of the division algorithm, when a is divided by b, there are unique integers q' and r' such that $a = bq' + r'$ and $0 \leq r' < |b|$.
Since $0 \leq r' < |b|$, then either $0 \leq r' \leq \dfrac{|b|}{2}$ or $\dfrac{|b|}{2} < r' < |b|$.
Case 2a: Suppose $\dfrac{|b|}{2} < r' < |b|$.
Let $r = r' - |b|$ and $q = q' - 1$.
Then $r' = r + |b|$ and $q' = 1 + q$.
Since q' is a unique integer and $q = q' - 1$, then q is a unique integer.
Since r' is a unique integer and $r = r' - |b|$, then r is a unique integer.
Since $b < 0$, then $|b| = -b > 0$, so $\dfrac{|b|}{2} > 0$.
Observe that

$$\begin{aligned} a &= bq' + r' \\ &= b(1 + q) + (r + |b|) \\ &= b + bq + r + |b| \\ &= b + bq + r - b \\ &= bq + r. \end{aligned}$$

Observe that

$$\begin{aligned}
\frac{|b|}{2} < r' < |b| &\Leftrightarrow \frac{|b|}{2} - |b| < r' - |b| < |b| - |b| \\
&\Leftrightarrow \frac{-|b|}{2} < r < 0 \\
&\Rightarrow \frac{-|b|}{2} < r < 0 < \frac{|b|}{2} \\
&\Rightarrow \frac{-|b|}{2} < r < \frac{|b|}{2}.
\end{aligned}$$

Therefore, there are unique integers q and r such that $a = bq + r$ and $\frac{-|b|}{2} < r < \frac{|b|}{2}$.

Case 2b: Suppose $0 \leq r' \leq \frac{|b|}{2}$.
Let $r = r'$ and $q = q'$.
Since q' is a unique integer and $q = q'$, then q is a unique integer.
Since r' is a unique integer and $r = r'$, then r is a unique integer.
Since $b < 0$, then $|b| = -b$ and $\frac{b}{2} < 0$.
Observe that

$$\begin{aligned}
a &= bq' + r' \\
&= bq + r.
\end{aligned}$$

Since $0 \leq r' \leq \frac{|b|}{2}$ and $|b| = -b$, then $0 \leq r' \leq \frac{-b}{2}$.
Since $\frac{b}{2} < 0$ and $0 \leq r' \leq \frac{-b}{2}$, then $\frac{b}{2} < 0 \leq r' \leq \frac{-b}{2}$, so $\frac{b}{2} < r' \leq \frac{-b}{2}$.
Observe that

$$\begin{aligned}
\frac{b}{2} < r' \leq \frac{-b}{2} &\Leftrightarrow \frac{b}{2} < r \leq \frac{-b}{2} \\
&\Leftrightarrow \frac{-|b|}{2} < r \leq \frac{|b|}{2}.
\end{aligned}$$

Therefore, there are unique integers q and r such that $a = bq + r$ and $\frac{-|b|}{2} < r \leq \frac{|b|}{2}$. ∎

Exercise 48. There is no integer in the sequence $11, 111, 1111, 11111, ...$ that is a perfect square.

Proof. Let (a_n) be the sequence $11, 111, 1111, 11111, ...$
Then $a_n = 10 * a_{n-1} + 1$ for positive integers $n > 1$ and $a_1 = 11$.
We first prove each term of the sequence has the form $4k+3$ for some integer k.

Thus, we must prove for all $n \in \mathbb{Z}^+$, there exists $k \in \mathbb{Z}$ such that $a_n = 4k+3$.

We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : (\exists k \in \mathbb{Z})(a_n = 4k+3)\}$.

Basis:

Since $1 \in \mathbb{Z}^+$ and $2 \in \mathbb{Z}$ and $a_1 = 11 = 4*2+3$, then $1 \in S$.

Since $2 \in \mathbb{Z}^+$ and $27 \in \mathbb{Z}$ and $a_2 = 10*a_1+1 = 10*11+1 = 111 = 4*27+3$, then $2 \in S$.

Induction:

Let $m \in \mathbb{Z}^+$ with $m \geq 2$ such that $p(m)$ is true.

Then there exists $k \in \mathbb{Z}$ such that $a_m = 4k+3$.

Since $m \in \mathbb{Z}^+$, then $m+1 \in \mathbb{Z}^+$.

Since $m+1 > m \geq 2 > 1$, then $m+1 > 1$.

Observe that

$$\begin{aligned}
a_{m+1} &= 10a_m + 1 \\
&= 10(4k+3)+1 \\
&= 40k+31 \\
&= 4\cdot 10k + (4\cdot 7+3) \\
&= (4\cdot 10k + 4\cdot 7)+3 \\
&= 4(10k+7)+3.
\end{aligned}$$

Let $p = 10k+7$.

Since $k \in \mathbb{Z}$, then $p \in \mathbb{Z}$ and $a_{m+1} = 4p+3$.

Since $m+1 \in \mathbb{Z}^+$ and there exists $p \in \mathbb{Z}$ such that $a_{m+1} = 4p+3$, then $m+1 \in S$.

Hence, $m \in S$ implies $m+1 \in S$ for all integers $m \geq 2$.

Since $1 \in S$ and $2 \in S$ and $m \in S$ implies $m+1 \in S$ for all integers $m \geq 2$, then by induction $S = \mathbb{Z}^+$.

Therefore, for all $n \in \mathbb{Z}^+$, there exists $k \in \mathbb{Z}$ such that $a_n = 4k+3$, so every term a_n has the form $4k+3$ for some integer k. $\square$

Proof. We prove no term of the sequence $11, 111, 1111, ...$ is a perfect square.

Let a_n be a term of the sequence $11, 111, 1111, ...$

Since every term a_n has the form $4k+3$ for some integer k, then a_n has the form $4k+3$ for some integer k, so a_n is of the form $4k+3$.

By lemma 37, every perfect square is either of the form $4k$ or $4k+1$, so if n is a perfect square, then either $n = 4k$ or $n = 4k+1$.

Hence, if $n \neq 4k$ and $n \neq 4k+1$, then n is not a perfect square.

Since $4k+3 \neq 4k$ and $4k+3 \neq 4k+1$, then we conclude $4k+3$ is not a perfect square.

Thus, a_n is not a perfect square.

Therefore, every term of the sequence $11, 111, 1111, ...$ is not a perfect square, so there is no term of the sequence that is a perfect square. $\square$

Chapter 2.2 The greatest common divisor

Example 49. Let $a, b, c \in \mathbb{Z}$.
Disprove: if $a|c$ and $b|c$, then $ab|c$.

Proof. Let $a = 6$ and $b = 8$ and $c = 24$.
Observe that $6|24$ and $8|24$, but $6 \cdot 8 \not| 24$. $\square$

Example 50. Let $a, b, c \in \mathbb{Z}$.
Disprove: if $a|bc$, then $a|b$ or $a|c$.

Proof. Let $a = 12$ and $b = 9$ and $c = 8$.
Observe that $12|9 \cdot 8$, but $12 \not| 8$. $\square$

Chapter 2.2 Problems

Exercise 51. Let $a, b, c \in \mathbb{Z}$.
If $a|b$ and $a|c$, then $a^2|bc$.

Proof. Suppose $a|b$ and $a|c$.
Then $b = am$ and $c = an$ for some integers m and n.
Thus, $bc = (am)(an) = a(ma)n = a(am)n = (aa)(mn) = a^2(mn)$.
Since $mn \in \mathbb{Z}$ and $bc = a^2(mn)$, then $a^2|bc$. $\square$

Exercise 52. Let $a, b, c \in \mathbb{Z}$.
Disprove: If $a|(b + c)$, then either $a|b$ or $a|c$.

Proof. Let $a = 3$ and $b = 4$ and $c = 5$.
Since $3|9$, then $3|(4 + 5)$, but $3 \not| 4$ and $3 \not| 5$. $\square$

Exercise 53. Let $a \in \mathbb{Z}$.
Then either a or $a + 2$ or $a + 4$ is divisible by 3.

Proof. By the division algorithm, when a is divided by 3, there exist unique integers q and r such that $a = 3q + r$ with $0 \leq r < 3$.
Thus, either $a = 3q$ or $a = 3q + 1$ or $a = 3q + 2$.
We consider these cases separately.
Case 1: Suppose $a = 3q$.
Since $a = 3q$ and $q \in \mathbb{Z}$, then $3|a$, so a is divisible by 3.
Case 2: Suppose $a = 3q + 1$.
Then $a + 2 = (3q + 1) + 2 = 3q + 3 = 3(q + 1)$.
Since $a + 2 = 3(q + 1)$ and $q + 1 \in \mathbb{Z}$, then $3|(a + 2)$, so $a + 2$ is divisible by 3.
Case 3: Suppose $a = 3q + 2$.
Then $a + 4 = (3q + 2) + 4 = 3q + 6 = 3(q + 2)$.
Since $a + 4 = 3(q + 2)$ and $q + 2 \in \mathbb{Z}$, then $3|(a + 4)$, so $a + 4$ is divisible by 3. $\square$

Exercise 54. A product of 3 consecutive integers is divisible by 3

Let $a \in \mathbb{Z}$.

Then $3|a(a+1)(a+2)$.

Proof. By the division algorithm, when a is divided by 3, then either $a = 3k$ or $a = 3k+1$ or $a = 3k+2$ for some integer k.

We consider these cases separately.

Case 1: Suppose $a = 3k$.

Then $3|a$, so 3 divides any multiple of a.

Hence, $3|a(a+1)(a+2)$.

Case 2: Suppose $a = 3k+1$.

Then $a+2 = (3k+1)+2 = 3k+3 = 3(k+1)$, so $3|(a+2)$.

Hence, 3 divides any multiple of $a+2$, so $3|a(a+1)(a+2)$.

Case 3: Suppose $a = 3k+2$.

Then $a+1 = (3k+2)+1 = 3k+3 = 3(k+1)$, so $3|(a+1)$.

Hence, 3 divides any multiple of $a+1$, so $3|a(a+1)(a+2)$.

Therefore, in all cases, $3|a(a+1)(a+2)$. □

Exercise 55. For any integer a, $4 \nmid (a^2+2)$.

Proof. Let $a \in \mathbb{Z}$.

By the division algorithm, when a is divided by 4, there exist unique integers q and r such that $a = 4q+r$ and $0 \leq r < 4$.

Thus, either $a = 4q$ or $a = 4q+1$ or $a = 4q+2$ or $a = 4q+3$.

We consider these cases separately.

Case 1: Suppose $a = 4q$.

Then $a^2+2 = (4q)^2+2 = 4^2q^2+2 = 4(4q^2)+2$.

Let $k = 4q^2$.

Then $k \in \mathbb{Z}$ and $a^2+2 = 4k+2$.

Case 2: Suppose $a = 4q+1$.

Then $a^2+2 = (4q+1)^2+2 = (16q^2+8q+1)+2 = 16q^2+8q+3 = 4(4q^2+2q)+3$.

Let $k = 4q^2+2q$.

Then $k \in \mathbb{Z}$ and $a^2+2 = 4k+3$.

Case 3: Suppose $a = 4q+2$.

Then $a^2+2 = (4q+2)^2+2 = (16q^2+16q+4)+2 = 4(4q^2+4q+1)+2$.

Let $k = 4q^2+4q+1$.

Then $k \in \mathbb{Z}$ and $a^2+2 = 4k+2$.

Case 4: Suppose $a = 4q+3$.

Then $a^2+2 = (4q+3)^2+2 = (16q^2+24q+9)+2 = 16q^2+24q+11 = 16q^2+24q+(4*2+3) = 4(4q^2+6q+2)+3$.

Let $k = 4q^2+6q+2$.

Then $k \in \mathbb{Z}$ and $a^2+2 = 4k+3$.

Therefore, in all cases, either $a^2 + 2 = 4k + 2$ or $a^2 + 2 = 4k + 3$ for some integer k, so the remainder is either 2 or 3 when $a^2 + 2$ is divided by 4.

Hence, the remainder is not zero when $a^2 + 2$ is divided by 4.

Since $4|(a^2 + 2)$ iff the remainder is zero when $a^2 + 2$ is divided by 4, then $4 \not|(a^2 + 2)$ iff the remainder is not zero when $a^2 + 2$ is divided by 4.

Since the remainder is not zero when a^2+2 is divided by 4, then we conclude $4 \not|(a^2 + 2)$, as desired. □

Proof. Let $a \in \mathbb{Z}$.

Suppose $4|(a^2 + 2)$.

Then there is an integer k such that $a^2 + 2 = 4k$.

Either a is even or not.

We consider these cases separately.

Case 1: Suppose a is even.

Then $a = 2m$ for some integer m.

Thus, $4k = a^2 + 2 = (2m)^2 + 2 = 4m^2 + 2 = 2(2m^2 + 1)$.

Hence, $2k = 2m^2 + 1$.

But, this equation implies the even integer $2k$ equals the odd integer $2m^2+1$, a contradiction.

Case 2: Suppose a is odd.

Then a^2 is odd, so $a^2 + 2$ is odd.

Since $2(2k) = 4k = a^2 + 2$ and $2k$ is an integer, then $a^2 + 2$ is even.

But, this contradicts the fact that $a^2 + 2$ is odd.

Therefore, $4 \not|(a^2 + 2)$. □

Proof. Let $a \in \mathbb{Z}$.

Then $a^2 \in \mathbb{Z}$ is a perfect square.

By lemma 37, every perfect square is either of the form $4k$ or $4k+1$ for some integer k, so if n is a perfect square, then either $n = 4k$ or $n = 4k + 1$ for some integer k.

Since a^2 is a perfect square, then we conclude either $a^2 = 4k$ or $a^2 = 4k + 1$ for some integer k.

Thus, either $a^2 + 2 = 4k + 2$ or $a^2 + 2 = (4k + 1) + 2 = 4k + 3$ for some integer k.

Hence, by the division algorithm, when a^2+2 is divided by 4, the remainder is either 2 or 3.

Thus, when $a^2 + 2$ is divided by 4, the remainder is not zero.

Since $4|(a^2 + 2)$ iff the remainder is zero when $a^2 + 2$ is divided by 4, then $4 \not|(a^2 + 2)$ iff the remainder is not zero when $a^2 + 2$ is divided by 4.

Since the remainder is not zero when a^2+2 is divided by 4, then we conclude $4 \not|(a^2 + 2)$. □

Exercise 56. For all $n \in \mathbb{Z}^+$, 7 divides $2^{3n} - 1$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : 7|(2^{3n} - 1)\}$.

Basis:

Since $2^{3*1} - 1 = 7 = 7 * 1$, then 7 divides $2^{3*1} - 1$, so $1 \in S$.

Induction:

Let $k \in \mathbb{Z}^+$ such that $k \in S$.

Then $7|(2^{3k} - 1)$.

Since $k \in \mathbb{Z}^+$, then $k + 1 \in \mathbb{Z}^+$.

Since $7|(2^{3k} - 1)$, then $2^{3k} - 1 = 7x$ for some integer x.

Observe that

$$\begin{aligned}
2^{3(k+1)} - 1 &= 2^{3k+3} - 1 \\
&= 2^{3k} * 2^3 - 1 \\
&= 8 \cdot 2^{3k} - 1 \\
&= 8 \cdot 2^{3k} - 8 + 7 \\
&= 8(2^{3k} - 1) + 7 \\
&= 8(7x) + 7 \\
&= 7(8x) + 7 \\
&= 7(8x + 1).
\end{aligned}$$

Since $8x + 1 \in \mathbb{Z}$ and $2^{3(k+1)} - 1 = 7(8x + 1)$, then 7 divides $2^{3(k+1)} - 1$.

Since $k + 1 \in \mathbb{Z}^+$ and 7 divides $2^{3(k+1)} - 1$, then $k + 1 \in S$.

Hence, $k \in S$ implies $k + 1 \in S$ for all $k \in \mathbb{Z}^+$.

Since $1 \in S$ and $k \in S$ implies $k + 1 \in S$ for all $k \in \mathbb{Z}^+$, then by induction, $S = \mathbb{Z}^+$, so $7|(2^{3n} - 1)$ for all $n \in \mathbb{Z}^+$. □

Exercise 57. For all $n \in \mathbb{Z}^+$, 8 divides $3^{2n} + 7$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : 8|3^{2n} + 7\}$.

Basis:

Since $3^{2*1} + 7 = 16 = 8 * 2$, then 8 divides $3^{2*1} + 7$, so $1 \in S$.

Induction:

Let $k \in \mathbb{Z}^+$ such that $k \in S$.

Then $8|(3^{2k} + 7)$.

Since $k \in \mathbb{Z}^+$, then $k + 1 \in \mathbb{Z}^+$.

Since $8|(3^{2k} + 7)$, then $3^{2k} + 7 = 8x$ for some integer x.

Observe that

$$
\begin{aligned}
3^{2(k+1)} + 7 &= 3^{2k+2} + 7 \\
&= 3^{2k} * 3^2 + 7 \\
&= 9 * 3^{2k} + 7 \\
&= (8+1)3^{2k} + 7 \\
&= 8(3^{2k}) + 3^{2k} + 7 \\
&= 8(3^{2k}) + 8x \\
&= 8(3^{2k} + x) \\
&= 8(9^k + x).
\end{aligned}
$$

Since $9^k + x \in \mathbb{Z}$ and $3^{2(k+1)} + 7 = 8(9^k + x)$, then 8 divides $3^{2(k+1)} + 7$.
Since $k+1 \in \mathbb{Z}^+$ and 8 divides $3^{2(k+1)} + 7$, then $k+1 \in S$.
Hence, $k \in S$ implies $k+1 \in S$ for all $k \in \mathbb{Z}^+$.

Since $1 \in S$ and $k \in S$ implies $k+1 \in S$ for all $k \in \mathbb{Z}^+$, then by induction $S = \mathbb{Z}^+$, so $8|(3^{2n} + 7)$ for all $n \in \mathbb{Z}^+$. $\square$

Exercise 58. For all $n \in \mathbb{Z}^+$, $2^n + (-1)^{n+1}$ is divisible by 3.

Proof. We prove by induction on n.
Let $S = \{n \in \mathbb{Z}^+ : 3|2^n + (-1)^{n+1}\}$.
Basis:
Since $2^1 + (-1)^{1+1} = 2 + 1 = 3 = 3 \cdot 1$, then 3 divides $2^1 + (-1)^{1+1}$, so $1 \in S$.
Induction:
Let $k \in \mathbb{Z}^+$ such that $k \in S$.
Then $3|2^k + (-1)^{k+1}$.
Since $k \in \mathbb{Z}^+$, then $k+1 \in \mathbb{Z}^+$.
Since $3|2^k + (-1)^{k+1}$, then $2^k + (-1)^{k+1} = 3x$ for some integer x.
Observe that

$$
\begin{aligned}
2^{k+1} + (-1)^{(k+1)+1} &= 2^k \cdot 2 + (-1)^{k+1}(-1) \\
&= 2^k + 2^k - (-1)^{k+1} \\
&= 2^k + (2-1)2^k - (-1)^{k+1} \\
&= 2^k + 2(2^k) - 2^k - (-1)^{k+1} \\
&= 3(2^k) - [2^k + (-1)^{k+1}] \\
&= 3(2^k) - 3x \\
&= 3(2^k - x).
\end{aligned}
$$

Since $2^k - x \in \mathbb{Z}$ and $2^{k+1} + (-1)^{(k+1)+1} = 3(2^k - x)$, then 3 divides $2^{k+1} + (-1)^{(k+1)+1}$.
Since $k+1 \in \mathbb{Z}^+$ and 3 divides $2^{k+1} + (-1)^{(k+1)+1}$, then $k+1 \in S$.
Hence, $k \in S$ implies $k+1 \in S$ for all $k \in \mathbb{Z}^+$.

Since $1 \in S$ and $k \in S$ implies $k+1 \in S$ for all $k \in \mathbb{Z}^+$, then by induction, $S = \mathbb{Z}^+$, so $3|(2^n + (-1)^{n+1})$ for all $n \in \mathbb{Z}^+$. ☐

Lemma 59. *If n is an odd integer, then $8|(n^2 - 1)$.*

Proof. Suppose n is an odd integer.

Then $n = 2a + 1$ for some integer a.

Thus $n^2 - 1 = (2a+1)^2 - 1 = 4a^2 + 4a + 1 - 1 = 4a^2 + 4a = 4a(a+1)$.

Since the product of two consecutive integers is even and $a(a+1)$ is a product of two consecutive integers a and $a+1$, then $a(a+1)$ is even.

Thus $a(a+1) = 2b$ for some integer b.

Therefore, $n^2 - 1 = 4a(a+1) = 4(2b) = 8b$, so $8|(n^2 - 1)$. ☐

Proof. Suppose n is an odd integer.

By the division algorithm, when n is divided by 4, there are unique integers q and r such that $n = 4q + r$ with $0 \leq r < 4$.

Since $r \in \mathbb{Z}$ and $0 \leq r < 4$, then either $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$, so either $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$.

Since $4q = 2(2q)$ is even and n is odd, then $n \neq 4q$.

Since $4q + 2 = 2(2q+1)$ is even and n is odd, then $n \neq 4q + 2$.

Since $n \neq 4q$ and $n \neq 4q+2$, then we conclude either $n = 4q+1$ or $n = 4q+3$.

We consider each case separately.

Case 1: Suppose $n = 4q + 1$.

Then $n^2 - 1 = (4q+1)^2 - 1 = 16q^2 + 8q + 1 - 1 = 16q^2 + 8q = 8(2q^2 + q)$.

Since $2q^2 + q \in \mathbb{Z}$ and $n^2 - 1 = 8(2q^2 + q)$, then $8|(n^2 - 1)$.

Case 2: Suppose $n = 4q + 3$.

Then $n^2 - 1 = (4q+3)^2 - 1 = 16q^2 + 24q + 9 - 1 = 16q^2 + 24q + 8 = 8(2q^2 + 3q + 1)$.

Since $2q^2 + 3q + 1 \in \mathbb{Z}$ and $n^2 - 1 = 8(2q^2 + 3q + 1)$, then $8|(n^2 - 1)$.

Therefore, in all cases, $8|(n^2 - 1)$. ☐

Lemma 60. *If n is an odd integer, then $n^2 \equiv 1 \pmod 8$.*

Proof. Suppose n is an odd integer.

Then $n = 2k + 1$ for some integer k.

Thus, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$.

Since the product of two consecutive integers is even and $k(k+1)$ is a product of two consecutive integers, then $k(k+1)$ is even, so $2|k(k+1)$.

Hence $4 \cdot 2|4k(k+1)$, so $8|4k(k+1)$.

Thus, $8|(4k^2 + 4k)$, so $4k^2 + 4k \equiv 0 \pmod 8$.

Therefore, $4k^2 + 4k + 1 \equiv 1 \pmod 8$, so $n^2 \equiv 1 \pmod 8$. ☐

Exercise 61. Let $a \in \mathbb{Z}$.

If $2 \not| a$ and $3 \not| a$, then $24|(a^2 - 1)$.

Proof. Suppose $2 \not| a$ and $3 \not| a$.

Since $2 \not| a$, then a is not even, so a is odd.

By lemma 59, if a is an odd integer, then $8|(a^2-1)$.

Since a is an odd integer, then we conclude $8|(a^2-1)$.

Since $3 \not| a$, then by the division algorithm, when a is divided by 3, either $a = 3m+1$ or $a = 3m+2$ for some integer m.

If $a = 3m+1$, then $a^2-1 = (3m+1)^2-1 = 9m^2+6m+1-1 = 9m^2+6m = 3m(3m+2)$, so $3|(a^2-1)$.

If $a = 3m+2$, then $a^2-1 = (3m+2)^2-1 = 9m^2+12m+4-1 = 9m^2+12m+3 = 3(3m^2+4m+1)$, so $3|(a^2-1)$.

In either case, $3|(a^2-1)$.

Since $3|(a^2-1)$ and $8|(a^2-1)$, then a^2-1 is a common multiple of 3 and 8.

Since $\gcd(3,8) = 1$, then 3 and 8 are relatively prime.

Since a^2-1 is a common multiple of 3 and 8 and 3 and 8 are relatively prime, then a^2-1 is a multiple of the product $3 \cdot 8 = 24$.

Therefore, a^2-1 is a multiple of 24, so $24|(a^2-1)$. $\square$

Exercise 62. The sum of the squares of two odd integers cannot be a perfect square.

Proof. Let x and y be two odd integers.

Then $x = 2a+1$ and $y = 2b+1$ for some integers a and b.

Thus,

$$\begin{aligned}
x^2+y^2 &= (2a+1)^2+(2b+1)^2 \\
&= 4a^2+4a+1+4b^2+4b+1 \\
&= 4a^2+4b^2+4a+4b+2 \\
&= 4(a^2+b^2+a+b)+2.
\end{aligned}$$

Let $k = a^2+b^2+a+b$.

Then $x^2+y^2 = 4k+2$ and $k \in \mathbb{Z}$, so x^2+y^2 is of the form $4k+2$ for some integer k.

By exercise 37, every perfect square is of the form $4k$ or $4k+1$ for some integer k.

Thus, if n is a perfect square, then either $n = 4k$ or $n = 4k+1$ for some integer k.

Hence, if $n \neq 4k$ and $n \neq 4k+1$ for some integer k, then n is not a perfect square.

Since $4k+2 \neq 4k$ and $4k+2 \neq 4k+1$, then $4k+2$ is not a perfect square.

Since $x^2+y^2 = 4k+2$, then we conclude x^2+y^2 is not a perfect square. $\square$

Exercise 63. The product of four consecutive integers is one less than a perfect square.

Proof. Let $n \in \mathbb{Z}$.

We must prove there exists $m \in \mathbb{Z}$ such that $n(n+1)(n+2)(n+3) = m^2 - 1$.

Let $m = (n+1)(n+2) - 1$.

Since $n \in \mathbb{Z}$, then $m \in \mathbb{Z}$.

Observe that

$$\begin{aligned} m^2 - 1 &= [(n+1)(n+2) - 1]^2 - 1 \\ &= (n^2 + 3n + 2 - 1)^2 - 1 \\ &= (n^2 + 3n + 1)^2 - 1 \\ &= (n^2 + 3n + 1 - 1)(n^2 + 3n + 1 + 1) \\ &= (n^2 + 3n)(n^2 + 3n + 2) \\ &= n(n+3)(n+2)(n+1) \\ &= n(n+1)(n+2)(n+3). \end{aligned}$$

□

Exercise 64. The difference of two consecutive cubes is never divisible by 2.

Proof. Let a and b be two consecutive cubes.

Then $a = n^3$ and $b = (n+1)^3$ for some $n \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned} b - a &= (n+1)^3 - n^3 \\ &= (n^3 + 3n^2 + 3n + 1) - n^3 \\ &= 3n^2 + 3n + 1 \\ &= 3n(n+1) + 1. \end{aligned}$$

Since a product of two consecutive integers is even and n and $n+1$ are consecutive integers, then the product $n(n+1)$ is even.

Hence, $n(n+1) = 2k$ for some integer k.

Thus, $b - a = 3n(n+1) + 1 = 3(2k) + 1 = 2(3k) + 1$ is odd, so $b - a$ is not even.

Therefore, $2 \nmid (b - a)$, so $b - a$ is not divisible by 2. □

Proof. Let a and b be two consecutive cubes.

Then $a = n^3$ and $b = (n+1)^3$ for some $n \in \mathbb{Z}^+$.

Since $n \in \mathbb{Z}$, then either n is even or n is not even.

We consider these cases separately.

Case 1: Suppose n is even.

Then n^3 is even and $n+1$ is odd.

Since n^3 is even and $a = n^3$, then a is even.

Since $n+1$ is odd, then $(n+1)^3$ is odd, so b is odd.

Since the difference of an even and odd integer is odd and b is odd and a is even, then the difference $b - a$ is odd.

Case 2: Suppose n is not even.

Then n is odd, so n^3 is odd and $n+1$ is even.
Since n^3 is odd and $a = n^3$, then a is odd.
Since $n+1$ is even, then $(n+1)^3$ is even, so b is even.
Since the difference of an even and odd integer is odd and b is even and a is odd, then the difference $b-a$ is odd.

Hence, in all cases, $b-a$ is odd, so $b-a$ is not even.
Therefore, $2 \nmid (b-a)$, so $b-a = (n+1)^3 - n^3$ is not divisible by 2. ☐

Exercise 65. Let $a \in \mathbb{Z}^*$.
Then $\gcd(a, 0) = |a|$.

Proof. Since $a \in \mathbb{Z}^*$, then $a \in \mathbb{Z}$ and $a \neq 0$, so either $a > 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$.
Then $\gcd(a, 0) = a = |a|$.
Case 2: Suppose $a < 0$.
Then $|a| = -a$ and $-a > 0$.
Since $-a > 0$, then $\gcd(-a, 0) = -a$.
Therefore, $\gcd(a, 0) = \gcd(-a, 0) = -a = |a|$.

In all cases, we have $\gcd(a, 0) = |a|$. ☐

Exercise 66. Let $a \in \mathbb{Z}^*$.
Then $\gcd(a, a) = |a|$.

Proof. Since $a \in \mathbb{Z}^*$, then $a \in \mathbb{Z}$ and $a \neq 0$, so either $a > 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$.
Then $\gcd(a, a) = a = |a|$.
Case 2: Suppose $a < 0$.
Then $|a| = -a$ and $-a > 0$.
Since $-a > 0$, then $\gcd(-a, -a) = -a$.
Therefore, $\gcd(a, a) = \gcd(-a, -a) = -a = |a|$.

In all cases, we have $\gcd(a, a) = |a|$. ☐

Exercise 67. Let $a \in \mathbb{Z}^*$.
Then $\gcd(a, 1) = 1$.

Proof. Since $a \in \mathbb{Z}^*$, then $a \in \mathbb{Z}$ and $a \neq 0$, so either $a > 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$.
Then $\gcd(a, 1) = 1$.
Case 2: Suppose $a < 0$.
Then $-a > 0$, so $\gcd(-a, 1) = 1$.
Therefore, $\gcd(a, 1) = \gcd(-a, 1) = 1$.

In all cases, we have $\gcd(a, 1) = 1$. $\square$

Exercise 68. Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$.
Then $\gcd(a, a+n)|n$.

Proof. Suppose $a = 0$ and $a + n = 0$.
Then $0 = a + n = 0 + n = n$, so $n = 0$.
Since $n \in \mathbb{Z}^+$, then $n > 0$, so $n \neq 0$.
Hence, we have $n = 0$ and $n \neq 0$, a contradiction.
Therefore, either $a \neq 0$ or $a + n \neq 0$, so a and $a + n$ are not both zero.
Thus, $\gcd(a, a+n)$ exists and is unique.

Let $d = \gcd(a, a+n)$.
Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|(a+n)$.
Since $d|(a+n)$ and $d|a$, then d is a common divisor of $a + n$ and a.
Hence, d divides the difference $(a+n) - a = a + n - a = n$.
Therefore, $d|n$, as desired. $\square$

Note: If d is a common divisor of $a + n$ and a, then $d|n$.

Exercise 69. Consecutive integers are relatively prime.
Let $a \in \mathbb{Z}$.
Then $\gcd(a, a+1) = 1$.

Proof. Since 1 divides any integer, then $1|a$ and $1|(a+1)$, so 1 is a common divisor of a and $a + 1$.

Let c be any common divisor of a and $a + 1$.
Then $c|a$ and $c|(a+1)$, so c divides the difference $(a+1) - a = 1$.
Hence, $c|1$, so any common divisor of a and $a + 1$ divides 1.
Since $1 \in \mathbb{Z}^+$ and 1 is a common divisor of a and $a + 1$, and any common divisor of a and $a+1$ divides 1, then by definition of gcd, $1 = \gcd(a, a+1)$. $\square$

Proof. Since $1 \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$, then by exercise 68, $\gcd(a, a+1)$ divides 1.
Since $n|1$ iff $n = \pm 1$, then $\gcd(a, a+1) = 1$ or $\gcd(a, a+1) = -1$.
Since the greatest common divisor is positive, then we conclude $\gcd(a, a+1) = 1$. $\square$

Proof. Since $1 = 0+1 = 0a+1 = (-1+1)a+1 = (-1)a+a+1 = (-1)a+1(a+1)$ is a linear combination of a and $a + 1$, then $1 = \gcd(a, a+1)$. $\square$

Exercise 70. Let $a, b \in \mathbb{Z}$.
If there exist integers x and y such that $ax+by = \gcd(a, b)$, then $\gcd(x, y) = 1$.

Proof. Suppose there exist integers x and y such that $ax + by = \gcd(a, b)$.
Let $d = \gcd(a, b)$.
Then $d|a$ and $d|b$ and $ax + by = d$.
Since $d|a$, then $a = dr$ for some integer r, so $r = \frac{a}{d}$.
Since $d|b$, then $b = ds$ for some integer s, so $s = \frac{b}{d}$.
Divide the equation by d to obtain $1 = \frac{ax+by}{d} = \frac{a}{d} \cdot x + \frac{b}{d} \cdot y$.
Since $1 = \frac{a}{d} \cdot x + \frac{b}{d} \cdot y$ and $\frac{a}{d} \in \mathbb{Z}$ and $\frac{b}{d} \in \mathbb{Z}$, then 1 is a linear combination of x and y.
Therefore, $\gcd(x, y) = 1$. ☐

Exercise 71. The product of any three consecutive integers is a multiple of 6.
For all $n \in \mathbb{Z}^+$, $6|(n^3 - n)$.

Proof. We prove the statement by induction.
Let $p(n)$ be the predicate $6|(n^3 - n)$ over $\mathbb{Z}^+$.
Basis:
Since $1^3 - 1 = 1 - 1 = 0 = 6 \cdot 0$, then $1^3 - 1 = 6 \cdot 0$, so $6|(1^3 - 1)$.
Hence, $p(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then $6|(k^3 - k)$, so $k^3 - k = 6a$ for some integer a.
Observe that

$$\begin{aligned}
(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\
&= k^3 + 3k^2 + 3k + 1 - k - 1 \\
&= k^3 + 3k^2 + 3k - k \\
&= k^3 - k + 3k^2 + 3k \\
&= (k^3 - k) + (3k^2 + 3k) \\
&= 6a + (3k^2 + 3k) \\
&= 6a + 3k(k+1).
\end{aligned}$$

Thus, $(k+1)^3 - (k+1) = 6a + 3k(k+1)$.
A product of two consecutive integers is even.
Since k and $k+1$ are consecutive integers, then $k(k+1)$ is even.
Hence, $k(k+1) = 2b$ for some integer b.
Observe that

$$\begin{aligned}
(k+1)^3 - (k+1) &= 6a + 3k(k+1) \\
&= 6a + 3(2b) \\
&= 6a + 6b \\
&= 6(a+b).
\end{aligned}$$

Since $a+b \in \mathbb{Z}$ and $(k+1)^3-(k+1) = 6(a+b)$, then 6 divides $(k+1)^3-(k+1)$, so $p(k+1)$ is true.

Thus, $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction $p(n)$ is true for all $n \in \mathbb{Z}^+$.

Therefore, $6|(n^3-n)$ for all $n \in \mathbb{Z}^+$. $\square$

Exercise 72. The product of any three consecutive integers is divisible by 6.

$\forall n \in \mathbb{Z}, 6|n(n+1)(n+2)$.

Proof. Let $n \in \mathbb{Z}$.

Let $p = n(n+1)(n+2)$.

We must prove $6|p$.

By the division algorithm, either $n = 6k$ or $n = 6k+1$ or $n = 6k+2$ or $n = 6k+3$ or $n = 6k+4$ or $n = 6k+5$ for some integer k.

We consider these cases separately.

Case 1: Suppose $n = 6k$.

Then $6|n$, so 6 divides any multiple of n.

Therefore, $6|p$.

Case 2: Suppose $n = 6k+1$.

Since $n+1 = (6k+1)+1 = 6k+2 = 2(3k+1)$, then $2|(n+1)$.

Since $n+2 = (6k+1)+2 = 6k+3 = 3(2k+1)$, then $3|(n+2)$.

Since $2|(n+1)$ and $3|(n+2)$, then $6|(n+1)(n+2)$.

Hence, 6 divides any multiple of $(n+1)(n+2)$, so $6|p$.

Case 3: Suppose $n = 6k+2$.

Then $n = 6k+2 = 2(3k+1)$, so $2|n$.

Since $n+1 = (6k+2)+1 = 6k+3 = 3(2k+1)$, then $3|(n+1)$.

Since $2|n$ and $3|(n+1)$, then $6|n(n+1)$.

Hence, 6 divides any multiple of $n(n+1)$, so $6|p$.

Case 4: Suppose $n = 6k+3$.

Then $n = 6k+3 = 3(2k+1)$, so $3|n$.

Since $n+1 = (6k+3)+1 = 6k+4 = 2(3k+2)$, then $2|(n+1)$.

Since $3|n$ and $2|(n+1)$, then $6|n(n+1)$.

Hence, 6 divides any multiple of $n(n+1)$, so $6|p$.

Case 5: Suppose $n = 6k+4$.

Then $n+2 = (6k+4)+2 = 6k+6 = 6(k+1)$, so $6|(n+2)$.

Hence, 6 divides any multiple of $n+2$, so $6|p$.

Case 6: Suppose $n = 6k+5$.

Then $n+1 = (6k+5)+1 = 6k+6 = 6(k+1)$, so $6|(n+1)$.

Hence, 6 divides any multiple of $n+1$, so $6|p$.

In all cases, $6|p$. ☐

Proof. Let $n \in \mathbb{Z}$.
Let $p = n(n+1)(n+2)$.
We must prove $6|p$.

Since a product of two consecutive integers is even and $n(n+1)$ is a product of two consecutive integers, then $n(n+1)$ is even.
Hence, 2 divides $n(n+1)$, so 2 divides any multiple of $n(n+1)$.
Therefore, $2|p$.

By the division algorithm, when n is divided by 3, there are unique integers q and r such that $n = 3q + r$ and $0 \leq r < 3$.
Since $r \in \mathbb{Z}$ and $0 \leq r < 3$, then $r = 0$ or $r = 1$ or $r = 2$, so $n = 3q$ or $n = 3q + 1$ or $n = 3q + 2$.
We consider these cases separately.
Case 1: Suppose $n = 3q$.
Then $3|n$, so 3 divides any multiple of n.
Hence, $3|p$.
Case 2: Suppose $n = 3q + 1$.
Then $n + 2 = (3q + 1) + 2 = 3q + 3 = 3(q + 1)$, so $3|n + 2$.
Hence, 3 divides any multiple of $n + 2$, so $3|p$.
Case 3: Suppose $n = 3q + 2$.
Then $n + 1 = (3q + 2) + 1 = 3q + 3 = 3(q + 1)$, so $3|n + 1$.
Hence, 3 divides any multiple of $n + 1$, so $3|p$.

In all cases, $3|p$.

Since $2|p$ and $3|p$ and $\gcd(2, 3) = 1$, then $2 \cdot 3$ divides p, so $6|p$, as desired. ☐

Proof. We prove by induction(strong).
Basis:
If $n = 1$ then the statement S_1 is $6|1 * 2 * 3$. This simplifies to $6|6$, which is true because 6 = 6 * 1.
If $n = 2$ then the statement S_2 is $6|2 * 3 * 4$. This simplifies to $6|24$, which is true because 24 = 6 * 4.
Induction:
We must prove $S_1 \wedge S_2 \wedge ... \wedge S_k \Rightarrow S_{k+1}$ for $k \geq 2$.
This implies we must prove $S_{k-1} \wedge S_k \Rightarrow S_{k+1}$ for $k \geq 2$.
For simplicity, let $m = k - 1$.
Then $S_{k-1} \wedge S_k \Rightarrow S_{k+1}$ for $k \geq 2$ becomes
$S_m \wedge S_{m+1} \Rightarrow S_{m+2}$ for $m \geq 1$.
We prove the latter statement using direct proof.
Suppose $S_m \wedge S_{m+1}$ for $m \geq 1$.

We must prove that these assumptions together imply S_{m+2}.

Since $S_m \wedge S_{m+1}$ is true by assumption, then S_m is certainly true.

This implies $6|m(m+1)(m+2)$ which implies $m(m+1)(m+2) = 6a, a \in \mathbb{Z}$, by definition of divisibility.

Thus $m(m+1)(m+2) = m(m^2+3m+2) = m^3+3m^2+2m = 6a$.

Observe the following equalities:

$$\begin{aligned}
(m+2)(m+3)(m+4) &= (m+2)(m^2+7m+12) \\
&= m^3+9m^2+26m+24 \\
&= (m^3+3m^2+2m)+(6m^2+24m+24) \\
&= 6a+6(m^2+4m+4) \\
&= 6(a+m^2+4m+4).
\end{aligned}$$

Since $a+m^2+4m+4 \in \mathbb{Z}$, then by definition of divisibility, $6|(m+2)(m+3)(m+4)$.

Hence $S_m \wedge S_{m+1} \Rightarrow S_{m+2}$ for $m \geq 1$.

Thus, $S_{k-1} \wedge S_k \Rightarrow S_{k+1}$ for $k \geq 2$.

It follows by strong induction that $6|n(n+1)(n+2)$ for all $n \in \mathbb{N}$. □

Exercise 73. The product of any four consecutive integers is divisible by 24.

$\forall n \in \mathbb{Z}, 24|n(n+1)(n+2)(n+3)$.

Proof. Let $n \in \mathbb{Z}$.

Let $p = n(n+1)(n+2)(n+3)$.

We must prove $24|p$.

By exercise 72, a product of three consecutive integers is divisible by 6.

Since $n(n+1)(n+2)$ is a product of three consecutive integers, then $n(n+1)(n+2)$ is divisible by 6.

Hence, 6 divides $n(n+1)(n+2)$, so 6 divides any multiple of $n(n+1)(n+2)$.

Therefore, $6|p$.

Since $3|6$ and $6|p$, then $3|p$.

By the division algorithm, when n is divided by 8, there are unique integers q and r such that $n = 8q+r$ and $0 \leq r < 8$.

Since $r \in \mathbb{Z}$ and $0 \leq r < 8$, then $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$ or $r = 4$ or $r = 5$ or $r = 6$ or $r = 7$, so $n = 8q$ or $n = 8q+1$ or $n = 8q+2$ or $n = 8q+3$ or $n = 8q+4$ or $n = 8q+5$ or $n = 8q+6$ or $n = 8q+7$.

We consider these cases separately.

Case 1: Suppose $n = 8q$.

Then $8|n$, so 8 divides any multiple of n.

Hence, $8|p$.

Case 2: Suppose $n = 8q+1$.

Then $n+3 = (8q+1)+3 = 8q+4 = 4(2q+1)$, so $4|n+3$.

Hence, 4 divides any multiple of $n+3$, so $4|(n+2)(n+3)$.

Since a product of two consecutive integers is even, then $n(n+1)$ is even, so $2|n(n+1)$.

Since $2|n(n+1)$ and $4|(n+2)(n+3)$, then the product $2 \cdot 4$ divides the product $n(n+1)(n+2)(n+3)$, so $8|p$.

Case 3: Suppose $n = 8q+2$.

Then $n+2 = (8q+2)+2 = 8q+4 = 4(2q+1)$, so $4|n+2$.

Hence, 4 divides any multiple of $n+2$, so $4|(n+2)(n+3)$.

Since a product of two consecutive integers is even, then $n(n+1)$ is even, so $2|n(n+1)$.

Since $2|n(n+1)$ and $4|(n+2)(n+3)$, then the product $2 \cdot 4$ divides the product $n(n+1)(n+2)(n+3)$, so $8|p$.

Case 4: Suppose $n = 8q+3$.

Then $n+1 = (8q+3)+1 = 8q+4 = 4(2q+1)$, so $4|n+1$.

Hence, 4 divides any multiple of $n+1$, so $4|n(n+1)$.

Since a product of two consecutive integers is even, then $(n+2)(n+3)$ is even, so $2|(n+2)(n+3)$.

Since $4|n(n+1)$ and $2|(n+2)(n+3)$, then the product $4 \cdot 2$ divides the product $n(n+1)(n+2)(n+3)$, so $8|p$.

Case 5: Suppose $n = 8q+4$.

Then $n = 8q+4 = 4(2q+1)$, so $4|n$.

Hence, 4 divides any multiple of n, so $4|n(n+1)$.

Since a product of two consecutive integers is even, then $(n+2)(n+3)$ is even, so $2|(n+2)(n+3)$.

Since $4|n(n+1)$ and $2|(n+2)(n+3)$, then the product $4 \cdot 2$ divides the product $n(n+1)(n+2)(n+3)$, so $8|p$.

Case 6: Suppose $n = 8q+5$.

Then $n+3 = (8q+5)+3 = 8q+8 = 8(q+1)$, so $8|n+3$.

Hence, 8 divides any multiple of $n+3$, so $8|p$.

Case 7: Suppose $n = 8q+6$.

Then $n+2 = (8q+6)+2 = 8q+8 = 8(q+1)$, so $8|n+2$.

Hence, 8 divides any multiple of $n+2$, so $8|p$.

Case 8: Suppose $n = 8q+7$.

Then $n+1 = (8q+7)+1 = 8q+8 = 8(q+1)$, so $8|n+1$.

Hence, 8 divides any multiple of $n+1$, so $8|p$.

In all cases, $8|p$.

Since $3|p$ and $8|p$ and $\gcd(3,8) = 1$, then $3 \cdot 8$ divides p, so $24|p$, as desired. $\square$

Exercise 74. The product of any five consecutive integers is divisible by 120**.**

$\forall n \in \mathbb{Z}, 120|n(n+1)(n+2)(n+3)(n+4)$.

Proof. Let $n \in \mathbb{Z}$.
Let $p = n(n+1)(n+2)(n+3)(n+4)$.
We must prove $120|p$.

By exercise 73, a product of four consecutive integers is divisible by 24.
Since $n(n+1)(n+2)(n+3)$ is a product of four consecutive integers, then $n(n+1)(n+2)(n+3)$ is divisible by 24.
Hence, 24 divides $n(n+1)(n+2)(n+3)$, so 24 divides any multiple of $n(n+1)(n+2)(n+3)$.
Therefore, $24|p$.

By the division algorithm, when n is divided by 5, there are unique integers q and r such that $n = 5q + r$ and $0 \leq r < 5$.
Since $r \in \mathbb{Z}$ and $0 \leq r < 5$, then $r = 0$ or $r = 1$ or $r = 2$ or $r = 3$ or $r = 4$, so $n = 5q$ or $n = 5q + 1$ or $n = 5q + 2$ or $n = 5q + 3$ or $n = 5q + 4$.
We consider these cases separately.
Case 1: Suppose $n = 5q$.
Then $5|n$, so 5 divides any multiple of n.
Hence, $5|p$.
Case 2: Suppose $n = 5q + 1$.
Then $n + 4 = (5q + 1) + 4 = 5q + 5 = 5(q + 1)$, so $5|n + 4$.
Hence, 5 divides any multiple of $n + 4$, so $5|p$.
Case 3: Suppose $n = 5q + 2$.
Then $n + 3 = (5q + 2) + 3 = 5q + 5 = 5(q + 1)$, so $5|n + 3$.
Hence, 5 divides any multiple of $n + 3$, so $5|p$.
Case 4: Suppose $n = 5q + 3$.
Then $n + 2 = (5q + 3) + 2 = 5q + 5 = 5(q + 1)$, so $5|n + 2$.
Hence, 5 divides any multiple of $n + 2$, so $5|p$.
Case 5: Suppose $n = 5q + 4$.
Then $n + 1 = (5q + 4) + 1 = 5q + 5 = 5(q + 1)$, so $5|n + 1$.
Hence, 5 divides any multiple of $n + 1$, so $5|p$.

In all cases, $5|p$.

Since $5|p$ and $24|p$ and $\gcd(5, 24) = 1$, then $5 \cdot 24$ divides p, so 120 divides p, as desired. $\square$

Exercise 75. If a is an odd integer, then $24|a(a^2 - 1)$.

Proof. Suppose a is an odd integer.
Let $p = a(a^2 - 1)$.
Then $p = a(a - 1)(a + 1) = (a - 1)a(a + 1)$ is a product of three consecutive integers.
By exercise 72, a product of three consecutive integers is divisible by 6.
Hence, p is divisible by 6, so $6|p$.
Since $3|6$ and $6|p$, then $3|p$.

By lemma 59, if n is an odd integer, then $8|(n^2 - 1)$.

Since a is an odd integer, then we conclude $8|(a^2 - 1)$.

Hence, 8 divides any multiple of $a^2 - 1$, so $8|p$.

Since $3|p$ and $8|p$, then p is a common multiple of 3 and 8.

Since $\gcd(3, 8) = 1$, then 3 and 8 are relatively prime.

Since p is a common multiple of 3 and 8 and 3 and 8 are relatively prime, then p is a multiple of the product $3 \cdot 8$, so p is a multiple of 24.

Therefore, $24|p$, as desired. $\square$

Exercise 76. If a and b are odd integers, then $8|(a^2 - b^2)$.

Proof. Suppose a and b are odd integers.

Then a is an odd integer and b is an odd integer.

By lemma 59, if n is an odd integer, then $8|(n^2 - 1)$.

Since a is an odd integer, then we conclude $8|(a^2 - 1)$, so $a^2 - 1 = 8k$ for some integer k.

Hence, $a^2 = 8k + 1$.

Since b is an odd integer, then we conclude $8|(b^2 - 1)$, so $b^2 - 1 = 8m$ for some integer m.

Hence, $b^2 = 8m + 1$.

Observe that

$$\begin{aligned} a^2 - b^2 &= (8k + 1) - (8m + 1) \\ &= 8k + 1 - 8m - 1 \\ &= 8k - 8m \\ &= 8(k - m). \end{aligned}$$

Since $k - m \in \mathbb{Z}$ and $a^2 - b^2 = 8(k - m)$, then 8 divides $a^2 - b^2$, so $8|(a^2 - b^2)$, as desired. $\square$

Proof. Suppose a and b are odd integers.

Then a is an odd integer and b is an odd integer.

By lemma 60, if n is any odd integer, then $n^2 \equiv 1 \pmod 8$.

Since a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

Since b is an odd integer, then $b^2 \equiv 1 \pmod 8$, so $1 \equiv b^2 \pmod 8$.

Since $a^2 \equiv 1 \pmod 8$ and $1 \equiv b^2 \pmod 8$, then $a^2 \equiv b^2 \pmod 8$.

Therefore, $8|(a^2 - b^2)$. $\square$

Proof. Suppose a and b are odd integers.

Since the sum of two odd integers is even and a and b are odd integers, then $a + b$ is even, so $a + b = 2m$ for some integer m.

Since the difference of two odd integers is even and a and b are odd integers, then $a - b$ is even, so $a - b = 2n$ for some integer n.

Thus, $(a + b) + (a - b) = 2m + 2n = 2(m + n)$, so $2a = 2(m + n)$.

Hence, $a = m + n$.

Since a is odd and $a = m + n$, then $m + n$ is odd.

Either m is even and n is even, or m is even and n is odd, or m is odd and n is even, or m is odd and n is odd.

Suppose m is even and n is even.

Since the sum of two even integers is even, then $m+n$ is even, so $m+n$ is not odd.

Hence, if m and n are both even, then $m+n$ is not odd, so if $m+n$ is odd, then m and n are not both even.

Since $m+n$ is odd, then we conclude m and n cannot be both even.

Suppose m is odd and n is odd.

Since the sum of two odd integers is even, then $m+n$ is even, so $m+n$ is not odd.

Hence, if m and n are both odd, then $m+n$ is not odd, so if $m+n$ is odd, then m and n are not both odd.

Since $m+n$ is odd, then we conclude m and n cannot be both odd.

Since m and n cannot be both even or both odd, then we conclude either m is even and n is odd, or m is odd and n is even.

We consider these cases separately.

Case 1: Suppose m is even and n is odd.

Since m is even, then $m = 2c$ for some integer c.

Observe that

$$\begin{aligned}
a^2 - b^2 &= (a+b)(a-b) \\
&= (2m)(2n) \\
&= 4mn \\
&= 4(2c)n \\
&= 8(cn).
\end{aligned}$$

Hence, $a^2 - b^2 = 8(cn)$, so 8 divides $a^2 - b^2$.

Case 2: Suppose m is odd and n is even.

Since n is even, then $n = 2d$ for some integer d.

Observe that

$$\begin{aligned}
a^2 - b^2 &= (a+b)(a-b) \\
&= (2m)(2n) \\
&= 4mn \\
&= 4m(2d) \\
&= 8(nd).
\end{aligned}$$

Hence, $a^2 - b^2 = 8(nd)$, so 8 divides $a^2 - b^2$.

Therefore, in all cases, 8 divides $a^2 - b^2$, so $8|(a^2 - b^2)$, as desired. $\square$

Exercise 77. Let $a \in \mathbb{Z}$.
If $2 \not| a$ and $3 \not| a$, then $24|(a^2 + 23)$.

Proof. Suppose $2 \not| a$ and $3 \not| a$.
Since $2 \not| a$, then a is not divisible by 2, so a is not even.
Hence, a is odd.
By lemma 59, if n is an odd integer, then $8|(n^2 - 1)$.
Since a is an odd integer, then we conclude $8|(a^2 - 1)$.
Since $8|(a^2 - 1)$ and $8|24$, then 8 divides the sum $(a^2 - 1) + 24 = a^2 + 23$, so $8|(a^2 + 23)$.

By the division algorithm, when a is divided by 3, there are unique integers q and r such that $a = 3q + r$ and $0 \leq r < 3$.
Since $r \in \mathbb{Z}$ and $0 \leq r < 3$, then either $r = 0$ or $r = 1$ or $r = 2$, so either $a = 3q$ or $a = 3q + 1$ or $a = 3q + 2$.
Since $3|a$ iff $a = 3q$, then $3 \not| a$ iff $a \neq 3q$.
Since $3 \not| a$, then we conclude $a \neq 3q$.
Thus, either $a = 3q + 1$ or $a = 3q + 2$.
We consider these cases separately.
Case 1: Suppose $a = 3q + 1$.
Observe that

$$\begin{aligned} a^2 + 23 &= (3q + 1)^2 + 23 \\ &= (9q^2 + 6q + 1) + 23 \\ &= 9q^2 + 6q + 24 \\ &= 3(3q^2 + 2q + 8). \end{aligned}$$

Thus, $a^2 + 23 = 3(3q^2 + 2q + 8)$, so $3|(a^2 + 23)$.
Case 2: Suppose $a = 3q + 2$.
Observe that

$$\begin{aligned} a^2 + 23 &= (3q + 2)^2 + 23 \\ &= (9q^2 + 12q + 4) + 23 \\ &= 9q^2 + 12q + 27 \\ &= 3(3q^2 + 4q + 9). \end{aligned}$$

Thus, $a^2 + 23 = 3(3q^2 + 4q + 9)$, so $3|(a^2 + 23)$.

Thus, in all cases, $3|(a^2 + 23)$.

Since $3|(a^2+23)$ and $8|(a^2+23)$, then a^2+23 is a common multiple of 3 and 8.

Since $\gcd(3,8)=1$, then 3 and 8 are relatively prime.

Since a^2+23 is a common multiple of 3 and 8 and 3 and 8 are relatively prime, then a^2+23 is a multiple of the product $3\cdot 8$, so a^2+23 is a multiple of 24.

Therefore, $24|(a^2+23)$. $\square$

Exercise 78. If $a \in \mathbb{Z}$, then $360|a^2(a^2-1)(a^2-4)$.

Proof. Let $a \in \mathbb{Z}$.

Let $p = a^2(a^2-1)(a^2-4)$.

Then $p = a^2(a-1)(a+1)(a-2)(a+2) = a(a-2)(a-1)a(a+1)(a+2)$.

Let $s = (a-2)(a-1)a(a+1)(a+2)$.

Then $p = as$ and s is a product of five consecutive integers.

By exercise 74, the product of any five consecutive integers is divisible by 120.

Since s is a product of five consecutive integers, then s is divisible by 120, so $120|s$.

Hence, 120 divides any multiple of s, so $120|p$.

Since $40|120$ and $120|p$, then $40|p$.

By the division algorithm, when a is divided by 3, either $a=3q$ or $a=3q+1$ or $a=3q+2$ for some integer q.

We consider each case separately.

Case 1: Suppose $a=3q$.

Then $a^2=(3q)^2=9q^2$, so $9|a^2$.

Hence, 9 divides any multiple of a^2, so $9|p$.

Case 2: Suppose $a=3q+1$.

Then $a-1=3q$, so $3|(a-1)$.

Since $a+2=(3q+1)+2=3q+3=3(q+1)$, then $3|(a+2)$.

Since $3|(a-1)$ and $3|(a+2)$, then the product $3\cdot 3$ divides the product $(a-1)(a+2)$, so 9 divides $(a-1)(a+2)$.

Hence, 9 divides any multiple of $(a-1)(a+2)$, so $9|p$.

Case 3: Suppose $a=3q+2$.

Then $a-2=3q$, so $3|(a-2)$.

Since $a+1=(3q+2)+1=3q+3=3(q+1)$, then $3|(a+1)$.

Since $3|(a-2)$ and $3|(a+1)$, then the product $3\cdot 3$ divides the product $(a-2)(a+1)$, so 9 divides $(a-2)(a+1)$.

Hence, 9 divides any multiple of $(a-2)(a+1)$, so $9|p$.

Therefore, in all cases, $9|p$.

Since $9|p$ and $40|p$ and $\gcd(9, 40) = 1$, then $9 \cdot 40$ divides p, so $360|p$, as desired. $\square$

Exercise 79. Let $a, b, c \in \mathbb{Z}$.
Then $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = \gcd(a, c) = 1$.

Proof. We prove if $\gcd(a, b) = \gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

Suppose $\gcd(a, b) = 1 = \gcd(a, c)$.
Since $\gcd(a, b) = 1$, then there exist integers m and n such that $1 = ma + nb$.
Since $\gcd(a, c) = 1$, then there exist integers r and s such that $1 = ra + sc$.
Observe that

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (ma + nb) \cdot (ra + sc) \\ &= mara + masc + nbra + nbsc \\ &= (mar + msc + nbr)a + nbsc \\ &= (mar + msc + nbr)a + (ns)bc. \end{aligned}$$

Since $mar + msc + nbr$ and ns are integers and $(mar + msc + nbr)a + (ns)bc = 1$, then 1 is a linear combination of a and bc, so $\gcd(a, bc) = 1$, as desired. $\square$

Proof. Conversely, we prove if $\gcd(a, bc) = 1$, then $\gcd(a, b) = \gcd(a, c) = 1$.

Suppose $\gcd(a, bc) = 1$.
Then there exist integers m and n such that $ma + n(bc) = 1$.
Since $1 = ma + n(bc) = ma + (nb)c$ and m and nb are integers, then 1 is a linear combination of a and c, so $\gcd(a, c) = 1$.
Since $1 = ma + n(bc) = ma + n(cb) = ma + (nc)b$ and m and nc are integers, then 1 is a linear combination of a and b so $1 = \gcd(a, b)$.
Therefore, $\gcd(a, b) = 1 = \gcd(a, c)$, as desired. $\square$

Exercise 80. Let $a, b, c \in \mathbb{Z}$.
If $\gcd(a, b) = 1$ and $c|a$, then $\gcd(b, c) = 1$.

Proof. Suppose $\gcd(a, b) = 1$ and $c|a$.
Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma + nb = 1$.
Since $c|a$, then $a = ck$ for some integer k.
Observe that

$$\begin{aligned} 1 &= ma + nb \\ &= m(ck) + nb \\ &= nb + m(ck) \\ &= nb + m(kc) \\ &= nb + (mk)c. \end{aligned}$$

Since n and mk are integers and $nb + (mk)c = 1$, then 1 is a linear combination of b and c, so $\gcd(b, c) = 1$. $\square$

Proof. Suppose $\gcd(a, b) = 1$ and $c|a$.
Since 1 divides every integer, then $1|b$ and $1|c$, so 1 is a common divisor of b and c.

Let d be any common divisor of b and c.
Then $d|b$ and $d|c$.
Since $d|c$ and $c|a$, then $d|a$.
Since $\gcd(a, b) = 1$, then $ma + nb = 1$ for some integers m and n.
Hence, 1 is a linear combination of a and b.
Since $d|a$ and $d|b$, then d divides any linear combination of a and b, so $d|1$.
Therefore, any common divisor of b and c divides 1.

Since 1 is a common divisor of b and c, and any common divisor of b and c divides 1, then by definition of gcd, $1 = \gcd(b, c)$. $\square$

Exercise 81. Let $a, b, c \in \mathbb{Z}$.
If $\gcd(a, b) = 1$, then $\gcd(ac, b) = \gcd(c, b)$.

Proof. Suppose $\gcd(a, b) = 1$.
Then $1 = ma + nb$ for some integers m and n.
Let $d = \gcd(c, b)$.
Then d is the least positive linear combination of c and b, and d is a common divisor of c and b.
Since d is the least positive linear combination of c and b, then $d \in \mathbb{Z}^+$ and $d = rc + sb$ for some integers r and s.
Observe that

$$\begin{aligned}
d &= 1 \cdot d \\
&= (ma + nb) \cdot (rc + sb) \\
&= marc + masb + nbrc + nbsb \\
&= (mr)ac + masb + nbrc + nbsb \\
&= (mr)ac + (mas + nrc + nbs)b.
\end{aligned}$$

Since mr and $mas+nrc+nbs$ are integers and $(mr)ac+(mas+nrc+nbs)b = d$, then d is a linear combination of ac and b.
Hence, d is a multiple of $\gcd(ac, b)$.
Let $e = \gcd(ac, b)$.
Then d is a multiple of e, so $e|d$.

Since $e = \gcd(ac, b)$, then $e \in \mathbb{Z}^+$ and any common divisor of ac and b divides e.
Since d is a common divisor of c and b, then $d|c$ and $d|b$.
Since $d|c$, then d divides any multiple of c, so $d|ac$.
Since $d|ac$ and $d|b$, then we conclude $d|e$.

Since $d \in \mathbb{Z}^+$ and $e \in \mathbb{Z}^+$ and $d|e$ and $e|d$, then $d = e$.

Therefore, $\gcd(ac, b) = e = d = \gcd(c, b)$, so $\gcd(ac, b) = \gcd(c, b)$, as desired. ☐

Exercise 82. Let $d, a, b \in \mathbb{Z}$.

If $d|(a+b)$ and $\gcd(a, b) = 1$, then $\gcd(d, a) = \gcd(d, b) = 1$.

Proof. Suppose $d|(a+b)$ and $\gcd(a, b) = 1$.

Since $d|(a+b)$, then $a + b = dk$ for some integer k.

Since $\gcd(a, b) = 1$, then $1 = ma + nb$ for some integers m and n.

Observe that

$$\begin{aligned}
1 &= ma + nb \\
&= m(dk - b) + nb \\
&= mdk - mb + nb \\
&= mkd - mb + nb \\
&= mkd + nb - mb \\
&= (mk)d + (n - m)b.
\end{aligned}$$

Since mk and $n - m$ are integers and $1 = (mk)d + (n - m)b$, then 1 is a linear combination of d and b, so $\gcd(d, b) = 1$.

Observe that

$$\begin{aligned}
1 &= ma + nb \\
&= ma + n(dk - a) \\
&= ma + ndk - na \\
&= ndk + ma - na \\
&= nkd + ma - na \\
&= (nk)d + (m - n)a.
\end{aligned}$$

Since nk and $m - n$ are integers and $1 = (nk)d + (m - n)a$, then 1 is a linear combination of d and a, so $1 = \gcd(d, a)$.

Therefore, $\gcd(d, a) = 1 = \gcd(d, b)$. ☐

Proof. Suppose $d|(a+b)$ and $\gcd(a, b) = 1$.

Let $e = \gcd(d, a)$.

Then $e \in \mathbb{Z}^+$ and e is a common divisor of d and a, so $e|d$ and $e|a$.

Since $e|d$ and $d|(a+b)$, then $e|(a+b)$.

Since $e|(a+b)$ and $e|a$, then e divides the difference $(a+b) - a = b$, so $e|b$.

Since $\gcd(a, b) = 1$, then any common divisor of a and b divides 1.

Since $e|a$ and $e|b$, then e is a common divisor of a and b, so $e|1$.

Since $e \in \mathbb{Z}^+$ and $e|1$, then $e = 1$.

Let $f = \gcd(d, b)$.
Then $f \in \mathbb{Z}^+$ and f is a common divisor of d and b, so $f|d$ and $f|b$.
Since $f|d$ and $d|(a+b)$, then $f|(a+b)$.
Since $f|(a+b)$ and $f|b$, then f divides the difference $(a+b)-b=a$, so $f|a$.
Since $\gcd(a,b)=1$, then any common divisor of a and b divides 1.
Since $f|a$ and $f|b$, then f is a common divisor of a and b, so $f|1$.
Since $f \in \mathbb{Z}^+$ and $f|1$, then $f=1$.

Therefore, $\gcd(d,a) = e = 1 = f = \gcd(d,b)$, so $\gcd(d,a) = 1 = \gcd(d,b)$, as desired. $\square$

Chapter 2.3 The Euclidean Algorithm

Example 83. Express $\gcd(12378, 3054)$ as a linear combination of 12378 and 3054.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$\begin{aligned}
12378 &= 3054 \cdot 4 + 162 \\
3054 &= 162 \cdot 18 + 138 \\
162 &= 138 \cdot 1 + 24 \\
138 &= 24 \cdot 5 + 18 \\
24 &= 18 \cdot 1 + 6 \\
18 &= 6 \cdot 3 + 0.
\end{aligned}$$

Thus, $\gcd(12378, 3054) = \gcd(3054, 162) = \gcd(162, 138) = \gcd(138, 24) = \gcd(24, 18) = \gcd(18, 6) = 6$.

We backtrack through the equations to find the linear combination.

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 \\
&= 24 - (138 - 24 \cdot 5) \cdot 1 \\
&= 6 \cdot 24 - 138 \\
&= 6(162 - 138 \cdot 1) - 138 \\
&= 6 \cdot 162 - 7 \cdot 138 \\
&= 6 \cdot 162 - 7(3054 - 162 \cdot 18) \\
&= 132 \cdot 162 - 7(3054) \\
&= 132(12378 - 3054 \cdot 4) - 7(3054) \\
&= 132 \cdot 12378 - 535 \cdot 3054 \\
&= 132 \cdot 12378 + (-535)3054.
\end{aligned}$$

Therefore, $\gcd(12378, 3054) = 6 = (132)12378 + (-535)3054$. $\square$

Example 84. Prove $\gcd(39, 42, 54) = 3$.

Proof. Since $39 = 3 \cdot 13$, then $3|39$.

Since $42 = 3 \cdot 14$, then $3|42$.

Since $54 = 3 \cdot 18$, then $3|54$.

Since $3|39$ and $3|42$ and $3|54$, then 3 is a common divisor of $39, 42$, and 54.

Since $3 \in \mathbb{Z}^+$ and 3 is a common divisor of $39, 42$, and 54, then 3 is a positive common divisor of $39, 42$, and 54.

Let $c \in \mathbb{Z}$ such that $c|39$ and $c|42$ and $c|54$.

Then $39 = ck_1$ and $42 = ck_2$ and $54 = ck_3$ for some integers k_1, k_2, and k_3.

Observe that

$$\begin{aligned} 3 &= 39(-1) + 42(1) + 54(0) \\ &= ck_1(-1) + ck_2(1) + ck_3(0) \\ &= c(-k_1) + ck_2 + 0 \\ &= c(-k_1) + ck_2 \\ &= c(-k_1 + k_2). \end{aligned}$$

Since $-k_1 + k_2 \in \mathbb{Z}$ and $3 = c(-k_1 + k_2)$, then $c|3$, so any common divisor of $39, 42, 54$ divides 3.

Since 3 is a positive common divisor of $39, 42, 54$, and any common divisor of $39, 42, 54$ divides 3, then $3 = \gcd(39, 42, 54)$, as desired. □

Example 85. Prove $\gcd(49, 210, 350) = 7$.

Proof. Since $49 = 7 \cdot 7$, then $7|49$.

Since $210 = 7 \cdot 30$, then $7|210$.

Since $350 = 7 \cdot 50$, then $7|350$.

Since $7|49$ and $7|210$ and $7|350$, then 7 is a common divisor of $49, 210$, and 350.

Since $7 \in \mathbb{Z}^+$ and 7 is a common divisor of $49, 210$, and 350, then 7 is a positive common divisor of $49, 210$, and 350.

Let $c \in \mathbb{Z}$ such that $c|49$ and $c|210$ and $c|350$.

Then $49 = ck_1$ and $210 = ck_2$ and $350 = ck_3$ for some integers k_1, k_2, and k_3.

Observe that

$$\begin{aligned} 7 &= 49(13) + 210(-3) + 350(0) \\ &= ck_1(13) + ck_2(-3) + ck_3(0) \\ &= c(13k_1) - 3ck_2 + 0 \\ &= c(13k_1) - 3ck_2 \\ &= c(13k_1 - 3k_2). \end{aligned}$$

Since $13k_1 - 3k_2 \in \mathbb{Z}$ and $7 = c(13k_1 - 3k_2)$, then $c|7$, so any common divisor of $49, 210, 350$ divides 7.

Since 7 is a positive common divisor of $49, 210$, and 350, and any common divisor of $49, 210, 350$ divides 7, then $7 = \gcd(49, 210, 350)$, as desired. ☐

Example 86. Prove $\gcd(6, 10, 15) = 1$.

Observe that $\gcd(6, 10) = 2$ and $\gcd(6, 15) = 3$ and $\gcd(10, 15) = 5$, but $\gcd(6, 10, 15) = 1$.

Therefore, three integers can be relatively prime as a triple, even though they are not relatively prime in pairs.

Proof. Since 1 divides every integer, then $1|6$ and $1|10$ and $1|15$, so 1 is a common divisor of $6, 10, 15$.

Since $1 \in \mathbb{Z}^+$ and 1 is a common divisor of $6, 10, 15$, then 1 is a positive common divisor of $6, 10, 15$.

Let $c \in \mathbb{Z}$ such that $c|6$ and $c|10$ and $c|15$.

Then $6 = ck_1$ and $10 = ck_2$ and $15 = ck_3$ for some integers k_1, k_2, and k_3.

Observe that

$$\begin{aligned} 1 &= 6(-14) + 10(7) + 15(1) \\ &= ck_1(-14) + ck_2(7) + ck_3(1) \\ &= c(-14k_1) + 7ck_2 + ck_3 \\ &= c(-14k_1 + 7k_2 + k_3). \end{aligned}$$

Since $-14k_1 + 7k_2 + k_3 \in \mathbb{Z}$ and $1 = c(-14k_1 + 7k_2 + k_3)$, then $c|1$, so any common divisor of $6, 10, 15$ divides 1.

Since 1 is a positive common divisor of $6, 10, 15$, and any common divisor of $6, 10, 15$ divides 1, then $1 = \gcd(6, 10, 15)$, as desired. ☐

Chapter 2.3 Problems

Exercise 87. Compute $\gcd(143, 227)$.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$
\begin{aligned}
227 &= 143 \cdot 1 + 84 \\
143 &= 84 \cdot 1 + 59 \\
84 &= 59 \cdot 1 + 25 \\
59 &= 25 \cdot 2 + 9 \\
25 &= 9 \cdot 2 + 7 \\
9 &= 7 \cdot 1 + 2 \\
7 &= 2 \cdot 3 + 1 \\
2 &= 1 \cdot 2 + 0.
\end{aligned}
$$

Observe that

$$
\begin{aligned}
\gcd(143, 227) &= \gcd(227, 143) \\
&= \gcd(143, 84) \\
&= \gcd(84, 59) \\
&= \gcd(59, 25) \\
&= \gcd(25, 9) \\
&= \gcd(9, 7) \\
&= \gcd(7, 2) \\
&= \gcd(2, 1) \\
&= 1.
\end{aligned}
$$

Therefore, $\gcd(143, 227) = 1$. □

Exercise 88. Compute $\gcd(306, 657)$.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$
\begin{aligned}
657 &= 306 \cdot 2 + 7 \\
306 &= 45 \cdot 6 + 36 \\
45 &= 36 \cdot 1 + 9 \\
36 &= 9 \cdot 4 + 0.
\end{aligned}
$$

Observe that

$$
\begin{aligned}
\gcd(306, 657) &= \gcd(657, 306) \\
&= \gcd(306, 45) \\
&= \gcd(45, 36) \\
&= \gcd(36, 9) \\
&= 9.
\end{aligned}
$$

Therefore, $\gcd(306, 657) = 9$. □

Exercise 89. Compute $\gcd(272, 1479)$.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$\begin{aligned}
1479 &= 272 \cdot 5 + 119 \\
272 &= 119 \cdot 2 + 34 \\
119 &= 34 \cdot 3 + 17 \\
34 &= 17 \cdot 2 + 0.
\end{aligned}$$

Observe that

$$\begin{aligned}
\gcd(272, 1479) &= \gcd(1479, 272) \\
&= \gcd(272, 119) \\
&= \gcd(119, 34) \\
&= \gcd(34, 17) \\
&= 17.
\end{aligned}$$

Therefore, $\gcd(272, 1479) = 17$. $\square$

Exercise 90. Express $\gcd(56, 72)$ as a linear combination of 56 and 72.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$\begin{aligned}
72 &= 56 \cdot 1 + 16 \\
56 &= 16 \cdot 3 + 8 \\
16 &= 8 \cdot 2 + 0.
\end{aligned}$$

Observe that

$$\begin{aligned}
\gcd(56, 72) &= \gcd(72, 56) \\
&= \gcd(56, 16) \\
&= \gcd(16, 8) \\
&= 8.
\end{aligned}$$

We backtrack through the equations to find the linear combination.

$$\begin{aligned}
8 &= 56 - 16 \cdot 3 \\
&= 56 - (72 - 56 \cdot 1) \cdot 3 \\
&= 56 \cdot 4 - 3 \cdot 72 \\
&= (4)56 + (-3)72.
\end{aligned}$$

Therefore, $\gcd(56, 72) = 8 = (4)56 + (-3)72$. $\square$

Exercise 91. Express $\gcd(24, 138)$ as a linear combination of 24 and 138.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$\begin{aligned} 138 &= 24 \cdot 5 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 + 0. \end{aligned}$$

Observe that

$$\begin{aligned} \gcd(24, 138) &= \gcd(138, 24) \\ &= \gcd(24, 18) \\ &= \gcd(18, 6) \\ &= 6. \end{aligned}$$

We backtrack through the equations to find the linear combination.

$$\begin{aligned} 6 &= 24 - 18 \cdot 1 \\ &= 24 - (138 - 24 \cdot 5) \cdot 1 \\ &= 6 \cdot 24 - 138 \cdot 1 \\ &= (6)24 + (-1)138. \end{aligned}$$

Therefore, $\gcd(24, 138) = 6 = (6)24 + (-1)138$. □

Exercise 92. Express $\gcd(119, 272)$ as a linear combination of 119 and 272.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$\begin{aligned} 272 &= 119 \cdot 2 + 34 \\ 119 &= 34 \cdot 3 + 17 \\ 34 &= 17 \cdot 2 + 0. \end{aligned}$$

Observe that

$$\begin{aligned} \gcd(119, 272) &= \gcd(272, 119) \\ &= \gcd(119, 34) \\ &= \gcd(34, 17) \\ &= 17. \end{aligned}$$

We backtrack through the equations to find the linear combination.

$$\begin{aligned} 17 &= 119 - 34 \cdot 3 \\ &= 119 - (272 - 119 \cdot 2) \cdot 3 \\ &= 7 \cdot 119 - 3 \cdot 272 \\ &= (7)119 + (-3)272. \end{aligned}$$

Therefore, $\gcd(119, 272) = 17 = (7)119 + (-3)272$. $\square$

Exercise 93. Express $\gcd(1769, 2378)$ as a linear combination of 1769 and 2378.

Solution. We use the Euclidean algorithm to obtain the equations below.

$$\begin{aligned}
2378 &= 1769 \cdot 1 + 609 \\
1769 &= 609 \cdot 2 + 551 \\
609 &= 551 \cdot 1 + 58 \\
551 &= 58 \cdot 9 + 29 \\
58 &= 29 \cdot 2 + 0.
\end{aligned}$$

Observe that

$$\begin{aligned}
\gcd(1769, 2378) &= \gcd(2378, 1769) \\
&= \gcd(1769, 609) \\
&= \gcd(609, 551) \\
&= \gcd(551, 58) \\
&= \gcd(58, 29) \\
&= 29.
\end{aligned}$$

We backtrack through the equations to find the linear combination.

$$\begin{aligned}
29 &= 551 - 58 \cdot 9 \\
&= 551 - (609 - 551 \cdot 1) \cdot 9 \\
&= 10 \cdot 551 - 9 \cdot 609 \\
&= 10(1769 - 609 \cdot 2) - 9 \cdot 609 \\
&= 10 \cdot 1769 - 29 \cdot 609 \\
&= 10 \cdot 1769 - 29(2378 - 1769 \cdot 1) \\
&= 39 \cdot 1769 - 29 \cdot 2378 \\
&= (39)1769 + (-29)2378.
\end{aligned}$$

Therefore, $\gcd(1769, 2378) = 29 = (39)1769 + (-29)2378$. $\square$

Proposition 94. *Let $a, b \in \mathbb{Z}$.*
Let d be a positive common divisor of a and b.
Then $d = \gcd(a, b)$ if and only if $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof. We prove if $d = \gcd(a, b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Suppose $d = \gcd(a, b)$.

Then d is the least positive linear combination of a and b.

Since d is a positive common divisor of a and b, then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$, so $a = dr$ and $b = ds$ for some integers r and s.

Thus, $r = \frac{a}{d}$ and $s = \frac{b}{d}$.

Since d is the least positive linear combination of a and b, then $d = xa + yb$ for some integers y and y.

Observe that

$$\begin{aligned} d &= xa + yb \\ &= x(dr) + y(ds) \\ &= xdr + yds \\ &= d(xr + ys). \end{aligned}$$

Since $d \in \mathbb{Z}^+$, then $d > 0$, so $d \neq 0$.

Thus, we divide the equation by d to obtain $1 = xr + ys$.

Since $1 = xr + ys$ and x and y are integers, then 1 is a linear combination of r and s, so $1 = \gcd(r, s)$.

Therefore, $1 = \gcd(r, s) = \gcd(\frac{a}{d}, \frac{b}{d})$, so $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, as desired. $\square$

Proof. Conversely, we prove if $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, then $d = \gcd(a, b)$.

Suppose $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Since d is a positive common divisor of a and b, then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$, so $a = dr$ and $b = ds$ for some integers r and s.

Thus, $r = \frac{a}{d}$ and $s = \frac{b}{d}$.

Hence, $1 = \gcd(\frac{a}{d}, \frac{b}{d}) = \gcd(r, s)$, so $\gcd(r, s) = 1$.

Since $d \in \mathbb{Z}^+$, then $d > 0$, so

$$\begin{aligned} \gcd(a, b) &= \gcd(dr, ds) \\ &= d \cdot \gcd(r, s) \\ &= d \cdot 1 \\ &= d. \end{aligned}$$

Therefore, $\gcd(a, b) = d$, as desired. $\square$

Proof. Conversely, we prove if $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, then $d = \gcd(a, b)$.

Suppose $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Then 1 is a linear combination of $\frac{a}{d}$ and $\frac{b}{d}$, so there exist integers m and n such that $m(\frac{a}{d}) + n(\frac{b}{d}) = 1$.

Since $d \in \mathbb{Z}^+$, then $d > 0$, so we multiply d to obtain $ma + nb = d$.

Since $d = ma + nb$ and m and n are integers, then d is a linear combination of a and b.

Let c be any common divisor of a and b.

Then $c \in \mathbb{Z}$ and c divides any linear combination of a and b, so $c|d$.

Thus, any common divisor of a and b divides d.

Since d is a positive common divisor of a and b, and any common divisor of a and b divides d, then $d = \gcd(a, b)$. $\square$

Exercise 95. Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$.

Then $\gcd(a + b, a - b)$ is 1 or 2.

Proof. Let $d = \gcd(a + b, a - b)$.

Then $d \in \mathbb{Z}^+$ and $d|(a + b)$ and $d|(a - b)$.

We must prove either $d = 1$ or $d = 2$.

Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma+nb = 1$.

Thus, $2ma + 2nb = 2$, so 2 is a linear combination of $2a$ and $2b$.

Since $d|(a + b)$ and $d|(a - b)$, then d divides the sum $(a + b) + (a - b) = 2a$, so $d|2a$.

Since $d|(a+b)$ and $d|(a-b)$, then d divides the difference $(a+b)-(a-b) = 2b$, so $d|2b$.

Since $d|2a$ and $d|2b$, then d divides any linear combination of $2a$ and $2b$, so $d|2$.

Since $d \in \mathbb{Z}^+$ and $d|2$, then either $d = 1$ or $d = 2$, as desired. $\square$

Exercise 96. Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$.

Then $\gcd(2a + b, a + 2b)$ is 1 or 3.

Proof. Let $d = \gcd(2a + b, a + 2b)$.

Then $d \in \mathbb{Z}^+$ and $d|(2a + b)$ and $d|(a + 2b)$.

We must prove either $d = 1$ or $d = 3$.

Since $\gcd(a, b) = 1$, then there exist integers m and n such that $ma+nb = 1$.

Thus, $3ma + 3nb = 3$, so 3 is a linear combination of $3a$ and $3b$.

Since $d|(2a + b)$ and $d|(a + 2b)$, then d divides any linear combination of $2a + b$ and $a + 2b$.

Observe that

$$\begin{aligned} 2(2a + b) - (a + 2b) &= 4a + 2b - a - 2b \\ &= 3a. \end{aligned}$$

Thus, $3a$ is a linear combination of $2a+b$ and $a+2b$, so $d|3a$.

Observe that

$$\begin{aligned} 2(a+2b)-(2a+b) &= 2a+4b-2a-b \\ &= 3b. \end{aligned}$$

Thus, $3b$ is a linear combination of $a+2b$ and $2a+b$, so $d|3b$.

Since $d|3a$ and $d|3b$, then d divides any linear combination of $3a$ and $3b$, so $d|3$.

Since $d \in \mathbb{Z}^+$ and $d|3$, then either $d=1$ or $d=3$, as desired. $\square$

Exercise 97. Let $a, b \in \mathbb{Z}$ such that $\gcd(a,b)=1$.

Then $\gcd(a+b, a^2+b^2)$ is 1 or 2.

Proof. Let $d = \gcd(a+b, a^2+b^2)$.

Then $d \in \mathbb{Z}^+$ and $d|(a+b)$ and $d|(a^2+b^2)$.

We must prove either $d=1$ or $d=2$.

Since $\gcd(a,b)=1$, then there exist integers m and n such that $ma+nb=1$.

Since $d|(a+b)$ and $d|(a^2+b^2)$, then d divides any linear combination of $a+b$ and a^2+b^2.

Observe that

$$\begin{aligned} (a^2+b^2)-(a-b)(a+b) &= a^2+b^2-(a^2-b^2) \\ &= a^2+b^2-a^2+b^2 \\ &= 2b^2. \end{aligned}$$

Hence, $2b^2$ is a linear combination of $a+b$ and a^2+b^2, so $d|2b^2$.

Observe that

$$\begin{aligned} (a+b)^2-(a^2+b^2) &= (a^2+2ab+b^2)-a^2-b^2 \\ &= 2ab. \end{aligned}$$

Hence, $2ab$ is a linear combination of $a+b$ and a^2+b^2, so $d|2ab$.

Observe that

$$\begin{aligned} 2b &= 2b \cdot 1 \\ &= 2b(ma+nb) \\ &= 2bma+2bnb \\ &= 2abm+2b^2n. \end{aligned}$$

Hence, $2b$ is a linear combination of $2ab$ and $2b^2$.

Since $d|2ab$ and $d|2b^2$, then d divides any linear combination of $2ab$ and $2b^2$, so $d|2b$.

Observe that

$$\begin{aligned} 2(a+b)^2-4ab-2b^2 &= 2(a^2+2ab+b^2)-4ab-2b^2 \\ &= 2a^2+4ab+2b^2-4ab-2b^2 \\ &= 2a^2. \end{aligned}$$

Hence, $2a^2$ is a linear combination of $a+b$ and $2ab$ and $2b^2$.

Since $d|(a+b)$ and $d|2ab$ and $d|2b^2$, then d divides any linear combination of $a+b$ and $2ab$ and $2b^2$, so $d|2a^2$.

Observe that

$$\begin{aligned} 2a &= 2a \cdot 1 \\ &= 2a(ma+nb) \\ &= 2ama + 2anb \\ &= 2a^2m + 2abn. \end{aligned}$$

Hence, $2a$ is a linear combination of $2a^2$ and $2ab$.

Since $d|2a^2$ and $d|2ab$, then d divides any linear combination of $2a^2$ and $2ab$, so $d|2a$.

Observe that

$$\begin{aligned} 2 &= 2 \cdot 1 \\ &= 2(ma+nb) \\ &= 2ma + 2nb. \end{aligned}$$

Hence, 2 is a linear combination of $2a$ and $2b$.

Since $d|2a$ and $d|2b$, then d divides any linear combination of $2a$ and $2b$, so $d|2$.

Since $d \in \mathbb{Z}^+$ and $d|2$, then either $d=1$ or $d=2$. $\square$

Exercise 98. Let $a, b \in \mathbb{Z}$ such that $\gcd(a,b)=1$.

Then $\gcd(a+b, a^2-ab+b^2)$ is 1 or 3.

Proof. Let $d = \gcd(a+b, a^2-ab+b^2)$.

Then $d \in \mathbb{Z}^+$ and $d|(a+b)$ and $d|(a^2-ab+b^2)$.

We must prove either $d=1$ or $d=3$.

Since $a^2-ab+b^2 = (a+b)(a-2b)+3b^2$, then $3b^2 = (a^2-ab+b^2)-(a+b)(a-2b)$, so $3b^2$ is a linear combination of a^2-ab+b^2 and $a+b$.

Since $d|(a+b)$ and $d|(a^2-ab+b^2)$, then d divides any linear combination of $a+b$ and a^2-ab+b^2, so $d|3b^2$.

Since $(a+b)^2-(a^2-ab+b^2) = (a^2+2ab+b^2)-a^2+ab-b^2 = 3ab$, then $3ab$ is a linear combination of $a+b$ and a^2-ab+b^2.

Since d divides any linear combination of $a+b$ and a^2-ab+b^2, then $d|3ab$.

Observe that

$$\begin{aligned} 3b &= 3b \cdot 1 \\ &= 3b(ma+nb) \\ &= 3bma + 3bnb \\ &= 3abm + 3b^2n. \end{aligned}$$

Hence, $3b$ is a linear combination of $3ab$ and $3b^2$.

Since $d|3ab$ and $d|3b^2$, then d divides any linear combination of $3ab$ and $3b^2$, so $d|3b$.

Since $2(a^2-ab+b^2)+(a+b)^2-3b^2 = (2a^2-2ab+2b^2)+(a^2+2ab+b^2)-3b^2 = 3a^2$, then $3a^2$ is a linear combination of a^2-ab+b^2 and $a+b$ and $3b^2$.

Since $d|(a^2-ab+b^2)$ and $d|(a+b)$ and $d|3b^2$, then d divides any linear combination of a^2-ab+b^2 and $a+b$ and $3b^2$, so $d|3a^2$.

Observe that

$$\begin{aligned} 3a &= 3a \cdot 1 \\ &= 3a(ma+nb) \\ &= 3ama + 3anb \\ &= 3a^2m + 3abn. \end{aligned}$$

Hence, $3a$ is a linear combination of $3a^2$ and $3ab$.

Since $d|3a^2$ and $d|3ab$, then d divides any linear combination of $3a^2$ and $3ab$, so $d|3a$.

Observe that

$$\begin{aligned} 3 &= 3 \cdot 1 \\ &= 3(ma+nb) \\ &= 3ma + 3nb. \end{aligned}$$

Hence, 3 is a linear combination of $3a$ and $3b$.

Since $d|3a$ and $d|3b$, then d divides any linear combination of $3a$ and $3b$, so $d|3$.

Since $d \in \mathbb{Z}^+$ and $d|3$, then this implies either $d = 1$ or $d = 3$. ☐

Exercise 99. Let $a, b \in \mathbb{Z}^+$.

If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.

Proof. Suppose $\gcd(a, b) = 1$.

Then $\gcd(b, a) = 1$.

By exercise 79, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = \gcd(a, c) = 1$ for all $a, b, c \in \mathbb{Z}$.

Hence, if $\gcd(a, b) = \gcd(a, c) = 1$, then $\gcd(a, bc) = 1$ for all $a, b, c \in \mathbb{Z}$.

Since $\gcd(b, a) = \gcd(b, a) = 1$, then we conclude $\gcd(b, aa) = 1 = \gcd(b, a^2) = \gcd(a^2, b)$.

Since $\gcd(a^2, b) = \gcd(a^2, b) = 1$, then we conclude $\gcd(a^2, bb) = 1 = \gcd(a^2, b^2)$.

Therefore, $\gcd(a^2, b^2) = 1$, as desired. ☐

Lemma 100. *Let* $a, b \in \mathbb{Z}^+$.

If $\gcd(a, b) = 1$*, then* $\gcd(a, b^n) = 1$ *for all* $n \in \mathbb{Z}^+$.

Proof. Suppose $\gcd(a, b) = 1$.

To prove $\gcd(a, b^n) = 1$ for all $n \in \mathbb{Z}^+$, let $p(n)$ be the predicate $\gcd(a, b^n) = 1$ defined over $\mathbb{Z}^+$.

We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Let $n = 1$.
Since $\gcd(a, b^1) = \gcd(a, b) = 1$, then $p(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then $\gcd(a, b^k) = 1$.
By exercise 79, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = \gcd(a, c) = 1$ for all $a, b, c \in \mathbb{Z}$.
Hence, if $\gcd(a, b) = \gcd(a, c) = 1$, then $\gcd(a, bc) = 1$ for all $a, b, c \in \mathbb{Z}$.
Since $\gcd(a, b^k) = \gcd(a, b) = 1$, then we conclude $\gcd(a, b^k b) = \gcd(a, b^{k+1}) = 1$, so $p(k+1)$ is true.
Thus, $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction, $p(n)$ is true for all $n \in \mathbb{Z}^+$.
Therefore, $\gcd(a, b^n) = 1$ for all $n \in \mathbb{Z}^+$. $\square$

Lemma 101. *Let $a, b \in \mathbb{Z}^+$.*
If $\gcd(a, b) = 1$, then $\gcd(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$.

Proof. Suppose $\gcd(a, b) = 1$.
Then $\gcd(b, a) = 1$.
To prove $\gcd(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$, let $p(n)$ be the predicate $\gcd(a^n, b^n) = 1$ defined over $\mathbb{Z}^+$.
We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Let $n = 1$.
Since $\gcd(a^1, b^1) = \gcd(a, b) = 1$, then $p(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then $\gcd(a^k, b^k) = 1$, so $\gcd(b^k, a^k) = 1$.
By lemma 100, for all $a, b \in \mathbb{Z}^+$, if $\gcd(a, b) = 1$, then $\gcd(a, b^n) = 1$ for all $n \in \mathbb{Z}^+$.
Hence, if $\gcd(b, a) = 1$, then $\gcd(b, a^k) = 1$.
Since $\gcd(b, a) = 1$, then we conclude $\gcd(b, a^k) = 1$.
Thus, $\gcd(a^k, b) = 1$.

By exercise 79, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = \gcd(a, c) = 1$ for all $a, b, c \in \mathbb{Z}$.
Hence, if $\gcd(a, b) = \gcd(a, c) = 1$, then $\gcd(a, bc) = 1$ for all $a, b, c \in \mathbb{Z}$.
Since $\gcd(a^k, b^k) = \gcd(a^k, b) = 1$, then we conclude $\gcd(a^k, b^{k+1}) = \gcd(a^k, b^k b) = 1$, so $\gcd(a^k, b^{k+1}) = 1$.

Since $\gcd(b, a^k) = \gcd(b, a) = 1$, then we conclude $\gcd(b, a^{k+1}) = \gcd(b, a^k a) = 1$, so $\gcd(b, a^{k+1}) = 1$.
Thus, $\gcd(a^{k+1}, b) = 1$.

Since $\gcd(a, b) = 1$, then $\gcd(a, b^k) = 1$.
Thus, $\gcd(b^k, a) = 1$.

Since $\gcd(b^k, a^k) = \gcd(b^k, a) = 1$, then $\gcd(b^k, a^{k+1}) = \gcd(b^k, a^k a) = 1$, so $\gcd(b^k, a^{k+1}) = 1$.
Hence, $\gcd(a^{k+1}, b^k) = 1$.

Since $\gcd(a^{k+1}, b^k) = \gcd(a^{k+1}, b) = 1$, then $\gcd(a^{k+1}, b^{k+1}) = \gcd(a^{k+1}, b^k b) = 1$, so $\gcd(a^{k+1}, b^{k+1}) = 1$.
Thus, $p(k+1)$ is true, so $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction, $p(n)$ is true for all $n \in \mathbb{Z}^+$.
Therefore, $\gcd(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$, as desired. □

Exercise 102. Let $a, b \in \mathbb{Z}^+$.
If $a^n \mid b^n$, then $a \mid b$ for all $n \in \mathbb{Z}^+$.

Proof. Let $n \in \mathbb{Z}^+$.
Suppose $a^n \mid b^n$.
Let $d = \gcd(a, b)$.
Then $d \in \mathbb{Z}^+$ and $d \mid a$ and $d \mid b$, so $a = dr$ and $b = ds$ for some integers r and s.
Thus, $d = \gcd(dr, ds) = d \cdot \gcd(r, s)$.
Since $d > 0$, then we divide to obtain $1 = \gcd(r, s)$.
By lemma 101, for all $a, b \in \mathbb{Z}^+$, if $\gcd(a, b) = 1$, then $\gcd(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$.
Thus, if $\gcd(r, s) = 1$, then $\gcd(r^n, s^n) = 1$ for all $n \in \mathbb{Z}^+$.
Since $\gcd(r, s) = 1$, then we conclude $\gcd(r^n, s^n) = 1$ for all $n \in \mathbb{Z}^+$.
In particular, $\gcd(r^n, s^n) = 1$.
Hence, there exist integers x and y such that $xr^n + ys^n = 1$.
Since $a^n \mid b^n$, then $(dr)^n|(ds)^n$, so $d^n r^n | d^n s^n$.
Since $d \neq 0$, then we have $r^n | s^n$, so $s^n = r^n t$ for some integer t.
Thus, $1 = xr^n + y(r^n t) = r^n(x + yt)$, so $r^n|1$.
Since $d > 0$ and $a > 0$ and $a = dr$, then $r > 0$.
Since $n > 0$, then $r^n > 0$.
Since $r \in \mathbb{Z}$, then $r^n \in \mathbb{Z}$.
Since $r^n \in \mathbb{Z}$ and $r^n > 0$, then $r^n \in \mathbb{Z}^+$.
Since $r^n \in \mathbb{Z}^+$ and $r^n|1$ and the only positive integer that divides 1 is 1, then $r^n = 1$.
Since $r \in \mathbb{Z}^+$ and $n \in \mathbb{Z}^+$ and $r^n = 1$, then we conclude $r = 1$.
Thus, $a = dr = d(1) = d$.

Hence, $\gcd(a, b) = d = a$.

Since $a|b$ iff $\gcd(a, b) = a$, then we conclude $a|b$, as desired. $\square$

Exercise 103. Compute $lcm(143, 227)$.

Solution. By exercise 87, we have $\gcd(143, 227) = 1$.

Hence, 143 and 227 are relatively prime, so the least common multiple of 143 and 227 is the product $143 \cdot 227$.

Therefore, $lcm(143, 227) = 143 \cdot 227 = 32461$. $\square$

Exercise 104. Compute $lcm(306, 657)$.

Solution. By exercise 88, we have $\gcd(306, 657) = 9$.

Observe that

$$\begin{aligned} lcm(306,657) &= \frac{306 \cdot 657}{\gcd(306,657)} \\ &= \frac{306 \cdot 657}{9} \\ &= 22338. \end{aligned}$$

$\square$

Exercise 105. Compute $lcm(272, 1479)$.

Solution. By exercise 89, we have $\gcd(272, 1479) = 17$.

Observe that

$$\begin{aligned} lcm(272,1479) &= \frac{272 \cdot 1479}{\gcd(272,1479)} \\ &= \frac{272 \cdot 1479}{17} \\ &= 23664. \end{aligned}$$

$\square$

Exercise 106. Find integers x, y, z such that $\gcd(198, 288, 512) = 198x+288y+512z$.

Solution. Let $d = \gcd(198, 288)$.

To compute $\gcd(198, 288)$ we use the Euclidean algorithm.

Observe that

$$\begin{aligned} 288 &= 198 \cdot 1 + 90 \\ 198 &= 90 \cdot 2 + 18 \\ 90 &= 18 \cdot 5 + 0. \end{aligned}$$

Thus,

$$\begin{aligned} d &= \gcd(198, 288) \\ &= 18 \\ &= 198 - (90) \cdot 2 \\ &= 198 - (288 - 198 \cdot 1) \cdot 2 \\ &= 198 - 288 \cdot 2 + 198 \cdot 2 \\ &= 3 \cdot 198 + (-2)288. \end{aligned}$$

Since $198x + 288y$ is a linear combination of 198 and 288, then $198x + 288y$ is a multiple of $\gcd(198, 288)$.

Hence, $198x + 288y = du$ for some integer u.

Observe that

$$\begin{aligned} \gcd(198, 288, 512) &= \gcd(\gcd(198, 288), 512) \\ &= \gcd(d, 512) \\ &= \gcd(18, 512). \end{aligned}$$

To compute $\gcd(18, 512)$ we use the Euclidean algorithm.

Observe that

$$\begin{aligned} 512 &= 18 * 28 + 8 \\ 18 &= 8 * 2 + 2 \\ 8 &= 2 * 4 + 0. \end{aligned}$$

Thus,

$$\begin{aligned} \gcd(18, 512) &= 2 \\ &= 18 - (8)2 \\ &= 18 - (512 - 18 * 28)2 \\ &= 18 - 512 * 2 + 18(28 * 2) \\ &= (57)18 + (-2)512. \end{aligned}$$

Hence,

$$\begin{aligned} \gcd(198, 288, 512) &= \gcd(18, 512) \\ &= 2 \\ &= (57)18 + (-2)512 \\ &= 57d + (-2)512 \\ &= 57[3 \cdot 198 + (-2)288] + (-2)512 \\ &= 57 \cdot 3 \cdot 198 + 57(-2)288 + (-2)512 \\ &= (171)198 + (-114)288 + (-2)512. \end{aligned}$$

Therefore, $\gcd(198, 288, 512) = 2 = (171)198 + (-114)288 + (-2)512$, so $x = 171$ and $y = -114$ and $z = -2$. $\square$

Chapter 2.4 The Diophantine Equation $ax + by = c$

Example 107. Find a general solution to the linear Diophantine equation $172x + 20y = 1000$.

Solution. We use the Euclidean algorithm to compute $\gcd(172, 20)$.

Observe that

$$\begin{aligned}
172 &= 20 \cdot 8 + 12 \\
20 &= 12 \cdot 1 + 8 \\
12 &= 8 \cdot 1 + 4 \\
8 &= 4 \cdot 2 + 0.
\end{aligned}$$

Thus, $\gcd(172, 20) = 4$.

Since $\gcd(172, 20) = 4$ and $4|1000$, then a solution exists.

We express the gcd as a linear combination of 172 and 20.

$$\begin{aligned}
4 &= 12 - (8)1 \\
&= 12 - (20 - 12 \cdot 1)1 \\
&= (12) \cdot 2 - 20 \cdot 1 \\
&= (172 - 20 \cdot 8) \cdot 2 - 20 \cdot 1 \\
&= 172 \cdot 2 - 20(17) \\
&= 172 \cdot 2 + 20(-17).
\end{aligned}$$

Thus, $\gcd(172, 20) = 4 = 172 \cdot 2 + 20(-17)$, so $1000 = 250 * 4 = 250(172 * 2 + 20(-17)) = 500 * 172 + 20(-4250)$.

Hence, a particular solution is $x_0 = 500$ and $y_0 = -4250$.

Therefore, a general solution is $x = 500 + (\frac{20}{4})t = 500 + 5t$ and $y = -4250 - (\frac{172}{4})t = -4250 - 43t$ for any integer t.

We can verify the general solution as shown below.

Observe that

$$\begin{aligned}
172x + 20y &= 172(500 + 5t) + 20(-4250 - 43t) \\
&= 172 * 500 + 172 * 5t + 20(-4250) + 20(-43t) \\
&= 86000 + 860t - 85000 - 860t \\
&= 1000.
\end{aligned}$$

□

Example 108. Find a general solution to the linear Diophantine equation $5x + 22y = 18$.

Solution. Since $\gcd(5, 22) = 1$ and $1|18$, then a solution exists.

A particular solution is $x_0 = 8$ and $y_0 = -1$ since $18 = 5(8) + 22(-1)$.

Since $\gcd(5, 22) = 1$, then a general solution is $x = 8 + 22t$ and $y = -1 - 5t$ for arbitrary integer t.

We can verify the general solution as shown below.
Observe that

$$\begin{aligned} 5x + 22y &= 5(8 + 22t) + 22(-1 - 5t) \\ &= 40 + 110t - 22 - 110t \\ &= 40 - 22 \\ &= 18. \end{aligned}$$

$\square$

Example 109. A customer brought a dozen pieces of fruit, apples and oranges, for 1.32.

If an apple costs 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

Solution. Let x be the number of apples bought.
Let y be the number of oranges bought.
Let z be the cost of oranges, in cents.
Then $x(z + 3) + yz = 132$ and $x + y = 12$.
Observe that

$$\begin{aligned} 132 &= x(z + 3) + yz \\ &= xz + 3x + yz \\ &= 3x + xz + yz \\ &= 3x + (x + y)z \\ &= 3x + 12z. \end{aligned}$$

Since $3x + 12z = 132$, then $x + 4z = 44$.

Since $d = \gcd(1, 4) = 1$ and $1|44$, then a solution to the equation $x+4z = 44$ exists, where $a = 1$ and $b = 4$.

We find a linear combination of 1 and 4 for 1, since 44 is a multiple of 1.

Thus, $1 = 1(-3) + 4(1)$, so multiplying by 44, we obtain $44 = (-3)44 + 4(44) = -132 + 4(44) = x + 4z$.

Hence, a particular solution is $x_0 = -132$ and $z_0 = 44$.

The general solution is $x = x_0 + \frac{bt}{d} = x_0 + \frac{bt}{1} = x_0 + bt = -132 + 4t$ and $z = z_0 - \frac{at}{d} = z_0 - \frac{at}{1} = z_0 - at = 44 - t$.

Thus, $x = -132 + 4t$ and $z = 44 - t$.

Since more apples than oranges were bought, then $x > y$.

Since $x + y = 12$ and $x > y$, then $x > 6$ and $x \leq 12$, so $6 < x \leq 12$.

Thus, $6 < -132 + 4t \leq 12$, so $6 < -132 + 4t$ and $-132 + 4t \leq 12$.

Observe that

$$\begin{aligned} 6 < -132 + 4t &\Rightarrow 138 < 4t \\ &\Rightarrow \frac{138}{4} < t \\ &\Rightarrow 34.5 < t. \end{aligned}$$

Thus, $34.5 < t$.
Observe that

$$\begin{aligned} -132 + 4t \leq 12 &\Rightarrow 4t \leq 144 \\ &\Rightarrow t \leq 36. \end{aligned}$$

Thus, $t \leq 36$.
Since $34.5 < t$ and $t \leq 36$, then $34.5 < t \leq 36$.
Since $t \in \mathbb{Z}$ and $34.5 < t \leq 36$, then $t = 35$ or $t = 36$.

If $t = 35$, then $x = -132 + 4t = -132 + 4(35) = -132 + 140 = 8$ and $z = 44 - t = 44 - 35 = 9$ and $y = 12 - x = 12 - 8 = 4$.
If $t = 36$, then $x = -132 + 4t = -132 + 4(36) = 12$ and $z = 44 - t = 44 - 36 = 8$ and $y = 12 - x = 12 - 12 = 0$.

Therefore, either there were 8 apples bought at 12 cents each and 4 oranges bought at 9 cents each, or there were 12 apples bought at 11 cents each. $\square$

Chapter 2.4 Problems

Exercise 110. Find all integer solutions to the equation $56x + 72y = 40$.

Solution. Since $\gcd(56, 72) = \gcd(8 \cdot 7, 8 \cdot 9) = 8 \cdot \gcd(7, 9) = 8 \cdot 1 = 8$ and $8|40$, then the equation has an integer solution.
Since $56x + 72y = 40$, then we divide by 8 to obtain $7x + 9y = 5$.
Since $\gcd(7, 9) = 1$ and $1|5$, then the equation $7x + 9y = 5$ has a solution.
We find 1 as a linear combination of 7 and 9.
Since $7(4) + 9(-3) = 1$, then we multiply by 40 to obtain $40(7)(4) + 40(9)(-3) = 40(1) = 40 = 56x + 72y$, so $56(20) + (72)(-15) = 40$.
Hence, a particular solution to the equation $56x + 72y = 40$ is $x_0 = 20$ and $y_0 = -15$.
Therefore, a general solution is $x = x_0 + \frac{72t}{\gcd(56,72)} = 20 + \frac{72t}{8} = 20 + 9t$ and $y = y_0 - \frac{56t}{\gcd(56,72)} = y_0 - \frac{56t}{8} = -15 - 7t$, so $x = 20 + 9t$ and $y = -15 - 7t$ for some integer t.
We verify the general solution below.
Observe that

$$\begin{aligned} 56x + 72y &= 56(20 + 9t) + 72(-15 - 7t) \\ &= 56 \cdot 20 + 56 \cdot 9t - 72(15) - 72(7t) \\ &= 1120 + 504t - 1080 - 504t \\ &= 40. \end{aligned}$$

$\square$

Exercise 111. Find all integer solutions to the equation $24x + 138y = 18$.

Solution. Since $\gcd(24, 138) = 6$ and $6|18$, then the equation has an integer solution.

Since $24x + 138y = 18$, then we divide by 6 to obtain $4x + 23y = 3$.

Since $\gcd(4, 23) = 1$ and $1|3$, then the equation $4x + 23y = 3$ has a solution.

We find 1 as a linear combination of 4 and 23.

Since $4(6) + 23(-1) = 1$, then we multiply by 18 to obtain $(4)(6)(18) + (23)(-1)(18) = 1(18) = 18 = 24x + 138y$, so $(24)(18) + (138)(-3) = 18 = 24x + 138y$.

Hence, a particular solution to the equation $24x + 138y = 18$ is $x_0 = 18$ and $y_0 = -3$.

Therefore, a general solution is $x = x_0 + \frac{138t}{\gcd(24, 138)} = 18 + \frac{138t}{6} = 18 + 23t$ and $y = y_0 - \frac{24t}{\gcd(24, 138)} = -3 - \frac{24t}{6} = -3 - 4t$, so $x = 18 + 23t$ and $y = -3 - 4t$ for some integer t.

We verify the general solution below.

Observe that

$$\begin{aligned}
24x + 138y &= 24(18 + 23t) + 138(-3 - 4t) \\
&= 24 \cdot 18 + 24 \cdot 23t - 138(3) - 138(4t) \\
&= 432 + 552t - 414 - 552t \\
&= 18.
\end{aligned}$$

$\square$

Exercise 112. Find all integer solutions to the equation $221x + 91y = 117$.

Solution. Since $\gcd(221, 91) = 13$ and $13|117$, then the equation has an integer solution.

Since $221x + 91y = 117$, then we divide by 13 to obtain $17x + 7y = 9$.

Since $\gcd(17, 7) = 1$ and $1|9$, then the equation $17x + 7y = 9$ has a solution.

We find 1 as a linear combination of 17 and 7.

Since $17(-2) + 7(5) = 1$, then we multiply by 117 to obtain $(17)(-2)(117) + (7)(5)(117) = 1(117) = 117 = 221x + 91y$, so $(221)(-18) + (91)(45) = 117 = 221x + 91y$.

Hence, a particular solution to the equation $221x + 91y = 117$ is $x_0 = -18$ and $y_0 = 45$.

Therefore, a general solution is $x = x_0 + \frac{91t}{\gcd(221, 91)} = -18 + \frac{91t}{13} = -18 + 7t$ and $y = y_0 - \frac{221t}{\gcd(221, 91)} = 45 - \frac{221t}{13} = 45 - 17t$, so $x = -18 + 7t$ and $y = 45 - 17t$ for some integer t.

We verify the general solution below.

Observe that

$$\begin{aligned}
221x + 91y &= 221(-18 + 7t) + 91(45 - 17t) \\
&= 221 \cdot (-18) + 221 \cdot 7t + 91(45) - 91 \cdot (17t)) \\
&= -3978 + 1547t + 4095 - 1547t \\
&= 117.
\end{aligned}$$

□

Exercise 113. Find all integer solutions to the equation $84x - 438y = 156$.

Solution. Since $\gcd(84, -438) = 6$ and $6|156$, then the equation has an integer solution.

Since $84x - 438y = 156$, then we divide by 6 to obtain $14x - 73y = 26$.

Since $\gcd(14, -73) = 1$ and $1|156$, then the equation $14x - 73y = 26$ has a solution.

We find 1 as a linear combination of 14 and -73.

Since $14(-26)+(-73)(-5) = 1$, then we multiply by 156 to obtain $(14)(-26)(156)+(-73)(-5)(156) = 1(156) = 156 = 84x - 438y$, so $(84)(-676) - (438)(-130) = 156 = 84x - 438y$.

Hence, a particular solution to the equation $84x - 438y = 156$ is $x_0 = -676$ and $y_0 = -130$.

Therefore, a general solution is $x = x_0 + \frac{-438t}{\gcd(84, -438)} = -676 - \frac{438t}{6} = -676 - 73t$ and $y = y_0 - \frac{84t}{\gcd(84, -438)} = -130 - \frac{84t}{6} = -130 - 14t$, so $x = -676 - 73t$ and $y = -130 - 14t$ for some integer t.

We verify the general solution below.

Observe that

$$\begin{aligned}
84x - 438y &= 84(-676 - 73t) - 438(-130 - 14t) \\
&= 84 \cdot (-676) - 84 \cdot 73t + 438(130) + 438(14t) \\
&= -56784 - 6132t + 56940 + 6132t \\
&= 156.
\end{aligned}$$

□

Exercise 114. Find all positive integer solutions to the equation $30x + 17y = 300$.

Solution. Since $\gcd(30, 17) = 1$ and $1|300$, then the equation has an integer solution.

We find 1 as a linear combination of 30 and 17.

Since $30(4) + 17(-7) = 1$, then we multiply by 300 to obtain $(30)(4)(300) + (17)(-7)(300) = 1(300) = 300 = 30x + 17y$, so $(30)(1200) + (17)(-2100) = 117 = 30x + 17y$.

Hence, a particular solution to the equation $30x + 17y = 300$ is $x_0 = 1200$ and $y_0 = -2100$.

Therefore, a general solution is $x = x_0 + \frac{17t}{\gcd(30,17)} = 1200 + \frac{17t}{1} = 1200 + 17t$ and $y = y_0 - \frac{30t}{\gcd(30,17)} = -2100 - \frac{30t}{1} = -2100 - 30t$, so $x = 1200 + 17t$ and $y = -2100 - 30t$ for some integer t.

We verify the general solution below.

Observe that

$$\begin{aligned} 30x + 17y &= 30(1200 + 17t) + 17(-2100 - 30t) \\ &= 30 \cdot (1200) + 30 \cdot 17t - 17(2100) - 17 \cdot (30t) \\ &= 36000 + 510t - 35700 - 510t \\ &= 300. \end{aligned}$$

A positive solution exists if and only if $x > 0$ and $y > 0$.

Assume $x > 0$.

Observe that

$$\begin{aligned} x > 0 &\Leftrightarrow 1200 + 17t > 0 \\ &\Leftrightarrow 17t > -1200 \\ &\Leftrightarrow t > \frac{-1200}{17}. \end{aligned}$$

Assume $y > 0$.

Observe that

$$\begin{aligned} y > 0 &\Leftrightarrow -2100 - 30t > 0 \\ &\Leftrightarrow -2100 > 30t \\ &\Leftrightarrow -70 > t \\ &\Leftrightarrow t < -70. \end{aligned}$$

Thus, $\frac{-1200}{17} < t$ and $t < -70$, so $\frac{-1200}{17} < t < -70$.

Since $t \in \mathbb{Z}$ and $\frac{-1200}{17} < t < -70$, then $-70 \leq t$ and $t < -70$, a contradiction.

Therefore, x and y cannot be greater than zero, so there are no positive integer solutions. $\square$

Exercise 115. Find all positive integer solutions to the equation $54x + 21y = 906$.

Solution. Since $\gcd(54, 21) = \gcd(3 \cdot 18, 3 \cdot 7) = 3 \cdot \gcd(18, 7) = 3 \cdot 1 = 3$ and $3|906$, then the equation has an integer solution.

Since $54x + 21y = 906$, then we divide by 3 to obtain $18x + 7y = 302$.

Since $\gcd(18,7) = 1$ and $1|302$, then the equation $18x + 7y = 302$ has a solution.

We find 1 as a linear combination of 18 and 7.

Since $18(2) + 7(-5) = 1$, then we multiply by 906 to obtain $(18)(2)(906) + (7)(-5)(906) = 1(906) = 906 = 54x + 21y$, so $(54)(604) + (21)(-1510) = 906 = 54x + 21y$.

Hence, a particular solution to the equation $54x + 21y = 906$ is $x_0 = 604$ and $y_0 = -1510$.

Therefore, a general solution is $x = x_0 + \frac{21t}{\gcd(54,21)} = 604 + \frac{21t}{3} = 604 + 7t$ and $y = y_0 - \frac{54t}{\gcd(54,21)} = -1510 - \frac{54t}{3} = -1510 - 18t$, so $x = 604 + 7t$ and $y = -1510 - 18t$ for some integer t.

We verify the general solution below.

Observe that

$$\begin{aligned} 54x + 21y &= 54(604 + 7t) + 21(-1510 - 18t) \\ &= 54 \cdot (604) + 54 \cdot 7t - 21(1510) - 21 \cdot (18t) \\ &= 32616 + 378t - 31710 - 378t \\ &= 906. \end{aligned}$$

A positive solution exists if and only if $x > 0$ and $y > 0$.

Assume $x > 0$.

Observe that

$$\begin{aligned} x > 0 &\Leftrightarrow 604 + 7t > 0 \\ &\Leftrightarrow 7t > -604 \\ &\Leftrightarrow t > \frac{-604}{7}. \end{aligned}$$

Assume $y > 0$.

Observe that

$$\begin{aligned} y > 0 &\Leftrightarrow -1510 - 18t > 0 \\ &\Leftrightarrow -1510 > 18t \\ &\Leftrightarrow \frac{-1510}{18} > t \\ &\Leftrightarrow \frac{-755}{9} > t. \end{aligned}$$

Thus, $\frac{-604}{7} < t$ and $t < \frac{-755}{9}$, so $\frac{-604}{7} < t < \frac{-755}{9}$.

Since $t \in \mathbb{Z}$ and $\frac{-604}{7} < t < \frac{-755}{9}$, then $-86 \leq t \leq -84$, so either $t = -86$ or $t = -85$ or $t = -84$.

Therefore, the positive solutions are:

$(2, 38), (9, 20), (16, 2)$. $\square$

Exercise 116. Find all positive integer solutions to the equation $123x+360y = 99$.

Solution. Since $\gcd(123, 360) = \gcd(3 \cdot 41, 3 \cdot 120) = 3 \cdot \gcd(41, 120) = 3 \cdot 1 = 3$ and $3|99$, then the equation has an integer solution.

Since $123x + 360y = 99$, then we divide by 3 to obtain $41x + 120y = 33$.

Since $\gcd(41, 120) = 1$ and $1|33$, then the equation $41x + 120y = 33$ has a solution.

We find 1 as a linear combination of 41 and 120.

Since $41(41)+120(-14) = 1$, then we multiply by 99 to obtain $(41)(41)(99)+(120)(-14)(99) = 1(99) = 99 = 123x + 360y$, so $(123)(1353) + (360)(-462) = 99 = 123x + 360y$.

Hence, a particular solution to the equation $123x + 360y = 99$ is $x_0 = 1353$ and $y_0 = -462$.

Therefore, a general solution is $x = x_0 + \frac{360t}{\gcd(123, 360)} = 1353 + \frac{360t}{3} = 1353 + 120t$ and $y = y_0 - \frac{123t}{\gcd(123, 360)} = -462 - \frac{123t}{3} = -462 - 41t$, so $x = 1353 + 120t$ and $y = -462 - 41t$ for some integer t.

We verify the general solution below.

Observe that

$$\begin{aligned} 123x + 360y &= 123(1353 + 120t) + 360(-462 - 41t) \\ &= 123 \cdot 1353 + 123 \cdot 120t - 360 \cdot 462 - 360 \cdot 41t \\ &= 166419 + 14760t - 166320 - 14760t \\ &= 99. \end{aligned}$$

A positive solution exists if and only if $x > 0$ and $y > 0$.

Assume $x > 0$.

Observe that

$$\begin{aligned} x > 0 &\Leftrightarrow 1353 + 120t > 0 \\ &\Leftrightarrow 120t > -1353 \\ &\Leftrightarrow t > \frac{-1353}{120} \\ &\Leftrightarrow t > \frac{-451}{40}. \end{aligned}$$

Assume $y > 0$.

Observe that

$$\begin{aligned} y > 0 &\Leftrightarrow -462 - 41t > 0 \\ &\Leftrightarrow -462 > 41t \\ &\Leftrightarrow \frac{-462}{41} > t \\ &\Leftrightarrow t < \frac{-462}{41}. \end{aligned}$$

Thus, $\frac{-451}{40} < t$ and $t < \frac{-462}{41}$, so $\frac{-451}{40} < t < \frac{-462}{41}$.

Since $t \in \mathbb{Z}$ and $\frac{-451}{40} < t < \frac{-462}{41}$, then there is no integer t that satisfies the inequality $\frac{-451}{40} < t < \frac{-462}{41}$, so no positive solution exists. $\square$

Exercise 117. Find all positive integer solutions to the equation $158x - 57y = 7$.

Solution. Since $\gcd(158, -57) = \gcd(158, 57) = 1$ and $1|7$, then the equation has an integer solution.

A particular solution to the equation $158x - 57y = 7$ is $x_0 = 74$ and $y_0 = 205$.

Therefore, a general solution is $x = x_0 + \frac{-57t}{\gcd(158,-57)} = 74 - \frac{57t}{1} = 74 - 57t$ and $y = y_0 - \frac{158t}{\gcd(158,-57)} = 205 - \frac{158t}{1} = 205 - 158t$, so $x = 74 - 57t$ and $y = 205 - 158t$ for some integer t.

We verify the general solution below.

Observe that

$$\begin{aligned} 158x - 57y &= 158(74 - 57t) - 57(205 - 158t) \\ &= 158 \cdot 74 - 158 \cdot 57t - 57 \cdot 205 + 57 \cdot 158t \\ &= 158 \cdot 74 - 57 \cdot 205 \\ &= 7. \end{aligned}$$

A positive solution exists if and only if $x > 0$ and $y > 0$.

Assume $x > 0$.

Observe that

$$\begin{aligned} x > 0 &\Leftrightarrow 74 - 57t > 0 \\ &\Leftrightarrow 74 > 57t \\ &\Leftrightarrow \frac{74}{57} > t \\ &\Leftrightarrow t < \frac{74}{57}. \end{aligned}$$

Assume $y > 0$.

Observe that

$$\begin{aligned} y > 0 &\Leftrightarrow 205 - 158t > 0 \\ &\Leftrightarrow 205 > 158t \\ &\Leftrightarrow \frac{205}{158} > t \\ &\Leftrightarrow t < \frac{205}{158}. \end{aligned}$$

Thus, $t < \frac{74}{57}$ and $t < \frac{205}{158}$.

Since $t \in \mathbb{Z}$ and $t < \frac{74}{57}$ and $t < \frac{205}{158}$, then $t \leq 1$.

Therefore, the positive integer solutions are: $x = 74 - 57t$ and $y = 205 - 158t$ for any integer $t \leq 1$. $\square$

Exercise 118. Let $a, b \in \mathbb{Z}^+$.

If a and b are relatively prime, then the Diophantine equation $ax - by = 1$ has infinitely many solutions in $\mathbb{Z}^+$.

Proof. Suppose a and b are relatively prime.

Then $\gcd(a, b) = 1$, so there exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$.

Let t be any integer such that $t > \max(\frac{x_0}{-b}, \frac{y_0}{a})$.

Let $x = x_0 + bt$ and $y = -y_0 + at$.

Observe that

$$\begin{aligned} ax - by &= a(x_0 + bt) - b(-y_0 + at) \\ &= ax_0 + abt + by_0 - bat \\ &= ax_0 + abt + by_0 - abt \\ &= ax_0 + by_0 \\ &= 1. \end{aligned}$$

Since $ax - by = 1$, then the general solution to the equation $ax - by = 1$ is the ordered pair of integers $(x_0 + bt, -y_0 + at)$, where t is any integer such that $t > \max(\frac{x_0}{-b}, \frac{y_0}{a})$.

We prove $x > 0$ and $y > 0$.

Either $\max(\frac{x_0}{-b}, \frac{y_0}{a}) = \frac{x_0}{-b}$ or $\max(\frac{x_0}{-b}, \frac{y_0}{a}) = \frac{y_0}{a}$.

We consider these cases separately.

Case 1: Suppose $\max(\frac{x_0}{-b}, \frac{y_0}{a}) = \frac{x_0}{-b}$.

Then $t > \frac{x_0}{-b}$ and $\frac{x_0}{-b} \geq \frac{y_0}{a}$, so $t > \frac{y_0}{a}$.

Since $b > 0$, then $-b < 0$.

Since $t > \frac{x_0}{-b}$ and $-b < 0$, then $-bt < x_0$, so $0 < x_0 + bt$.

Therefore, $0 < x$, so $x > 0$.

Since $t > \frac{y_0}{a}$ and $a > 0$, then $at > y_0$, so $-y_0 + at > 0$.

Therefore, $y > 0$.

Case 2: Suppose $\max(\frac{x_0}{-b}, \frac{y_0}{a}) = \frac{y_0}{a}$.

Then $t > \frac{y_0}{a}$ and $\frac{y_0}{a} \geq \frac{x_0}{-b}$, so $t > \frac{x_0}{-b}$.

Since $b > 0$, then $-b < 0$.

Since $t > \frac{x_0}{-b}$ and $-b < 0$, then $-bt < x_0$, so $0 < x_0 + bt$.

Therefore, $0 < x$, so $x > 0$.

Since $t > \frac{y_0}{a}$ and $a > 0$, then $at > y_0$, so $-y_0 + at > 0$.
Therefore, $y > 0$.

In all cases, we have $x > 0$ and $y > 0$, so $x_0 + bt > 0$ and $-y_0 + at > 0$.
Therefore, the general solution to the equation $ax - by = 1$ is the ordered pair of positive integers $(x_0 + bt, -y_0 + at)$, where t is any integer such that $t > \max(\frac{x_0}{-b}, \frac{y_0}{a})$. $\square$

Exercise 119. Find all solutions in the integers of the equation $15x + 12y + 30z = 24$.

Solution. The linear diophantine equation $15x+12y+30z = 24$ has a solution in the integers iff $\gcd(15, 12, 30)|24$.
Since $\gcd(15, 12, 30) = \gcd(\gcd(15, 12), 30) = \gcd(3, 30) = 3$ and $3|24$, then the equation $15x + 12y + 30z = 24$ has a solution in the integers.
Since $15x + 12y + 30z = 24$, then $15x + 30z = 24 - 12y$.

The linear diophantine equation $15x + 30z = 24 - 12y$ has a solution for a fixed integer y iff $\gcd(15, 30) \mid (24 - 12y)$.
Let $y = 2 - 5s$ for some integer s.
Then $2 - y = 5s$, so $5|(2 - y)$.
Hence, 5 divides any multiple of $2 - y$, so $5|4(2 - y)$.
Thus, $5|8 - 4y$, so $3 \cdot 5|3(8 - 4y)$.
Consequently, $15|(24 - 12y)$.
Since $\gcd(15, 30) = 15$ and $15 \mid (24 - 12y)$, then we conclude the equation $15x + 30z = 24 - 12y$ has a solution for a fixed integer y.
We find a solution to the equation $15x + 30z = 24 - 12y$.

We find $\gcd(15, 30)$ as a linear combination of 15 and 30.
Observe that $\gcd(15, 30) = 15 = 15(1) + 30(0)$.
Hence,

$$\begin{aligned}
15x + 30z &= 24 - 12y \\
&= 24 - 12(2 - 5s) \\
&= 24 - 24 + 60s \\
&= 60s \\
&= 15 \cdot 4s \\
&= \gcd(15, 30) \cdot 4s \\
&= [15(1) + 30(0)] \cdot 4s \\
&= 15(4s) + 30(0).
\end{aligned}$$

Therefore, a particular solution to the equation $15x + 30z = 24 - 12y$ is $x_0 = 4s$ and $z_0 = 0$, so a general solution is $x = 4s + \frac{30t}{15} = 4s + 2t$ and $z = 0 - \frac{15t}{15} = 0 - t = -t$ for any integer t.

Observe that

$$\begin{aligned}15x + 12y + 30z &= 15(4s + 2t) + 12(2 - 5s) + 30(-t)\\ &= 60s + 30t + 24 - 60s - 30t\\ &= 30t + 24 - 30t\\ &= 24.\end{aligned}$$

Therefore, a general solution to the equation $15x + 12y + 30z = 24$ is $x = 4s + 2t$ and $y = 2 - 5s$ and $z = -t$ for any integers s and t. $\square$

Exercise 120. A man has \$4.55 in change composed entirely of dimes and quarters. What are the maximum and minimum number of coins that he can have? Is it possible for the number of dimes to equal the number of quarters?

Solution. Let d be the number of dimes and q be the number of quarters.

Then $10d + 25q = 455$.

Since $10d + 25q = 455$ is a linear Diophantine equation, then an integer solution exists iff $\gcd(10, 25) \mid 455$.

Since $\gcd(10, 25) = 5$ and $5|455$, then the equation has a solution in the integers.

We find a particular solution using the Euclidean algorithm and obtain $\gcd(10, 25)$ as a linear combination.

Observe that

$$\begin{aligned}25 &= 10 \cdot 2 + 5\\ 10 &= 5 \cdot 2 + 0.\end{aligned}$$

Thus, $\gcd(10, 25) = 5 = 25 - (10)2 = 10(-2) + 25(1)$.

Observe that

$$\begin{aligned}10d + 25q &= 455\\ &= 91 \cdot 5\\ &= 91 \cdot \gcd(10, 25)\\ &= 91[10(-2) + 25(1)]\\ &= 10(-182) + 25(91).\end{aligned}$$

Therefore, a particular solution is $d_0 = -182$ and $q_0 = 91$, so a general solution is $d = -182 + (\frac{25}{5})t = -182 + 5t$ and $q = 91 - (\frac{10}{5})t = 91 - 2t$ for any integer t.

Since $d \geq 0$ and $q \geq 0$, then $-182 + 5t \geq 0$ and $91 - 2t \geq 0$.

This leads to $t \geq 36.4$ and $t \leq 45.5$, so $37 \leq t \leq 45$.

We compute the various values of d and q for each t in the integer range $[37, 45]$.

The maximum number of coins is 44 coins, with 43 dimes and 1 quarter.

The minimum number of coins is 20 coins, with 3 dimes and 17 quarters.

There can be an equal number of dimes and quarters, with 13 dimes and 13 quarters. $\square$

Exercise 121. A theatre charges \$1.80 for adult admissions and 75 cents for children.

On a particular evening the total receipts were \$90. Assuming that more adults than children were present, how many people attended?

Solution. Let x be the number of adults and y be the number of children that attended.

Then $180x + 75y = 9000$.

Since $180x + 75y = 9000$ is a linear Diophantine equation, then a solution exists iff $\gcd(180, 75) \mid 9000$.

Since $\gcd(180, 75) = 15$ and $15|9000$, then there is a solution in the integers.

We find a particular solution using the Euclidean algorithm and obtain $\gcd(180, 75)$ as a linear combination.

Observe that

$$\begin{aligned} 180 &= 75 \cdot 2 + 30 \\ 75 &= 30 \cdot 2 + 15 \\ 30 &= 15 \cdot 2 + 0. \end{aligned}$$

Thus,

$$\begin{aligned} \gcd(180, 75) &= 15 \\ &= 75 - (30)2 \\ &= 75 - (180 - 75 \cdot 2)2 \\ &= 75 - 180 \cdot 2 + 75 \cdot 4 \\ &= 75(5) - 180(2) \\ &= 180(-2) + 75(5). \end{aligned}$$

Hence,

$$\begin{aligned} 180x + 75y &= 9000 \\ &= 600 \cdot 15 \\ &= 600 \cdot \gcd(180, 75) \\ &= 600[180(-2) + 75(5)] \\ &= 180(-1200) + 75(3000). \end{aligned}$$

Therefore, a particular solution is $x_0 = -1200$ and $y_0 = 3000$, so a general solution is $x = -1200 + (\frac{75}{15})t = -1200 + 5t$ and $y = 3000 - (\frac{180}{15})t = 3000 - 12t$ for any integer t.

Since $x \geq 0$ and $y \geq 0$, then $-1200 + 5t \geq 0$ and $3000 - 12t \geq 0$.

This leads to $t \geq 240$ and $t \leq 250$, so $240 \leq t \leq 250$.

We compute the various values of x and y for each t in the integer range $[240, 250]$, such as by writing a Sage function to compute the values satisfying the conditions above.

This leads to potential solutions : $(40, 24), (45, 12), (50, 0)$.

There are either 40 adults and 24 children or 45 adults and 12 children or only 50 adults and no children that attended. □

Exercise 122. A certain number of sixes and nines are added to give a sum of 126.

If the number of sixes and nines are interchanged, the new sum is 114.

How many of each were there originally?

Solution. Let x be the original number of sixes and y be the original number of nines.

Then $6x + 9y = 126$ and $6y + 9x = 114$, so $9x + 6y = 114$.

Since $6x + 9y = 126$, then we multiply by 3 to obtain $18x + 27y = 378$.

Since $9x + 6y = 114$, then we multiply by 2 to obtain $18x + 12y = 228$.

We subtract the equations to get $15y = 378 - 228 = 150$, so $y = 10$.

Thus, $6x + 9(10) = 126$, so $6x = 126 - 9(10) = 36$.

Hence, $x = 6$.

Therefore, $x = 6$ and $y = 10$, so there were 6 sixes and 10 nines originally. □

Exercise 123. A farmer purchased one hundred head of livestock for a total cost of 4000.

Prices in dollars were 120 for each calf, 50 for each lamb, and 25 for each piglet.

If the farmer obtained at least one animal of each type, how many did he buy?

Solution. Let x be the number of calves purchased.

Let y be the number of lambs purchased.

Let z be the number of piglets purchased.

Then $120x + 50y + 25z = 4000$ and $x + y + z = 100$ and $x \geq 1$ and $y \geq 1$ and $z \geq 1$.

Since $x+y+z = 100$, then $z = 100-x-y$, so $120x+50y+25(100-x-y) = 4000$.

Observe that

$$\begin{aligned} 4000 &= 120x + 50y + 25(100 - x - y) \\ &= 120x + 50y + 2500 - 25x - 25y \\ &= 95x + 25y + 2500. \end{aligned}$$

Thus, $95x + 25y + 2500 = 4000$, so $95x + 25y = 1500$.

Since $\gcd(95, 25) = 5$ and $5|1500$, then an integer solution exists to the linear diophantine equation $95x + 25y = 1500$

We obtain gcd(95, 25) as a linear combination using the Euclidean algorithm. Observe that

$$\begin{aligned} 95 &= 25 \cdot 3 + 20 \\ 25 &= 20 \cdot 1 + 5 \\ 20 &= 5 \cdot 4 + 0. \end{aligned}$$

Thus,

$$\begin{aligned} \gcd(95, 25) &= 5 \\ &= 25 - 20 \cdot 1 \\ &= 25 - (95 - 25 \cdot 3) \cdot 1 \\ &= -95 + 25 \cdot 4 \\ &= 95(-1) + 25(4). \end{aligned}$$

Observe that

$$\begin{aligned} 95x + 25y &= 1500 \\ &= 300 \cdot 5 \\ &= 300 \cdot \gcd(95, 25) \\ &= 300[95(-1) + 25(4)] \\ &= 95(-300) + 25(1200). \end{aligned}$$

Hence, a particular solution is $x_0 = -300$ and $y_0 = 1200$, so a general solution is $x = -300 + \frac{25t}{5} = -300 + 5t$ and $y = 1200 - \frac{95t}{5} = 1200 - 19t$ for any integer t.

We verify the general solution below.

$$\begin{aligned} 95x + 25y &= 95(-300 + 5t) + 25(1200 - 19t) \\ &= -28500 + 475t + 30000 - 475t \\ &= -28500 + 30000 \\ &= 1500. \end{aligned}$$

Observe that

$$\begin{aligned} z &= 100 - x - y \\ &= 100 - (-300 + 5t) - (1200 - 19t) \\ &= 100 + 300 - 5t - 1200 + 19t \\ &= -800 + 14t. \end{aligned}$$

Since $z \geq 1$, then $-800 + 14t \geq 1$.

Since $y \geq 1$, then $1200 - 19t \geq 1$.

Since $x \geq 1$, then $-300 + 5t \geq 1$.

These inequalities lead to $t \geq \frac{301}{5}$ and $t \leq \frac{1199}{19}$ and $t \geq \frac{801}{14}$.

Since $t \in \mathbb{Z}$, then we have $t \geq 61$ and $t \leq 63$ and $t \geq 58$, so $t \geq 61$ and $t \leq 63$.

Thus, $t \in \mathbb{Z}$ and $61 \leq t \leq 63$, so either $t = 61$ or $t = 62$ or $t = 63$.

If $t = 61$, then $x = 5$ and $y = 41$ and $z = 54$.

If $t = 62$, then $x = 10$ and $y = 22$ and $z = 68$.

If $t = 63$, then $x = 15$ and $y = 3$ and $z = 82$.

The farmer purchased 5 calves, 41 lambs, and 54 piglets, or the farmer purchased 10 calves, 22 lambs, and 68 piglets, or the farmer purchased 15 calves, 3 lambs, and 82 piglets. $\square$

Exercise 124. When Mr. Smith cashed a check at his bank, the teller mistook the number of cents for the number of dollars and vice versa.

Unaware of this, Mr. Smith spent 68 cents and then noticed to his surprise that he had twice the amount of the original check.

Determine the smallest value for which the check could have been written.

Solution. Let x be the original dollar amount of the check.

Let y be the original cents amount of the check.

Then $100y + x - 68 = 2(100x + y)$.

Observe that

$$\begin{aligned}
2(100x + y) &= 100y + x - 68 \\
68 &= 100y + x - 2(100x + y) \\
&= 100y + x - 200x - 2y \\
&= -199x + 98y.
\end{aligned}$$

Thus, $68 = -199x + 98y$, so $-68 = 199x - 98y$.

Since $\gcd(199, -98) = \gcd(199, 98) = 1$ and $1 | -68$, then the linear diophantine equation $199x - 98y = -68$ has an integer solution.

We use the Euclidean algorithm to find $\gcd(199, 98)$ as a linear combination of 199 and 98.

Observe that

$$\begin{aligned}
199 &= 98 \cdot 2 + 3 \\
98 &= 3 \cdot 32 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2 + 0.
\end{aligned}$$

Observe that

$$\begin{aligned}
\gcd(199,98) &= 1\\
&= 3-2\cdot 1\\
&= 3-(98-3\cdot 32)1\\
&= 3-98+3\cdot 32\\
&= 33\cdot 3-98\\
&= 33(199-98\cdot 2)-98\\
&= 33\cdot 199-66\cdot 98-98\\
&= 199(33)-98(67).
\end{aligned}$$

Observe that

$$\begin{aligned}
199x+(-98)y &= 199x-98y\\
&= -68\\
&= 1\cdot(-68)\\
&= \gcd(199,98)\cdot(-68)\\
&= [199(33)-98(67)]\cdot(-68)\\
&= 199(33)(-68)+(-98)(67)(-68)\\
&= 199(-2244)+(-98)(-4556).
\end{aligned}$$

Hence, a particular solution is $x_0 = -2244$ and $y_0 = -4556$, so a general solution is $x = -2244 + \frac{-98t}{1} = -2244 - 98t$ and $y = -4556 - \frac{199t}{1} = -4556 - 199t$.

We verify the general solution.
Observe that

$$\begin{aligned}
199x-98y &= 199(-2244-98t)-98(-4556-199t)\\
&= 199(-2244)-199(98t)+98(4556)+98(199t)\\
&= 199(-2244)+98(4556)\\
&= -68.
\end{aligned}$$

Since the dollars amount is greater than or equal to zero, then $x \geq 0$.
Thus, $-2244-98t \geq 0$, so $t \leq \frac{-2244}{98}$.
Since the cents amount is between zero and 99, then $0 \leq y \leq 99$, so $0 \leq -4556-199t \leq 99$.
Hence, $4556 \leq -199t \leq 4655$, so $\frac{-4556}{199} \geq t \geq \frac{-4655}{199}$.
Thus, $\frac{-4655}{199} \leq t \leq \frac{-2244}{98}$.
Since $\frac{-4655}{199} \leq t \leq \frac{-2244}{98}$ and $t \leq \frac{-2244}{98}$, then $\frac{-4655}{199} \leq t \leq \frac{-2244}{98}$.

Since $t \in \mathbb{Z}$ and $\frac{-4655}{199} \leq t \leq \frac{-2244}{98}$, then $t = -23$.

Hence, $x = -2244 - 98t = -2244 - 98(-23) = 10$ and $y = -4556 - 199t = -4556 - 199(-23) = 21$.

Therefore, the check was written for 10 dollars and 21 cents. ☐

Chapter 3 Primes

Chapter 3.1 The Fundamental Theorem of Arithmetic

Chapter 3.1 Problems

Exercise 125. It is conjectured that there are infinitely many primes of the form $n^2 - 2$ for integer n.

Exhibit 5 such primes.

Solution. If $n = 2$, then $2^2 - 2 = 4 - 2 = 2$ is prime.
If $n = 3$, then $3^2 - 2 = 9 - 2 = 7$ is prime.
If $n = 5$, then $5^2 - 2 = 25 - 2 = 23$ is prime.
If $n = 7$, then $7^2 - 2 = 49 - 2 = 47$ is prime.
If $n = 9$, then $9^2 - 2 = 81 - 2 = 79$ is prime. ☐

Exercise 126. Show that the conjecture is not true:

Every positive integer can be written in the form $p + a^2$, where p is either prime or 1, and integer $a \geq 0$.

Proof. We must prove there exists a positive integer n that cannot be written in the form $p + a^2$, where p is either prime or 1, and integer $a \geq 0$.

Thus, we must prove there exists a positive integer n such that $n \neq p + a^2$, where p is either prime or 1, and integer $a \geq 0$.

Let $n = 25$.

We shall prove $25 \neq p + a^2$, where p is either prime or 1, and integer $a \geq 0$.

Suppose for the sake of contradiction $25 = p + a^2$, where p is either prime or 1, and integer $a \geq 0$.

Suppose $p = 1$.
Then $a^2 = 25 - p = 25 - 1 = 24$, so $a^2 = 24$.
But, 24 is not a perfect square, so there is no integer a such that $a^2 = 24$.
Therefore, $p \neq 1$.

Since p is either prime or 1 and $p \neq 1$, then p must be prime.

Suppose $p = 2$.
Then $a^2 = 25 - p = 25 - 2 = 23$, so $a^2 = 23$.
But, 23 is not a perfect square, so there is no integer a such that $a^2 = 23$.
Therefore, $p \neq 2$.

Suppose $p = 3$.
Then $a^2 = 25 - p = 25 - 3 = 22$, so $a^2 = 22$.
But, 22 is not a perfect square, so there is no integer a such that $a^2 = 22$.
Therefore, $p \neq 3$.

Suppose $p = 5$.
Then $a^2 = 25 - p = 25 - 5 = 20$, so $a^2 = 20$.
But, 20 is not a perfect square, so there is no integer a such that $a^2 = 20$.
Therefore, $p \neq 5$.

Suppose $p = 7$.
Then $a^2 = 25 - p = 25 - 7 = 18$, so $a^2 = 18$.
But, 18 is not a perfect square, so there is no integer a such that $a^2 = 18$.
Therefore, $p \neq 7$.

Suppose $p = 11$.
Then $a^2 = 25 - p = 25 - 11 = 14$, so $a^2 = 14$.
But, 14 is not a perfect square, so there is no integer a such that $a^2 = 14$.
Therefore, $p \neq 11$.

Suppose $p = 13$.
Then $a^2 = 25 - p = 25 - 13 = 12$, so $a^2 = 12$.
But, 12 is not a perfect square, so there is no integer a such that $a^2 = 12$.
Therefore, $p \neq 13$.

Suppose $p = 17$.
Then $a^2 = 25 - p = 25 - 17 = 8$, so $a^2 = 8$.
But, 8 is not a perfect square, so there is no integer a such that $a^2 = 8$.
Therefore, $p \neq 17$.

Suppose $p = 19$.
Then $a^2 = 25 - p = 25 - 19 = 6$, so $a^2 = 6$.
But, 6 is not a perfect square, so there is no integer a such that $a^2 = 6$.
Therefore, $p \neq 19$.

Suppose $p = 23$.
Then $a^2 = 25 - p = 25 - 23 = 2$, so $a^2 = 2$.
But, 2 is not a perfect square, so there is no integer a such that $a^2 = 2$.
Therefore, $p \neq 23$.

Suppose $p > 23$.
Since p is prime and $p > 23$, then $p \geq 29$, so $-p \leq -29$.
Thus, $a^2 = 25 - p \leq 25 - 29 = -4 < 0$, so $a^2 < 0$.
Since $a \geq 0$, then $a^2 \geq 0$.
Thus, we have $a^2 \geq 0$ and $a^2 < 0$, a contradiction.
Hence, p cannot be greater than 23.

Therefore, p cannot be prime.

Since $p \neq 1$ and p cannot be prime, then $25 \neq p + a^2$, as desired. □

Exercise 127. Every prime of the form $3n + 1$ is also of the form $6m + 1$.

Proof. Let p be a prime of the form $3n + 1$ for some integer n.
Then p is prime and $p = 3n + 1$ for some integer n.
To prove p is of the form $6m+1$, we must prove $p = 6m+1$ for some integer m.
Since $n \in \mathbb{Z}$, then either n is even or n is odd.

Suppose n is odd.
Then $3n$ is odd, so $p = 3n + 1$ is even.
Therefore, p is even.
Since p is prime and p is even, then p is an even prime, so $p = 2$.
Hence, $3n = p - 1 = 2 - 1 = 1$, so $3n = 1$.
Therefore, $3|1$.
But, 1 is not a multiple of 3, so n is not odd.

Since either n is even or n is odd, and n is not odd, then n is even.
Hence, $n = 2m$ for some integer m, so $p = 3n + 1 = 3(2m) + 1 = 6m + 1$.
Therefore, $p = 6m + 1$ for some integer m, as desired. □

Lemma 128. *The product of any finite number of integers of the form $3a + 1$ is of the same form.*

Proof. We must prove $(3a_1 + 1)(3a_2 + 1) \cdot \ldots \cdot (3a_n + 1) = 3m + 1$ for some integer m for all $n \in \mathbb{Z}^+$.
Thus, we must prove: for all $n \in \mathbb{Z}^+$, $\prod_{i=1}^{n}(3a_i + 1) = 3m + 1$ for some integer m.
Let $p(n)$ be the predicate defined over $\mathbb{Z}^+$ by '$\prod_{i=1}^{n}(3a_i + 1) = 3m + 1$ for some integer m'.
We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Let $n = 1$.
Then $\prod_{i=1}^{1}(3a_i + 1) = 3a_1 + 1$ for some integer a_1.
Therefore, $p(1)$ is true.

Let $n = 2$.

Then $\prod_{i=1}^{2}(3a_i + 1) = (3a_1 + 1)(3a_2 + 1)$ for some integers a_1 and a_2.

Observe that

$$\begin{aligned}
\prod_{i=1}^{2}(3a_i + 1) &= (3a_1 + 1)(3a_2 + 1) \\
&= 9a_1a_2 + 3a_1 + 3a_2 + 1 \\
&= 3(3a_1a_2 + a_1 + a_2) + 1 \\
&= 3m + 1.
\end{aligned}$$

Hence, $\prod_{i=1}^{2}(3a_i+1) = 3m+1$ for some integer m, where $m = 3a_1a_2+a_1+a_2$.

Therefore, $p(2)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 2$ such that $p(k)$ is true.

Then $\prod_{i=1}^{k}(3a_i + 1) = 3s + 1$ for some integer s.

Observe that

$$\begin{aligned}
\prod_{i=1}^{k+1}(3a_i + 1) &= \prod_{i=1}^{k}(3a_i + 1) \cdot (3a_{k+1} + 1) \\
&= (3s + 1)(3a_{k+1} + 1) \\
&= 9sa_{k+1} + 3s + 3a_{k+1} + 1 \\
&= 3(3sa_{k+1} + s + a_{k+1}) + 1 \\
&= 3t + 1.
\end{aligned}$$

Hence, $\prod_{i=1}^{k+1}(3a_i+1) = 3t+1$ for some integer t, where $t = 3sa_{k+1}+s+a_{k+1}$.

Therefore, $p(k + 1)$ is true.

Thus, $p(k)$ implies $p(k + 1)$ for all $k \in \mathbb{Z}^+$ with $k \geq 2$.

Since $p(1)$ is true and $p(2)$ is true, and $p(k)$ implies $p(k + 1)$ for all $k \in \mathbb{Z}^+$ with $k \geq 2$, then by induction, $p(k)$ is true for all $k \in \mathbb{Z}^+$.

Therefore, for all $n \in \mathbb{Z}^+$, $\prod_{i=1}^{n}(3a_i + 1) = 3m + 1$ for some integer m. $\square$

Exercise 129. Every positive integer of the form $3n + 2$ has a prime factor of this form.

Proof. Suppose for the sake of contradiction not every positive integer of the form $3n + 2$ has a prime factor of this form.

Then there is some positive integer of the form $3n + 2$ that does not have a prime factor of this form.

Let a be a positive integer of the form $3n + 2$ that does not have a prime factor of this form.

Then $a \in \mathbb{Z}^+$ and $a = 3n+2$ for some integer n and a does not have a prime factor of the same form.

Since $a \in \mathbb{Z}^+$, then $a \geq 1$, so either $a > 1$ or $a = 1$.

Suppose $a = 1$.

Then $3n = a - 2 = 1 - 2 = -1$, so -1 is a multiple of 3.

But, -1 is not a multiple of 3, so $a \neq 1$.

Since $a > 1$ or $a = 1$ and $a \neq 1$, then we conclude $a > 1$.

Hence, by the Fundamental Theorem of Arithmetic, a can be represented as a product of one or more primes.

Since $a|a$, then a is a factor of a.

Since a is a factor of a and $a = 3n + 2$ and a does not have a prime factor of the same form as a, then a cannot be prime.

Since a can be represented as a product of one or more primes, and a cannot be prime, then a can be represented as a product of more than one prime.

Thus, $a = p_1 \cdot p_2 \cdot ...p_k$ for primes $p_1, p_2, ..., p_k$.

Let p be an arbitrary prime factor of a.

Then p is prime and $p|a$.

Since $a = 3n + 2$, then by the division algorithm, 2 is the unique remainder when a is divided by 3.

Since the remainder when a is divided by 3 is not zero, then 3 cannot divide a, so $3 \nmid a$.

By the division algorithm, when p is divided by 3, then there are unique integers q and r such that $p = 3q + r$ and $0 \leq r < 3$.

Since $0 \leq r < 3$, then either $r = 0$ or $r = 1$ or $r = 2$.

Hence, either $p = 3q$ or $p = 3q + 1$ or $p = 3q + 2$.

Suppose $p = 3q$.

Then $3|p$.

Since $3|p$ and $p|a$, then $3|a$.

But, this contradicts $3 \nmid a$.

Hence, $p \neq 3q$.

Suppose $p = 3q + 2$.

Since p is a prime factor of a and $p = 3q + 2$, then a has a prime factor of the same form as a.

But, this contradicts the hypothesis that there is no prime factor of a of the same form as a.

Hence, $p \neq 3q + 2$.

Since either $p = 3q$ or $p = 3q + 1$ or $p = 3q + 2$, and $p \neq 3q$ and $p \neq 3q + 2$, then we must conclude $p = 3q + 1$.

Therefore, every prime factor of a is of the form $3q + 1$ for some integer q.

Since $p_1, p_2, ..., p_k$ are all prime factors of a, then $p_1 = 3q_1 + 1$ and $p_2 = 3q_2 + 1$ and ... and $p_k = 3q_k + 1$ for some integers $q_1, q_2, ..., q_k$.

By lemma 128, the product of any finite number of integers of the form $3q+1$ is of the same form.

Therefore, $(3q_1 + 1)(3q_2 + 1) \cdot \ldots \cdot (3q_k + 1) = 3m + 1$ for some integer m.

Observe that

$$\begin{aligned} 3n + 2 &= a \\ &= p_1 \cdot p_2 \cdot \ldots \cdot p_k \\ &= (3q_1 + 1) \cdot (3q_2 + 1) \cdot \ldots \cdot (3q_k + 1) \\ &= 3m + 1. \end{aligned}$$

Thus, $3n + 2 = 3m + 1$ for some integer m, so $3n + 1 = 3m$.

Therefore, $1 = 3m - 3n = 3(m - n)$.

Since $m - n \in \mathbb{Z}$ and $1 = 3(m - n)$, then $3|1$.

But, $3 \not| 1$.

Consequently, there is no positive integer of the form $3n + 2$ that does not have a prime factor of this form.

Therefore, every positive integer of the form $3n + 2$ has a prime factor of this form. $\square$

Exercise 130. The only prime of the form $n^3 - 1$ is 7.

Proof. Since 7 is prime and $7 = 2^3 - 1$, then 7 is a prime of the form $n^3 - 1$ for integer $n = 2$.

We prove there is no prime of the form $n^3 - 1$ other than 7 by contradiction.

Suppose there is some prime of the form $n^3 - 1$ other than 7.

Let p be a prime of the form $n^3 - 1$ other than 7.

Then p is prime and $p = n^3 - 1$ for some integer n and $p \neq 7$.

Since p is prime, then $p > 1$.

Since $p > 1 > 0$, then $n^3 - 1 = p > 0$, so $n^3 - 1 > 0$.

Hence, $n^3 > 1$.

Since $n \in \mathbb{Z}$ and $n^3 > 1$, then $n > 1$, so $n - 1 > 0$.

Since $n - 1 \in \mathbb{Z}$ and $n - 1 > 0$, then $n - 1 \in \mathbb{Z}^+$.

Since $p = n^3 - 1 = (n-1)(n^2+n+1)$ and $n^2+n+1 \in \mathbb{Z}$, then $n-1$ divides p.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $n - 1 \in \mathbb{Z}^+$ and $n - 1$ divides p, then this implies either $n - 1 = 1$ or $n - 1 = p$.

Suppose $n - 1 = 1$.

Then $n = 2$, so $p = n^3 - 1 = 2^3 - 1 = 7$.

But, $p \neq 7$, so $n - 1 \neq 1$.

Since either $n-1=1$ or $n-1=p$, and $n-1\neq 1$, then $n-1=p$.
Observe that

$$\begin{aligned} 0 &= n^3-1-p \\ &= (n-1)(n^2+n+1)-p \\ &= p(n^2+n+1)-p \\ &= p(n^2+n+1-1) \\ &= p(n^2+n) \\ &= pn(n+1). \end{aligned}$$

Thus, $pn(n+1)=0$, so either $p=0$ or $n=0$ or $n+1=0$.
Since p is prime and 0 is not prime, then $p\neq 0$.
Since $n>1$ and $1>0$, then $n>0$, so $n\neq 0$.
Since $p=0$ or $n=0$ or $n+1=0$, and $p\neq 0$ and $n\neq 0$, then $n+1=0$, so $n=-1$.
Since $n>0$ and $0>-1$, then $n>-1$, so $n\neq -1$.
Hence, $n=-1$ and $n\neq -1$, a contradiction.
Therefore, there is no prime of the form n^3-1 other than 7.

Since 7 is a prime of the form n^3-1, and there is no prime of the form n^3-1 other than 7, then 7 is the only prime of the form n^3-1 for some integer n. $\square$

Exercise 131. The only prime p such that $3p+1$ is a perfect square is $p=5$.

Proof. Let p be a prime such that $3p+1$ is a perfect square.
Then p is prime and $3p+1=n^2$ for some $n\in\mathbb{Z}^+$.
Since p is prime, then $p>1$.
Since $3p+1=n^2$, then $3p=n^2-1=(n-1)(n+1)$.
Since 3 is prime and p is prime, then $3p$ is a product of primes.
Since a product of primes is greater than 1, then $3p>1$.
Since $3p\in\mathbb{Z}$ and $3p>1$, then by the fundamental theorem of arithmetic, $3p$ has a unique prime factorization.
Since $3p=(n-1)(n+1)$, then this implies either $3=n-1$ or $3=n+1$.

Suppose $3=n+1$.
Then $n=2$, so $3p=n^2-1=2^2-1=3$.
Hence, $3p=3$, so $p=1$.
But, $p>1$, so $p\neq 1$.
Therefore, $3\neq n+1$.

Since either $3=n-1$ or $3=n+1$, and $3\neq n+1$, then we conclude $3=n-1$, so $n=4$.
Thus, $3p=n^2-1=4^2-1=15$, so $3p=15$.
Therefore, $p=5$.

Hence, if p is a prime such that $3p+1$ is a perfect square, then $p=5$, so if $3p+1$ is a perfect square for prime p, then $p=5$.

Therefore, $3p+1$ is a perfect square for prime p only if $p=5$, so the only prime p such that $3p+1$ is a perfect square is $p=5$. $\square$

Lemma 132. *Let $p \in \mathbb{Z}^+$.*

If p is prime and $p \geq 5$, then either $p = 6k+1$ or $p = 6k+5$ for some integer k.

Proof. Suppose p is prime and $p \geq 5$.

Since $p \geq 5 > 2$, then $p > 2$.

Since p is prime and $p > 2$, then p must be odd, so $2 \not| p$.

Since $p \geq 5 > 3$, then $p > 3$.

We must prove there exists an integer k such that $p = 6k+1$ or $p = 6k+5$.

By the division algorithm, there is a unique integer k such that either $p = 6k$ or $p = 6k+1$ or $p = 6k+2$ or $p = 6k+3$ or $p = 6k+4$ or $p = 6k+5$.

We consider each case separately.

Case 1: Suppose $p = 6k$.

Then $p = 6k = 2 \cdot 3k$, so $2|p$.

Thus, we have $2|p$ and $2 \not| p$, a contradiction.

Therefore, $p \neq 6k$.

Case 2: Suppose $p = 6k+2$.

Then $p = 2(3k+1)$, so $2|p$.

Thus, we have $2|p$ and $2 \not| p$, a contradiction.

Therefore, $p \neq 6k+2$.

Case 3: Suppose $p = 6k+3$.

Then $p = 3(2k+1)$, so $3|p$.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $3|p$, then this implies either $3 = 1$ or $3 = p$.

Since $3 \neq 1$, then this implies $3 = p$.

But, $p > 3$, so $p \neq 3$.

Therefore, we must conclude $p \neq 6k+3$.

Case 4: Suppose $p = 6k+4$.

Then $p = 2(3k+2)$, so $2|p$.

Thus, we have $2|p$ and $2 \not| p$, a contradiction

Therefore, $p \neq 6k+4$.

Since $p \neq 6k$ and $p \neq 6k+2$ and $p \neq 6k+3$ and $p \neq 6k+4$ and either $p = 6k$ or $p = 6k+1$ or $p = 6k+2$ or $p = 6k+3$ or $p = 6k+4$ or $p = 6k+5$, then we must conclude either $p = 6k+1$ or $p = 6k+5$, as desired. $\square$

Exercise 133. Let $p \in \mathbb{Z}^+$.

If p is prime and $p > 3$, then p^2+2 is composite.

Proof. Suppose p is prime and $p > 3$.

By the division algorithm, $p = 3q + r$ for some unique integers q and r with $0 \leq r < 3$, so either $r = 0$ or $r = 1$ or $r = 2$.

Thus, either $p = 3q$ or $p = 3q+1$ or $p = 3q+2$.

Suppose $p = 3q$.
Then $3|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since 3 is positive and $3|p$ and $3 \neq 1$, then this implies $3 = p$.
But, $p > 3$, so $p \neq 3$.
Therefore, we conclude $p \neq 3q$.

Hence, either $p = 3q + 1$ or $p = 3q + 2$.
We consider each case separately.
Case 1: Suppose $p = 3q + 1$.
Observe that

$$\begin{aligned} p^2 + 2 &= (3q + 1)^2 + 2 \\ &= 9q^2 + 6q + 1 + 2 \\ &= 9q^2 + 6q + 3 \\ &= 3(3q^2 + 2q + 1). \end{aligned}$$

Therefore, $3|(p^2 + 2)$.
Case 2: Suppose $p = 3q + 2$.
Observe that

$$\begin{aligned} p^2 + 2 &= (3q + 2)^2 + 2 \\ &= 9q^2 + 12q + 4 + 2 \\ &= 9q^2 + 12q + 6 \\ &= 3(3q^2 + 4q + 2). \end{aligned}$$

Therefore, $3|(p^2 + 2)$.
Hence, in all cases, $3|(p^2 + 2)$.

Since $p > 3$, then $p^2 > 9$, so $p^2 + 2 > 11$.
Since $0 < 1 < 3 < 11$ and $11 < p^2 + 2$, then $0 < 1 < 3 < 11 < p^2 + 2$, so $0 < p^2 + 2$ and $1 < 3 < p^2 + 2$.
Since $p^2 + 2 \in \mathbb{Z}$ and $p^2 + 2 > 0$, then $p^2 + 2 \in \mathbb{Z}^+$.
A composite number has a positive divisor between 1 and itself.
Since $p^2 + 2 \in \mathbb{Z}^+$ and $3 \in \mathbb{Z}^+$ and $3|(p^2 + 2)$ and $1 < 3 < p^2 + 2$, then we conclude $p^2 + 2$ is composite. □

Exercise 134. Let $a, p \in \mathbb{Z}^+$.
If p is prime and $p|a^n$, then $p^n|a^n$ for all $n \in \mathbb{Z}^+$.

Proof. Let $n \in \mathbb{Z}^+$.
Suppose p is prime and $p|a^n$.
By corollary one to Euclid's lemma, if a prime p divides a product of integers, then p divides one of those integers.
Therefore, $p|a$.

Hence, $a = pk$ for some integer k.
Therefore $a^n = (pk)^n = p^n k^n$.
Since $a^n = p^n k^n$ and $k^n \in \mathbb{Z}$, then $p^n | a^n$, as desired. □

Proof. Let $r(n)$ be the predicate : 'if p is prime and $p|a^n$, then $p^n|a^n$' defined over $\mathbb{Z}^+$.
We prove $r(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Let $n = 1$.
Suppose p is prime and $p|a^1$.
Since $p^1 = p$ and $p|a^1$, then $p^1|a^1$.
Therefore, $r(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $r(k)$ is true.
Then $p^k|a^k$ whenever p is prime and $p|a^k$.

Suppose p is prime and $p|a^{k+1}$.
By corollary one to Euclid's lemma, if p is prime and p divides a product of integers, then p divides one of those integers.
Since p is prime and $p|a^{k+1}$, then we conclude $p|a$.
Hence, p divides any multiple of a.
Since $k \in \mathbb{Z}^+$, then $k \geq 1$, so $k - 1 \geq 0$.
Thus, $a^{k-1} \in \mathbb{Z}$.
Since $a^{k-1} \in \mathbb{Z}$, then $a^{k-1} \cdot a$ is a multiple of a.
Hence, p divides $a^{k-1} \cdot a = a^k$, so $p|a^k$.
Since p is prime and $p|a^k$, then $p^k|a^k$, by the induction hypothesis.
Since $p^k|a^k$ and $p|a$, then the product $p^k \cdot p$ divides the product $a^k \cdot a$, so $p^{k+1}|a^{k+1}$.
Thus, $r(k+1)$ is true.
Consequently, $r(k)$ implies $r(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $r(1)$ is true and $r(k)$ implies $r(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction, we conclude $r(n)$ is true for all $n \in \mathbb{Z}^+$.
Therefore, if p is prime and $p|a^n$, then $p^n|a^n$ for all $n \in \mathbb{Z}^+$. □

Exercise 135. Let $a, b, p \in \mathbb{Z}^+$.
If p is prime and $\gcd(a, b) = p$, then $\gcd(a^2, b^2) = p^2$.

Proof. Suppose p is prime and $\gcd(a, b) = p$.
Since p is prime, then $p \in \mathbb{Z}^+$ and $p > 1$.
Since $\gcd(a, b) = p$, then $p \in \mathbb{Z}^+$ and $p|a$ and $p|b$.

Since $p \in \mathbb{Z}^+$ and $a \in \mathbb{Z}^+$ and $p|a$, then $p \leq a$.
Since $a \geq p$ and $p > 1$, then $a > 1$.
Hence, by the fundamental theorem of arithmetic, a has a unique prime power factorization.
Therefore, $a = p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$, where for each $i = 1, 2, ..., r$, each exponent e_i is a positive integer and each p_i is a prime with $p_1 < p_2 < ... < p_r$.
Since $p|a$ and $a = p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$, then p divides the product $p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$.
If a prime p divides a product of primes, then p is one of those primes.
Since p is prime and p divides the product $p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$ of primes, then p is one of the primes $p_1, p_2, ..., p_r$.
Thus, there exists an integer k such that $p = p_k$ and $1 \leq k \leq r$, so $a = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p^{e_k} \cdot ... \cdot p_r^{e_r}$.

Since $p \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $p|b$, then $p \leq b$.
Since $b \geq p$ and $p > 1$, then $b > 1$.
Hence, by the fundamental theorem of arithmetic, b has a unique prime power factorization.
Therefore, $b = q_1^{f_1} q_2^{f_2} \cdot ... \cdot q_s^{f_s}$, where for each $i = 1, 2, ..., s$, each exponent e_i is a positive integer and each q_i is a prime with $q_1 < q_2 < ... < q_s$.
Since $p|b$ and $b = q_1^{f_1} q_2^{f_2} \cdot ... \cdot q_s^{f_s}$, then p divides the product $q_1^{f_1} q_2^{f_2} \cdot ... \cdot q_s^{f_s}$.
If a prime p divides a product of primes, then p is one of those primes.
Since p is prime and p divides the product $q_1^{f_1} q_2^{f_2} \cdot ... \cdot q_s^{f_s}$ of primes, then p is one of the primes $q_1, q_2, ..., q_s$.
Thus, there exists an integer m such that $p = q_m$ and $1 \leq m \leq s$, so $b = q_1^{f_1} \cdot q_2^{f_2} \cdot ... \cdot p^{f_m} \cdot ... \cdot q_s^{f_s}$.

We next prove p is the only common prime factor of a and b.
Suppose for the sake of contradiction p is not the only common prime factor of a and b.
Then there exists some other prime factor of a and b.
Let q be some other prime factor of a and b.
Then q is prime and $q \neq p$ and $q|a$ and $q|b$.
Since q is prime, then $q \in \mathbb{Z}^+$ and $q > 1$.
Since $q|a$ and $q|b$, then q is a common divisor of a and b.
Any common divisor of a and b must divide $\gcd(a, b)$.
Thus, q must divide $\gcd(a, b) = p$, so $q|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since $q \in \mathbb{Z}^+$ and $q|p$, then this implies either $q = 1$ or $q = p$.
Since $q > 1$, then $q \neq 1$, so $q = p$.
But, this contradicts $q \neq p$.
Therefore, p is the only common prime factor of a and b.

Since $\gcd(a, b) = p = p^1$, then $1 = \min(e_k, f_m)$.
Observe that $a^2 = (p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p^{e_k} \cdot ... \cdot p_r^{e_r})^2 = p_1^{2e_1} p_2^{2e_2} \cdot ... \cdot p^{2e_k} \cdot ... \cdot p_r^{2e_r}$.
Observe that $b^2 = (q_1^{f_1} \cdot q_2^{f_2} \cdot ... \cdot p^{f_m} \cdot ... \cdot q_s^{f_s})^2 = q_1^{2f_1} q p_2^{2f_2} \cdot ... \cdot p^{2f_m} \cdot ... \cdot q_s^{2f_s}$.

Since $1 = \min(e_k, f_m)$, then either $e_k = 1$ and $f_m \geq 1$, or $f_m = 1$ and $e_k \geq 1$.

Thus, either $e_k = 1$ and $f_m > 1$, or $e_k = 1$ and $f_m = 1$, or $f_m = 1$ and $e_k > 1$, or $f_m = 1$ and $e_k = 1$.

Therefore, either $e_k = 1$ and $f_m > 1$, or $e_k = 1$ and $f_m = 1$, or $e_k > 1$ and $f_m = 1$.

We consider these cases separately.

Case 1: Suppose $e_k = 1$ and $f_m > 1$.

Since $e_k = 1$, then $2e_k = 2$.

Since $f_m \in \mathbb{Z}^+$ and $f_m > 1$, then $f_m \geq 2$, so $2f_m \geq 4$.

Since $2e_k = 2$ and $2f_m \geq 4$, then $\min(2e_k, 2f_m) = 2$.

Case 2: Suppose $e_k = 1$ and $f_m = 1$.

Then $\min(2e_k, 2f_m) = \min(2 \cdot 1, 2 \cdot 1) = \min(2, 2) = 2$.

Case 3: Suppose $e_k > 1$ and $f_m = 1$.

Since $e_k \in \mathbb{Z}^+$ and $e_k > 1$, then $e_k \geq 2$, so $2e_k \geq 4$.

Since $f_m = 1$, then $2f_m = 2$.

Since $2e_k \geq 4$ and $2f_m = 2$, then $\min(2e_k, 2f_m) = 2$.

Hence, in all cases, $\min(2e_k, 2f_m) = 2$, so 2 is the least power of p in the prime factorization of a^2 and b^2.

Since p is the only common prime factor of a and b, then p is the only common prime factor of a^2 and b^2.

Since p is the only common prime factor of a^2 and b^2, and 2 is the least power of p in the prime factorization of a^2 and b^2, then $\gcd(a^2, b^2) = p^2$, as desired. $\square$

Exercise 136. Let $a, b, p \in \mathbb{Z}^+$.

If p is prime and $\gcd(a, b) = p$, then either $\gcd(a^2, b) = p$ or $\gcd(a^2, b) = p^2$.

Solution. Let's compute some examples.

Observe that $\gcd(6, 9) = 3$ and 3 is prime and $\gcd(6^2, 9) = \gcd(36, 9) = 9 = 3^2$.

Observe that $\gcd(6, 10) = 2$ and 2 is prime and $\gcd(6^2, 10) = 2$.

We conjecture if $\gcd(a, b) = p$ and p is prime, then $\gcd(a^2, b) = p$ or p^2. $\square$

Proof. Suppose p is prime and $\gcd(a, b) = p$.

Since p is prime, then $p > 1$.

Since $\gcd(a, b) = p$, then $p \in \mathbb{Z}^+$ and $p|a$ and $p|b$.

Since $p \in \mathbb{Z}^+$ and $a \in \mathbb{Z}^+$ and $p|a$, then $p \leq a$.

Since $a \geq p$ and $p > 1$, then $a > 1$.

Hence, by the fundamental theorem of arithmetic, a has a unique prime power factorization.

Therefore, $a = p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$, where for each $i = 1, 2, ..., r$, each exponent e_i is a positive integer and each p_i is a prime with $p_1 < p_2 < ... < p_r$.

Since $p|a$ and $a = p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$, then p divides the product $p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$.

If a prime p divides a product of primes, then p is one of those primes.

Since p is prime and p divides the product $p_1^{e_1}p_2^{e_2}\cdot ... \cdot p_r^{e_r}$ of primes, then p is one of the primes $p_1, p_2, ..., p_r$.

Thus, there exists an integer k such that $p = p_k$ and $1 \leq k \leq r$, so $a = p_1^{e_1}\cdot p_2^{e_2}\cdot ... \cdot p^{e_k}\cdot ... \cdot p_r^{e_r}$.

Since $p \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $p|b$, then $p \leq b$.

Since $b \geq p$ and $p > 1$, then $b > 1$.

Hence, by the fundamental theorem of arithmetic, b has a unique prime power factorization.

Therefore, $b = q_1^{f_1}q_2^{f_2}\cdot ... \cdot q_s^{f_s}$, where for each $i = 1, 2, ..., s$, each exponent e_i is a positive integer and each q_i is a prime with $q_1 < q_2 < ... < q_s$.

Since $p|b$ and $b = q_1^{f_1}q_2^{f_2}\cdot ... \cdot q_s^{f_s}$, then p divides the product $q_1^{f_1}q_2^{f_2}\cdot ... \cdot q_s^{f_s}$.

If a prime p divides a product of primes, then p is one of those primes.

Since p is prime and p divides the product $q_1^{f_1}q_2^{f_2}\cdot ... \cdot q_s^{f_s}$ of primes, then p is one of the primes $q_1, q_2, ..., q_s$.

Thus, there exists an integer m such that $p = q_m$ and $1 \leq m \leq s$, so $b = q_1^{f_1}\cdot q_2^{f_2}\cdot ... \cdot p^{f_m}\cdot ... \cdot q_s^{f_s}$.

We next prove p is the only common prime factor of a and b.

Suppose for the sake of contradiction p is not the only common prime factor of a and b.

Then there exists some other prime factor of a and b.

Let q be some other prime factor of a and b.

Then q is prime and $q \neq p$ and $q|a$ and $q|b$.

Since q is prime, then $q \in \mathbb{Z}^+$ and $q > 1$.

Since $q|a$ and $q|b$, then q is a common divisor of a and b.

Any common divisor of a and b must divide $\gcd(a, b)$.

Thus, q must divide $\gcd(a, b) = p$, so $q|p$.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $q \in \mathbb{Z}^+$ and $q|p$, then this implies either $q = 1$ or $q = p$.

Since $q > 1$, then $q \neq 1$, so $q = p$.

But, this contradicts $q \neq p$.

Therefore, p is the only common prime factor of a and b.

Since $\gcd(a, b) = p = p^1$, then $1 = \min(e_k, f_m)$.

Observe that $a^2 = (p_1^{e_1}\cdot p_2^{e_2}\cdot ... \cdot p^{e_k}\cdot ... \cdot p_r^{e_r})^2 = p_1^{2e_1}p_2^{2e_2}\cdot ... \cdot p^{2e_k}\cdot ... \cdot p_r^{2e_r}$.

Since $1 = \min(e_k, f_m)$, then either $e_k = 1$ and $f_m \geq 1$, or $f_m = 1$ and $e_k \geq 1$.

Thus, either $e_k = 1$ and $f_m > 1$, or $e_k = 1$ and $f_m = 1$, or $f_m = 1$ and $e_k > 1$, or $f_m = 1$ and $e_k = 1$.

Therefore, either $e_k = 1$ and $f_m > 1$, or $e_k = 1$ and $f_m = 1$, or $e_k > 1$ and $f_m = 1$.

We consider these cases separately.

Case 1: Suppose $e_k = 1$ and $f_m > 1$.

Since $e_k = 1$, then $2e_k = 2$.

Since $f_m \in \mathbb{Z}^+$ and $f_m > 1$, then $f_m \geq 2$.

Since $2e_k = 2$ and $f_m \geq 2$, then $\min(2e_k, f_m) = 2$.
Case 2: Suppose $e_k = 1$ and $f_m = 1$.
Then $\min(2e_k, f_m) = \min(2 \cdot 1, 1) = \min(2, 1) = 1$.
Case 3: Suppose $e_k > 1$ and $f_m = 1$.
Since $e_k \in \mathbb{Z}^+$ and $e_k > 1$, then $e_k \geq 2$, so $2e_k \geq 4$.
Since $2e_k \geq 4$ and $f_m = 1$, then $\min(2e_k, f_m) = 1$.

Hence, in all cases, either $\min(2e_k, f_m) = 1$ or $\min(2e_k, f_m) = 2$, so either 1 or 2 is the least power of p in the prime factorization of a^2 and b.

Since p is the only common prime factor of a and b, then p is the only common prime factor of a^2 and b.

Since p is the only common prime factor of a^2 and b, and 1 or 2 is the least power of p in the prime factorization of a^2 and b, then $\gcd(a^2, b) = p$ or $\gcd(a^2, b) = p^2$, as desired. ☐

Exercise 137. Let $a, b, p \in \mathbb{Z}^+$.

If p is prime and $\gcd(a, b) = p$, then $\gcd(a^3, b^2) = p^2$ or $\gcd(a^3, b^2) = p^3$.

Solution. Let's compute some examples.

Observe that $\gcd(2, 4) = 2$ and 2 is prime and $\gcd(2^3, 4^2) = \gcd(8, 16) = 8 = 2^3$.

Observe that $\gcd(3, 12) = 3$ and 3 is prime and $\gcd(3^3, 12^2) = \gcd(9, 144) = 9 = 3^2$.

We conjecture if $\gcd(a, b) = p$ and p is prime, then $\gcd(a^3, b^2) = p^2$ or p^3. ☐

Proof. Suppose p is prime and $\gcd(a, b) = p$.
Since p is prime, then $p > 1$.
Since $\gcd(a, b) = p$, then $p \in \mathbb{Z}^+$ and $p|a$ and $p|b$.

Since $p \in \mathbb{Z}^+$ and $a \in \mathbb{Z}^+$ and $p|a$, then $p \leq a$.
Since $a \geq p$ and $p > 1$, then $a > 1$.

Hence, by the fundamental theorem of arithmetic, a has a unique prime power factorization.

Therefore, $a = p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$, where for each $i = 1, 2, ..., r$, each exponent e_i is a positive integer and each p_i is a prime with $p_1 < p_2 < ... < p_r$.

Since $p|a$ and $a = p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$, then p divides the product $p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$.

If a prime p divides a product of primes, then p is one of those primes.

Since p is prime and p divides the product $p_1^{e_1} p_2^{e_2} \cdot ... \cdot p_r^{e_r}$ of primes, then p is one of the primes $p_1, p_2, ..., p_r$.

Thus, there exists an integer k such that $p = p_k$ and $1 \leq k \leq r$, so $a = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p^{e_k} \cdot ... \cdot p_r^{e_r}$.

Since $p \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $p|b$, then $p \leq b$.

Since $b \geq p$ and $p > 1$, then $b > 1$.

Hence, by the fundamental theorem of arithmetic, b has a unique prime power factorization.

Therefore, $b = q_1^{f_1} q_2^{f_2} \cdot ... \cdot q_s^{f_s}$, where for each $i = 1, 2, ..., s$, each exponent e_i is a positive integer and each q_i is a prime with $q_1 < q_2 < ... < q_s$.

Since $p|b$ and $b = q_1^{f_1} q_2^{f_2} \cdot ... \cdot q_s^{f_s}$, then p divides the product $q_1^{f_1} q_2^{f_2} \cdot ... \cdot q_s^{f_s}$.

If a prime p divides a product of primes, then p is one of those primes.

Since p is prime and p divides the product $q_1^{f_1} q_2^{f_2} \cdot ... \cdot q_s^{f_s}$ of primes, then p is one of the primes $q_1, q_2, ..., q_s$.

Thus, there exists an integer m such that $p = q_m$ and $1 \leq m \leq s$, so $b = q_1^{f_1} \cdot q_2^{f_2} \cdot ... \cdot p^{f_m} \cdot ... \cdot q_s^{f_s}$.

We next prove p is the only common prime factor of a and b.

Suppose for the sake of contradiction p is not the only common prime factor of a and b.

Then there exists some other prime factor of a and b.

Let q be some other prime factor of a and b.

Then q is prime and $q \neq p$ and $q|a$ and $q|b$.

Since q is prime, then $q \in \mathbb{Z}^+$ and $q > 1$.

Since $q|a$ and $q|b$, then q is a common divisor of a and b.

Any common divisor of a and b must divide $\gcd(a, b)$.

Thus, q must divide $\gcd(a, b) = p$, so $q|p$.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $q \in \mathbb{Z}^+$ and $q|p$, then this implies either $q = 1$ or $q = p$.

Since $q > 1$, then $q \neq 1$, so $q = p$.

But, this contradicts $q \neq p$.

Therefore, p is the only common prime factor of a and b.

Since $\gcd(a, b) = p = p^1$, then $1 = \min(e_k, f_m)$.

Observe that $a^3 = (p_1^{e_1} p_2^{e_2} \dots p^{e_k} \dots p_r^{e_r})^3 = p_1^{3e_1} p_2^{3e_2} \dots p^{3e_k} \dots p_r^{3e_r}$.

Observe that $b^2 = (q_1^{f_1} q_2^{f_2} \dots p^{f_m} \dots q_s^{f_s})^2 = q_1^{2f_1} q_2^{2f_2} \dots p^{2f_m} \dots q_s^{2f_s}$.

Since $1 = \min(e_k, f_m)$, then either $e_k = 1$ and $f_m \geq 1$, or $f_m = 1$ and $e_k \geq 1$.

Thus, either $e_k = 1$ and $f_m > 1$, or $e_k = 1$ and $f_m = 1$, or $f_m = 1$ and $e_k > 1$, or $f_m = 1$ and $e_k = 1$.

Therefore, either $e_k = 1$ and $f_m > 1$, or $e_k = 1$ and $f_m = 1$, or $e_k > 1$ and $f_m = 1$.

We consider these cases separately.

Case 1: Suppose $e_k = 1$ and $f_m > 1$.

Since $e_k = 1$, then $3e_k = 3$.

Since $f_m \in \mathbb{Z}^+$ and $f_m > 1$, then $f_m \geq 2$, so $2f_m \geq 4$.

Since $3e_k = 3$ and $2f_m \geq 4$, then $\min(3e_k, 2f_m) = 3$.

Case 2: Suppose $e_k = 1$ and $f_m = 1$.

Then $\min(3e_k, 2f_m) = \min(3 \cdot 1, 2 \cdot 1) = \min(3, 2) = 2$.

Case 3: Suppose $e_k > 1$ and $f_m = 1$.

Since $e_k \in \mathbb{Z}^+$ and $e_k > 1$, then $e_k \geq 2$, so $3e_k \geq 6$.
Since $f_m = 1$, then $2f_m = 2$.
Since $3e_k \geq 6$ and $2f_m = 2$, then $\min(3e_k, 2f_m) = 2$.

Hence, in all cases, either $\min(3e_k, 2f_m) = 2$ or $\min(3e_k, 2f_m) = 3$, so either 2 or 3 is the least power of p in the prime factorization of a^3 and b^2.

Since p is the only common prime factor of a and b, then p is the only common prime factor of a^3 and b^2.

Since p is the only common prime factor of a^3 and b^2, and 2 or 3 is the least power of p in the prime factorization of a^3 and b^2, then $\gcd(a^3, b^2) = p^2$ or $\gcd(a^3, b^2) = p^3$, as desired. $\square$

Exercise 138. Let $n \in \mathbb{Z}^+$.

If $n > 1$, then every integer of the form $n^4 + 4$ is composite.

Proof. Suppose $n > 1$.

To prove every integer of the form $n^4 + 4$ is composite, let k be an integer of the form $n^4 + 4$.

Then $k \in \mathbb{Z}$ and $k = n^4 + 4$.

We must prove k is composite.

Observe that

$$\begin{aligned} k &= n^4 + 4 \\ &= (n^2)^2 + 2n^2(2) + 2^2 - 4n^2 \\ &= (n^2 + 2)^2 - 4n^2 \\ &= (n^2 + 2 + 2n)(n^2 + 2 - 2n) \\ &= (n^2 + 2n + 2)(n^2 - 2n + 2). \end{aligned}$$

Therefore, $k = (n^2+2n+2)(n^2-2n+2)$ and $n^2+2n+2 \in \mathbb{Z}$ and $n^2-2n+2 \in \mathbb{Z}$.

Since $k = (n^2 + 2n + 2)(n^2 - 2n + 2)$ and $n^2 - 2n + 2 \in \mathbb{Z}$, then $n^2 + 2n + 2$ divides k.

We first prove $n^2 + 2n + 2 > 1$.

Since $n > 1$, then $n + 1 > n > 1 > 0$, so $n + 1 > 1$ and $n + 1 > 0$ and $n + 1 > n$.

Since $n + 1 > 1$ and $n + 1 > 0$, then $(n + 1)^2 > n + 1$.

Observe that

$$\begin{aligned} n^2 + 2n + 2 &= n^2 + 2n + 1 + 1 \\ &= (n + 1)^2 + 1 \\ &> (n + 1) + 1 \\ &> n + 1 \\ &> n \\ &> 1. \end{aligned}$$

Therefore, $n^2 + 2n + 2 > 1$.

We next prove $n^2 + 2n + 2 < k$.
Since $n > 1$, then $n^2 > 1$ and $n + 1 > 2$, so $n^2(n + 1) > 2$.
Since $n > 1$, then $n - 1 > 0$, so $n^2(n + 1)(n - 1) > 2(n - 1)$.
Observe that

$$\begin{array}{rcl} n^4 - n^2 & = & n^2(n^2 - 1) \\ & = & n^2(n + 1)(n - 1) \\ & > & 2(n - 1) \\ & = & 2n - 2. \end{array}$$

Hence, $n^4 - n^2 > 2n - 2$, so $n^4 > n^2 + 2n - 2$.
Therefore, $n^4 + 4 > n^2 + 2n + 2$, so $k > n^2 + 2n + 2$.

Since $k > n^2 + 2n + 2$ and $n^2 + 2n + 2 > 1$, then $k > n^2 + 2n + 2 > 1$, so $1 < n^2 + 2n + 2 < k$.
A composite number has a positive divisor between 1 and itself.
Since $n^2 + 2n + 2 \in \mathbb{Z}$ and $n^2 + 2n + 2$ divides k and $1 < n^2 + 2n + 2 < k$, then k is composite, as desired. $\square$

Proof. Suppose $n > 1$.
Since $n \in \mathbb{Z}$, then $n^4 + 4 \in \mathbb{Z}$.
Observe that

$$\begin{array}{rcl} n^4 + 4 & = & (n^2)^2 + 2n^2(2) + 2^2 - 4n^2 \\ & = & (n^2 + 2)^2 - 4n^2 \\ & = & (n^2 + 2 + 2n)(n^2 + 2 - 2n) \\ & = & (n^2 + 2n + 2)(n^2 - 2n + 2). \end{array}$$

Therefore, $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$ and $n^2 + 2n + 2 \in \mathbb{Z}$ and $n^2 - 2n + 2 \in \mathbb{Z}$.

Since $n > 1$, then $n^2 > 1$ and $n + 1 > 2$, so $n^2(n + 1) > 2$.
Thus, $n^2(n + 1) - 2 > 0$.
Since $n > 1$, then $n - 1 > 0$.
Since $n - 1 > 0$ and $n^2(n + 1) - 2 > 0$, then $(n - 1)[n^2(n + 1) - 2] > 0$.
Thus, $(n - 1)(n^3 + n^2 - 2) > 0$, so $n^4 - n^2 - 2n + 2 > 0$.
Therefore, $n^4 > n^2 + 2n - 2$, so $n^4 + 4 > n^2 + 2n + 2$.

Since $n > 1$, then $n + 1 > 2$, so $n + 1 > 0$.
Hence, $(n + 1)^2 > 0$, so $n^2 + 2n + 1 > 0$.
Therefore, $n^2 + 2n + 2 > 1$.
Since $n^4 + 4 > n^2 + 2n + 2$ and $n^2 + 2n + 2 > 1$, then $n^4 + 4 > n^2 + 2n + 2 > 1$, so $1 < n^2 + 2n + 2 < n^4 + 4$.

Since $n^2 > 1$, then $n^2 > 0$.

Since $n - 1 > 0$ and $n^2 > 0$, then $n^2(n-1) > 0 > -2$, so $n^2(n-1) > -2$.

Thus, $n^2(n-1) + 2 > 0$.

Since $n > 1$, then $n + 1 > 2 > 0$, so $n + 1 > 0$.

Since $n + 1 > 0$ and $n^2(n-1) + 2 > 0$, then $(n+1)[n^2(n-1) + 2] > 0$, so $(n+1)(n^3 - n^2 + 2) > 0$.

Thus, $n^4 - n^2 + 2n + 2 > 0$, so $n^4 > n^2 - 2n - 2$.

Therefore, $n^4 + 4 > n^2 - 2n + 2$.

Since $n > 1$, then $n - 1 > 0$, so $(n-1)^2 > 0$.

Therefore, $n^2 - 2n + 1 > 0$, so $n^2 - 2n + 2 > 1$.

Since $n^4 + 4 > n^2 - 2n + 2$ and $n^2 - 2n + 2 > 1$, then $n^4 + 4 > n^2 - 2n + 2 > 1$, so $1 < n^2 - 2n + 2 < n^4 + 4$.

A composite number is composed of smaller positive factors.

Since $n^2 + 2n + 2 \in \mathbb{Z}$ and $n^2 - 2n + 2 \in \mathbb{Z}$, and $1 < n^2 + 2n + 2 < n^4 + 4$ and $1 < n^2 - 2n + 2 < n^4 + 4$, and $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$, then the integer $n^4 + 4$ is composite. $\square$

Exercise 139. Let $n \in \mathbb{Z}^+$.

If $n > 4$ and n is composite, then n divides $(n-1)!$.

Proof. Suppose $n > 4$ and n is composite.

Since n is composite, then n is composed of smaller factors, so $n = ab$ for some positive integers a and b with $1 < a < n$ and $1 < b < n$.

Since $(n-1)!$ is the product of the first $n-1$ positive integers, then $(n-1)! = 1 \cdot 2 \cdot \ldots \cdot (n-1) = 2 \cdot ... \cdot (n-1)$.

Let S be the set of factors $2, 3, ..., n-1$ of $(n-1)!$.

Then $S = \{2, 3, ..., n-1\}$, so $S = \{s \in \mathbb{Z}^+ : 2 \leq s \leq n-1\}$.

Since $|S| = n - 2 > 4 - 2 = 2$, then $|S| > 2$, so $|S| \geq 3$.

Hence, $S \neq \emptyset$.

Since a and b are integers, then either $a = b$ or $a \neq b$.

We consider these cases separately.

Case 1: Suppose $a \neq b$.

Then a and b are distinct integers, so the set $\{a, b\}$ contains exactly 2 elements.

Since $a \in \mathbb{Z}$ and $n \in \mathbb{Z}$ and $1 < a < n$, then $2 \leq a \leq n-1$, so $a \in S$.

Since $b \in \mathbb{Z}$ and $n \in \mathbb{Z}$ and $1 < b < n$, then $2 \leq b \leq n-1$, so $b \in S$.

Let T be the set of all elements of S excluding a and b.

Then $T = S - \{a, b\}$ and $T \cup \{a, b\} = S$ and $T \cap \{a, b\} = \emptyset$.

Observe that $|T| = |S| - |\{a, b\}| = (n-2) - 2 = n - 4$.

Since $n > 4$, then $n - 4 > 0$.

Since $n - 4 \in \mathbb{Z}$ and $n - 4 > 0$, then $n - 4 \geq 1$.

Hence, $|T| = n - 4 \geq 1$, so $|T| \geq 1$.

Therefore, T contains at least 1 element, so T is not empty.

Thus, $T \neq \emptyset$.

Since $T \cup \{a, b\} = S$, then if $x \in S$, then either $x \in T$ or $x \in \{a, b\}$, so either $x \in T$ or $x \in \{a, b\}$ for every $x \in S$.

Since $T \neq \emptyset$ and $\{a, b\} \neq \emptyset$ and $T \cap \{a, b\} = \emptyset$, and either $x \in T$ or $x \in \{a, b\}$ for every $x \in S$, then T and $\{a, b\}$ form a partition of S.

Hence, the product of all elements of T with all elements of $\{a, b\}$ is $(n-1)!$.

Therefore, $(n-1)!$ is the product of all elements of T and ab.

Let t be the product of all elements of T.

Then $(n-1)! = t(ab) = tn = nt$ and $t \in \mathbb{Z}$.

Since $(n-1)! = nt$ and $t \in \mathbb{Z}$, then n divides $(n-1)!$.

Case 2: Suppose $a = b$.

Then $n = ab = aa = a^2$.

Since $a \in \mathbb{Z}$ and $n \in \mathbb{Z}$ and $1 < a < n$, then $2 \leq a \leq n-1$, so $a \in S$.

Let A be the set of all elements of S less than or equal to a.

Then $A = \{x \in S : x \leq a\}$.

Let B be the set of all elements of S greater than a.

Then $B = \{x \in S : x > a\}$.

Observe that $S = A \cup B$ and $A \cap B = \emptyset$.

Suppose $x \in A$ and $y \in B$.

Since $A \cap B = \emptyset$, then A and B are disjoint sets, so $x \neq y$.

Since $x \in A$ and $A \subset S$, then $x \in S$, so x is a factor of $(n-1)!$.

Since $y \in B$ and $B \subset S$, then $y \in S$, so y is a factor of $(n-1)!$.

Since $x \neq y$ and x is a factor of $(n-1)!$ and y is a factor of $(n-1)!$, then x and y are distinct factors of $(n-1)!$, so the product xy is a factor of $(n-1)!$.

Therefore, the product xy is a factor of $(n-1)!$ for all $x \in A$ and all $y \in B$.

Let $k = 2a$.

Then $k \in \mathbb{Z}$ and $a|k$.

We prove $k \in B$.

Since $1 < a < n$, then $1 < a$.

Since $a > 1$ and $1 > 0$, then $a > 0$.

Since $2 > 1$ and $a > 0$, then $k = 2a > a$, so $k > a$.

Since $a > 1$ and $a > 1$, then $a + a > 1 + 1$, so $2a > 2$.

Since $k = 2a$ and $2a > 2$, then $k > 2$, so $2 < k$.

Since $n = a^2$ and $n > 4$, then $a^2 > 4$.

Since $a^2 > 4$ and $a > 0$, then $a > 2$.

Since $a > 2$ and $a > 0$, then $n = a^2 > 2a = k$, so $n > k$.

Since $k \in \mathbb{Z}$ and $n \in \mathbb{Z}$ and $k < n$, then $k \leq n-1$.

Since $k \in \mathbb{Z}$ and $2 < k$ and $k \leq n-1$, then $2 < k \leq n-1$, so $k \in S$.

Since $k \in S$ and $k > a$, then $k \in B$.

Since $a \in A$ and $k \in B$, then a and k are distinct factors of $(n-1)!$, so the product ak is a factor of $(n-1)!$.

Hence, $(n-1)! = ak(c)$ for some integer c.

Observe that

$$\begin{aligned}
(n-1)! &= ak(c) \\
&= a(2a)c \\
&= 2a^2c \\
&= 2nc \\
&= n(2c).
\end{aligned}$$

Since $(n-1)! = n(2c)$ and $2c \in \mathbb{Z}$, then n divides $(n-1)!$.

In all cases, we conclude n divides $(n-1)!$, as desired. $\square$

Exercise 140. Let $n \in \mathbb{Z}^+$.

Every integer of the form $8^n + 1$ is composite.

Proof. Since $n \in \mathbb{Z}^+$, then $8^n + 1 \in \mathbb{Z}$ and $n \geq 1$.

Observe that

$$\begin{aligned}
8^n + 1 &= (2^3)^n + 1 \\
&= (2 \cdot 2^2)^n + 1 \\
&= 2^n \cdot 2^{2n} + 1 \\
&= 2^{2n}(2^n + 1) + 1 - 2^{2n} \\
&= 2^{2n}(2^n + 1) - 2^n(2^n + 1) + (2^n + 1) \\
&= (2^n + 1)(2^{2n} - 2^n + 1).
\end{aligned}$$

Therefore, $8^n + 1 = (2^n + 1)(2^{2n} - 2^n + 1)$.

Since $n \geq 1$ and $1 > 0$, then $n > 0$.

Therefore, $2^n > 0$, so $2^n + 1 > 1$.

Since $3 > 1$ and $n > 0$, then $3n > n$, so $2^{3n} > 2^n$.

Since $8^n = 2^{3n}$, then $8^n > 2^n$, so $8^n + 1 > 2^n + 1$.

Since $8^n + 1 > 2^n + 1$ and $2^n + 1 > 1$, then $8^n + 1 > 2^n + 1 > 1$, so $1 < 2^n + 1 < 8^n + 1$.

Since $n > 0$, then $4^n > 2^n$, so $4^n - 2^n > 0$.

Since $4^n - 2^n > 0 > -1$, then $4^n - 2^n > -1$, so $4^n > 2^n - 1$.

Since $2^n > 0$, then $2^n(4^n) > 2^n(2^n - 1)$, so $8^n > 2^{2n} - 2^n$.

Therefore, $8^n + 1 > 2^{2n} - 2^n + 1$.

Since $2 > 1$ and $n > 0$, then $2n > n$, so $2^{2n} > 2^n$.

Therefore, $2^{2n} - 2^n > 0$, so $2^{2n} - 2^n + 1 > 1$.

Since $8^n+1 > 2^{2n}-2^n+1$ and $2^{2n}-2^n+1 > 1$, then $8^n+1 > 2^{2n}-2^n+1 > 1$, so $1 < 2^{2n} - 2^n + 1 < 8^n + 1$.

A composite number is composed of smaller positive factors.

Since $8^n + 1$ is an integer and $2^n + 1$ is an integer and $2^{2n} - 2^n + 1$ is an integer and $1 < 2^n + 1 < 8^n + 1$ and $1 < 2^{2n} - 2^n + 1 < 8^n + 1$ and $8^n + 1 = (2^n + 1)(2^{2n} - 2^n + 1)$, then $8^n + 1$ is composite. □

Exercise 141. Every integer $n > 11$ can be written as the sum of two composite numbers.

Proof. Let n be an integer greater than 11.

Then $n \in \mathbb{Z}$ and $n > 11$, so $n \geq 12$.

To prove n is the sum of two composite numbers, we prove $n = 2a + 3b$ for some composite numbers $2a$ and $3b$.

Thus, we must prove $n = 2a + 3b$ and $2a$ and $3b$ are composite.

Since $n \in \mathbb{Z}$, then either n is even or n is odd.

We consider these cases separately.

Case 1: Suppose n is even.

Then $n = 2m$ for some integer m.

Let $a = m - 3$ and $b = 2$.

Observe that

$$\begin{aligned} 2a + 3b &= 2(m-3) + 3(2) \\ &= 2m - 6 + 6 \\ &= 2m \\ &= n. \end{aligned}$$

Hence, $n = 2a + 3b$.

Since $n = 2m$ and $n \geq 12$, then $2m \geq 12$, so $m \geq 6$.

Thus, $a = m - 3 \geq 6 - 3 = 3 > 1$, so $a > 1$.

Since $b > 2$ and $2 > 1$, then $b > 1$.

Therefore, $n = 2a + 3b$ and $a > 1$ and $b > 1$.

Case 2: Suppose n is odd.

Then $n = 2m + 1$ for some integer m.

Let $a = m - 4$ and $b = 3$.

Observe that

$$\begin{aligned}
2a + 3b &= 2(m-4) + 3(3) \\
&= 2m - 8 + 9 \\
&= 2m + 1 \\
&= n.
\end{aligned}$$

Thus, $n = 2a + 3b$.

Since $n \geq 12$ and $n = 2m+1$, then $2m + 1 \geq 12$, so $2m \geq 11$.
Hence, $m \geq \frac{11}{2} = 5.5$.
Since $m \in \mathbb{Z}$ and $m \geq 5.5$, then $m \geq 6$.
Hence, $a = m - 4 \geq 6 - 4 = 2 > 1$, so $a > 1$.

Since $b = 3$ and $3 > 1$, then $b > 1$.

Therefore, $n = 2a + 3b$ and $a > 1$ and $b > 1$.

Therefore, in all cases, $n = 2a + 3b$ and $a > 1$ and $b > 1$.

We prove $2a$ is composite.
Since $a > 1$ and $1 > 0$, then $a > 0$.
Since $a \in \mathbb{Z}$ and $a > 0$, then $a \in \mathbb{Z}^+$.
Since $2 \in \mathbb{Z}^+$ and $a \in \mathbb{Z}^+$, then $2a \in \mathbb{Z}^+$.
Since $2|2$, then 2 divides any multiple of 2, so $2|2a$.
Since $a > 1$, then $2a > 2$. so $2 < 2a$.
Since $1 < 2$ and $2 < 2a$, then $1 < 2 < 2a$.
Since $2a \in \mathbb{Z}^+$ and $2 \in \mathbb{Z}^+$ and $2|2a$ and $1 < 2 < 2a$, then $2a$ is composite.

We prove $3b$ is composite.
Since $b > 1$ and $1 > 0$, then $b > 0$.
Since $b \in \mathbb{Z}$ and $b > 0$, then $b \in \mathbb{Z}^+$.
Since $3 \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$, then $3b \in \mathbb{Z}^+$.
Since $3|3$, then 3 divides any multiple of 3, so $3|3b$.
Since $b > 1$, then $3b > 3$. so $3 < 3b$.
Since $1 < 3$ and $3 < 3b$, then $1 < 3 < 3b$.
Since $3b \in \mathbb{Z}^+$ and $3 \in \mathbb{Z}^+$ and $3|3b$ and $1 < 3 < 3b$, then $3b$ is composite.

Therefore, $n = 2a + 3b$ and $2a$ and $3b$ are composite, as desired. $\square$

Exercise 142. Compute all prime numbers that divide $50!$.

Solution. Observe that $50! = 1 \cdot 2 \cdot 3 \ldots \cdot 49 \cdot 50 > 1$.

Since $50! \in \mathbb{Z}$ and $50! > 1$, then by the fundamental theorem of arithmetic, $50!$ has a unique prime power factorization.

The prime power factorization is $50! = 2^{47} \cdot 3^{22} \cdot 5^{12} \cdot 7^8 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47$.

Therefore, the set of primes that divide $50!$ is $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$.

$\square$

Exercise 143. Let $p, q \in \mathbb{Z}^+$.

If p and q are primes and $p \geq q > 3$, then $24|(p^2 - q^2)$.

Proof. Suppose p and q are primes and $p \geq q > 3$.

Then p is prime and q is prime and $p \geq q$ and $q > 3$.

To prove $24|(p^2 - q^2)$, we prove

1. $3|(p^2 - q^2)$.
2. $8|(p^2 - q^2)$.

We first prove $3|(p^2 - q^2)$.

We divide p by 3.

By the division algorithm, there are unique integers a and b such that $p = 3a + b$ and $0 \leq b < 3$.

Since $b \in \mathbb{Z}$ and $0 \leq b < 3$, then either $b = 0$ or $b = 1$ or $b = 2$.

Suppose $b = 0$.

Then $p = 3a + b = 3a + 0 = 3a$, so $3|p$.

Since $p \geq q > 3$, then $p > 3$, so $p \neq 3$.

Since p is prime, then the only positive divisors of p are 1 and p, so $1|p$ and $p|p$.

Since $3 \in \mathbb{Z}^+$ and $3|p$ and $3 \neq 1$ and $p|p$, then we must conclude $3 = p$, so $p = 3$.

But, this contradicts $p \neq 3$.

Therefore, $b \neq 0$.

Since either $b = 0$ or $b = 1$ or $b = 2$, and $b \neq 0$, then either $b = 1$ or $b = 2$.

We divide q by 3.

By the division algorithm, there are unique integers c and d such that $q = 3c + d$ and $0 \leq d < 3$.

Since $d \in \mathbb{Z}$ and $0 \leq d < 3$, then either $d = 0$ or $d = 1$ or $d = 2$.

Suppose $d = 0$.

Then $q = 3c + d = 3c + 0 = 3c$, so $3|q$.

Since $q > 3$, then $q \neq 3$.

Since q is prime, then the only positive divisors of q are 1 and q, so $1|q$ and $q|q$.

Since $3 \in \mathbb{Z}^+$ and $3|q$ and $3 \neq 1$ and $q|q$, then we must conclude $3 = q$, so $q = 3$.

But, this contradicts $q \neq 3$.

Therefore, $d \neq 0$.

Since either $d = 0$ or $d = 1$ or $d = 2$, and $d \neq 0$, then either $d = 1$ or $d = 2$.

Observe that

$$\begin{aligned} p^2 - q^2 &= (3a + b)^2 - (3c + d)^2 \\ &= (9a^2 + 6ab + b^2) - (9c^2 + 6cd + d^2) \\ &= 9a^2 + 6ab + b^2 - 9c^2 - 6cd - d^2 \\ &= 9a^2 + 6ab - 9c^2 - 6cd + b^2 - d^2 \\ &= 3(3a^2 + 2ab - 3c^2 - 2cd) + (b^2 - d^2). \end{aligned}$$

Therefore, $p^2 - q^2 = 3(3a^2 + 2ab - 3c^2 - 2cd) + (b^2 - d^2)$.

Since either $b = 1$ or $b = 2$, and either $d = 1$ or $d = 2$, then either $b = 1$ and $d = 1$, or $b = 1$ and $d = 2$, or $b = 2$ and $d = 1$, or $b = 2$ and $d = 2$.

We consider these cases separately.

Case 1: Suppose $b = 1$ and $d = 1$, or $b = 2$ and $d = 2$.

Then $b = 1 = d$ or $b = 2 = d$, so $b = d$ or $b = d$.

Therefore, $b = d$.

Hence, $b^2 - d^2 = b^2 - b^2 = 0$.

Since $3|0$ and $b^2 - d^2 = 0$, then $3|(b^2 - d^2)$.

Case 2: Suppose $b = 1$ and $d = 2$, or $b = 2$ and $d = 1$.

Then $b + d = 1 + 2 = 3$ or $b + d = 2 + 1 = 3$, so either $b + d = 3$ or $b + d = 3$.

Therefore, $b + d = 3$.

Hence, $b^2 - d^2 = (b + d)(b - d) = 3(b - d)$, so $3|(b^2 - d^2)$.

Therefore, in all cases, $3|(b^2 - d^2)$.

Since 3 divides $3(3a^2 + 2ab - 3c^2 - 2cd)$ and 3 divides $b^2 - d^2$, then 3 divides the sum $3(3a^2 + 2ab - 3c^2 - 2cd) + (b^2 - d^2) = p^2 - q^2$.

Therefore, 3 divides $p^2 - q^2$, so $3|(p^2 - q^2)$, as desired. $\square$

Proof. We next prove $8|(p^2 - q^2)$.

Since $p \geq q > 3$ and $3 > 2$, then $p > 2$.

Since $q > 3$ and $3 > 2$, then $q > 2$.

Any prime greater than 2 is odd.

Since p is prime and $p > 2$, then p is odd, so $p = 2m + 1$ for some integer m.

Since q is prime and $q > 2$, then q is odd, so $q = 2n + 1$ for some integer n.

Observe that

$$\begin{aligned}
p^2 - q^2 &= (2m+1)^2 - (2n+1)^2 \\
&= (4m^2+4m+1) - (4n^2+4n+1) \\
&= 4m^2+4m+1-4n^2-4n-1 \\
&= 4m^2+4m-4n^2-4n \\
&= 4m(m+1) - 4n(n+1).
\end{aligned}$$

A product of two consecutive integers is even.

Since m and $m+1$ are consecutive integers, then $m(m+1)$ is even, so $m(m+1) = 2s$ for some integer s.

Since n and $n+1$ are consecutive integers, then $n(n+1)$ is even, so $n(n+1) = 2t$ for some integer t.

Observe that

$$\begin{aligned}
p^2 - q^2 &= 4m(m+1) - 4n(n+1) \\
&= 4(2s) - 4(2t) \\
&= 8s - 8t \\
&= 8(s-t).
\end{aligned}$$

Therefore, $p^2 - q^2 = 8(s-t)$, so $8|(p^2-q^2)$, as desired. □

Proof. Since $3|(p^2-q^2)$ and $8|(p^2-q^2)$, then p^2-q^2 is a common multiple of 3 and 8.

Since $\gcd(3,8) = 1$, then 3 and 8 are relatively prime.

Since p^2-q^2 is a common multiple of 3 and 8, and 3 and 8 are relatively prime, then p^2-q^2 is a multiple of the product $3 \cdot 8 = 24$.

Therefore, $24|(p^2-q^2)$. □

Exercise 144. An unanswered question is whether there are infinitely many primes which are 1 more than a power of 2, such as $5 = 2^2 + 1$.

Find two more of these primes.

Solution. Observe that $2^4 + 1 = 17$ is prime and $2^8 + 1 = 257$ is prime. □

Exercise 145. A more general conjecture is that there exist infinitely many primes of the form $n^2 + 1$; for example, $257 = 16^2 + 1$.

Exhibit five more primes of this type.

Solution. Observe that $4^2 + 1 = 17$ is prime and $10^2 + 1 = 101$ is prime and $14^2 + 1 = 197$ is prime and $20^2 + 1 = 401$ is prime, and $24^2 + 1 = 577$ is prime. □

Exercise 146. Let $p \in \mathbb{Z}^+$.

If p is an odd prime and $p \neq 5$, then either $10|(p^2-1)$ or $10|(p^2+1)$.

Proof. Suppose p is an odd prime and $p \neq 5$.

Then p is odd and p is prime and $p \neq 5$.

Since p is odd, then p^2 is odd, so $p^2 - 1$ is even and $p^2 + 1$ is even.

Hence, $2|(p^2-1)$ and $2|(p^2+1)$.

By the division algorithm, there are unique integers q and r such that $p = 5q + r$ with $0 \leq r < 5$, so either $p = 5q$ or $p = 5q + 1$ or $p = 5q + 2$ or $p = 5q + 3$ or $p = 5q + 4$.

Suppose $p = 5q$.
Then $5|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since $5 \in \mathbb{Z}^+$ and $5|p$ and $5 \neq 1$, then this implies $5 = p$, so $p = 5$.
But, this contradicts the hypothesis $p \neq 5$.
Therefore, $p \neq 5q$.

Thus, either $p = 5q + 1$ or $p = 5q + 2$ or $p = 5q + 3$ or $p = 5q + 4$.
We consider these cases separately.
Case 1: Suppose $p = 5q + 1$.
Then $p^2 - 1 = (5q + 1)^2 - 1 = 25q^2 + 10q + 1 - 1 = 25q^2 + 10q = 5q(5q + 2)$, so $5|(p^2 - 1)$.
Case 2: Suppose $p = 5q + 2$.
Then $p^2 + 1 = (5q + 2)^2 + 1 = 25q^2 + 20q + 4 + 1 = 25q^2 + 20q + 5 = 5(5q^2 + 4q + 1)$, so $5|(p^2 + 1)$.
Case 3: Suppose $p = 5q + 3$.
Then $p^2 + 1 = (5q + 3)^2 + 1 = 25q^2 + 30q + 9 + 1 = 25q^2 + 30q + 10 = 5(5q^2 + 6q + 2)$, so $5|(p^2 + 1)$.
Case 4: Suppose $p = 5q + 4$.
Then $p^2 - 1 = (5q + 4)^2 - 1 = 25q^2 + 40q + 16 - 1 = 25q^2 + 40q + 15 = 5(5q^2 + 8q + 3)$, so $5|(p^2 - 1)$.
Therefore, in all cases, either $5|(p^2 - 1)$ or $5|(p^2 + 1)$.

We consider these cases separately.
Case 1: Suppose $5|(p^2 - 1)$.
Since $2|(p^2 - 1)$ and $5|(p^2 - 1)$, then $p^2 - 1$ is a common multiple of 2 and 5.
Since $\gcd(2, 5) = 1$, then 2 and 5 are relatively prime.
Since $p^2 - 1$ is a common multiple of 2 and 5, and 2 and 5 are relatively prime, then $p^2 - 1$ is a multiple of the product $2 \cdot 5 = 10$.
Therefore, $10|(p^2 - 1)$.
Case 2: Suppose $5|(p^2 + 1)$.
Since $2|(p^2 + 1)$ and $5|(p^2 + 1)$, then $p^2 + 1$ is a common multiple of 2 and 5.
Since $\gcd(2, 5) = 1$, then 2 and 5 are relatively prime.
Since $p^2 + 1$ is a common multiple of 2 and 5, and 2 and 5 are relatively prime, then $p^2 + 1$ is a multiple of the product $2 \cdot 5 = 10$.
Therefore, $10|(p^2 + 1)$.

In all cases, either $10|(p^2 - 1)$ or $10|(p^2 + 1)$, as desired. $\square$

Exercise 147. Another unproven conjecture is that there are an infinitude of primes which are 1 less than a power of 2, such as $3 = 2^2 - 1$.

Find four more of these primes.

Solution. Observe that $2^3 - 1 = 7$ is prime, and $2^5 - 1 = 31$ is prime, and $2^7 - 1 = 127$ is prime, and $2^{13} - 1 = 8191$ is prime. $\square$

Lemma 148. *For all positive integers n, $3|(4^n - 1)$.*

Proof. To prove $3|(4^n - 1)$ for all $n \in \mathbb{Z}^+$, let $p(n)$ be the predicate '$3|(4^n - 1)$' defined over $\mathbb{Z}^+$.

We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.

Basis:

Let $n = 1$.

Then $4^1 - 1 = 3 = 3 \cdot 1$, so $3|(4^1 - 1)$.

Therefore, $p(1)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.

Since $p(k)$ is true, then $3|(4^k - 1)$, so $4^k - 1 = 3a$ for some integer a.

Observe that

$$\begin{aligned}
4^{k+1} - 1 &= 4^k \cdot 4 - 1 \\
&= 4^k(3 + 1) - 1 \\
&= 4^k \cdot 3 + 4^k - 1 \\
&= 4^k \cdot 3 + 3a \\
&= 3(4^k + a).
\end{aligned}$$

Thus, $4^{k+1} - 1 = 3(4^k + a)$.

Since $4^{k+1} - 1 = 3(4^k + a)$ and $4^k + a \in \mathbb{Z}$, then $3|(4^{k+1} - 1)$, so $p(k + 1)$ is true.

Hence, $p(k)$ implies $p(k + 1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true, and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction, $p(k)$ is true for all $k \in \mathbb{Z}^+$.

Therefore, $3|(4^n - 1)$ for all $n \in \mathbb{Z}^+$. $\square$

Exercise 149. Let k be a positive integer.

If $2^k - 1$ is prime, then k is an odd, except when $k = 2$.

Solution. We compute $2^k - 1$ for various values of k.

If $k = 2$, then $2^k - 1 = 3 = 3$ is prime.

If $k = 3$, then $2^k - 1 = 7 = 7$ is prime.

If $k = 4$, then $2^k - 1 = 15 = 3 \cdot 5$ is not prime.

If $k = 5$, then $2^k - 1 = 31 = 31$ is prime.

If $k = 6$, then $2^k - 1 = 63 = 3^2 \cdot 7$ is not prime.

If $k = 7$, then $2^k - 1 = 127$ is prime.

If $k = 8$, then $2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$ is not prime.

If $k = 9$, then $2^k - 1 = 511 = 7 \cdot 73$ is not prime.

If $k = 10$, then $2^k - 1 = 1023 = 3 \cdot 11 \cdot 31$ is not prime.

If $k = 11$, then $2^k - 1 = 2047 = 23 \cdot 89$ is not prime.
If $k = 12$, then $2^k - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$ is not prime.
We make the following observations.
1. If $k = 2$, then $2^k - 1$ is prime and k is even.
2. If $k > 2$ and k is odd, then $2^k - 1$ can be prime or not prime.
3. If $k > 2$ and k is even, then $2^k - 1$ is not prime. $\square$

Proof. We must prove:
1. If $2^k - 1$ is prime and $k = 2$, then k is not odd.
2. If $2^k - 1$ is prime and $k \neq 2$, then k is odd.

We first prove: if $2^k - 1$ is prime and $k = 2$, then k is not odd.
Suppose $2^k - 1$ is prime and $k = 2$.
Then $k = 2$.
Since 2 is even, then 2 is not odd.
Since $k = 2$ and 2 is not odd, then k is not odd, as desired.

We next prove: if $2^k - 1$ is prime and $k \neq 2$, then k is odd.
Suppose $2^k - 1$ is prime and $k \neq 2$.
We must prove k is odd.
Suppose for the sake of contradiction k is not odd.
Then k is even, so $k = 2n$ for some integer n.
Since $k \in \mathbb{Z}^+$ and $2 \in \mathbb{Z}^+$ and $k = 2n$, then $n \in \mathbb{Z}^+$.

Let $p = 2^k - 1$.
Then p is prime.
We divide p by 3.
By the division algorithm, there are unique integers q and r such that $p = 3q + r$ and $0 \leq r < 3$, so either $p = 3q$ or $p = 3q + 1$ or $p = 3q + 2$.
We consider these cases separately.
Case 1: Suppose $p = 3q$.
Then $3|p$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since $3 \in \mathbb{Z}^+$ and $3|p$ and $3 \neq 1$, then $3 = p$.
Hence, $3 = p = 2^k - 1$, so $4 = 2^k$.
Since $2^k = 4$ and $k \in \mathbb{Z}^+$, then $k = 2$.
But, $k \neq 2$, by hypothesis.
Therefore, $p \neq 3q$.
Case 2: Suppose $p = 3q + 1$.
Then $3q + 1 = p = 2^k - 1 = 2^{2n} - 1 = (2^2)^n - 1 = 4^n - 1$, so $3q + 1 = 4^n - 1$.
By the division algorithm, 1 is the unique remainder when $4^n - 1$ is divided by 3.
By lemma 148, $3|(4^n - 1)$ for all $n \in \mathbb{Z}^+$.
Since $n \in \mathbb{Z}^+$, then $3|(4^n - 1)$.
Hence, the remainder is 0 when $4^n - 1$ is divided by 3.

Since the remainder is unique when $4^n - 1$ is divided by 3, then the remainder cannot be both 0 and 1.

Therefore, $p \neq 3q + 1$.

Case 3: Suppose $p = 3q + 2$.

Then $3q + 2 = p = 2^k - 1$, so $3q + 3 = 2^k$.

Hence, $2^k = 3(q + 1)$, so $3|2^k$.

Since $k \in \mathbb{Z}^+$ and 2 is prime, then 2^k is a product of primes.

Since 3 is prime and $3|2^k$ and 2^k is a product of primes, then 3 is one of the primes in 2^k, so $3 = 2$, a contradiction.

Therefore, $p \neq 3q + 2$.

Since either $p = 3q$ or $p = 3q + 1$ or $p = 3q + 2$, and $p \neq 3q$ and $p \neq 3q + 1$ and $p \neq 3q + 2$, then we must conclude k is odd. ☐

Proof. We must prove:

1. If $2^k - 1$ is prime and $k = 2$, then k is not odd.
2. If $2^k - 1$ is prime and $k \neq 2$, then k is odd.

We first prove: if $2^k - 1$ is prime and $k = 2$, then k is not odd.

Suppose $2^k - 1$ is prime and $k = 2$.

Then $k = 2$.

Since 2 is even, then 2 is not odd.

Since $k = 2$ and 2 is not odd, then k is not odd, as desired.

We next prove: if $2^k - 1$ is prime and $k \neq 2$, then k is odd.

Suppose $2^k - 1$ is prime and $k \neq 2$.

Let $p = 2^k - 1$.

Then p is prime.

We must prove k is odd.

Suppose for the sake of contradiction k is not odd.

Then k is even, so $k = 2n$ for some integer n.

Since $k = 2n$ and $k \in \mathbb{Z}^+$ and $2 \in \mathbb{Z}^+$, then $n \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned} p &= 2^k - 1 \\ &= 2^{2n} - 1 \\ &= (2^n)^2 - 1 \\ &= (2^n - 1)(2^n + 1). \end{aligned}$$

Hence, $p = (2^n - 1)(2^n + 1)$.

Since $n \in \mathbb{Z}^+$, then $2^n \in \mathbb{Z}$, so $2^n - 1 \in \mathbb{Z}$ and $2^n + 1 \in \mathbb{Z}$.

Since $k \in \mathbb{Z}^+$, then $k \geq 1$.

Suppose $k = 1$.
Then $p = 2^1 - 1 = 1$, so $p = 1$ is prime.
But, 1 is not prime.
Therefore, $k \neq 1$.

Since $k \geq 1$ and $k \neq 1$, then $k > 1$.
Since $k \in \mathbb{Z}^+$ and $k > 1$ and $k \neq 2$, then $k > 2$.
Since $2n = k$ and $k > 2$, then $2n > 2$, so $n > 1$.

Since $n > 1$, then $2^n > 2$, so $2^n - 1 > 1$.
Since $2^n - 1 > 1$ and $1 > 0$, then $2^n - 1 > 0$.
Since $2^n - 1 \in \mathbb{Z}$ and $2^n - 1 > 0$, then $2^n - 1 \in \mathbb{Z}^+$.
Since $n \in \mathbb{Z}^+$, then $2^n > 0$, so $2^n + 1 > 1$.
Since $2^n + 1 > 1$ and $1 > 0$, then $2^n + 1 > 0$.
Since $2^n + 1 \in \mathbb{Z}$ and $2^n + 1 > 0$, then $2^n + 1 \in \mathbb{Z}^+$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since $p = (2^n - 1)(2^n + 1)$ and $2^n - 1 \in \mathbb{Z}^+$ and $2^n + 1 \in \mathbb{Z}^+$, then one of the factors $2^n - 1$ and $2^n + 1$ must be 1, so either $2^n - 1 = 1$ or $2^n + 1 = 1$.

Suppose $2^n - 1 = 1$.
Then $2^n = 2$.
Since $2^n = 2$ and $n \in \mathbb{Z}^+$, then $n = 1$.
But, $n > 1$, so $n \neq 1$.
Therefore, $2^n - 1 \neq 1$.

Suppose $2^n + 1 = 1$.
Then $2^n = 0$.
Since $n \in \mathbb{Z}^+$ and $2^n = 0$, then 0 is a positive integral power of 2.
But, there is no positive integer n such that $2^n = 0$.
Therefore, $2^n + 1 \neq 1$.

Since either $2^n - 1 = 1$ or $2^n + 1 = 1$, and $2^n - 1 \neq 1$ and $2^n + 1 \neq 1$, then we must conclude k is odd, as desired. $\square$

Proof. We must prove:
1. If $2^k - 1$ is prime and $k = 2$, then k is not odd.
2. If $2^k - 1$ is prime and $k \neq 2$, then k is odd.

We first prove: if $2^k - 1$ is prime and $k = 2$, then k is not odd.
Suppose $2^k - 1$ is prime and $k = 2$.
Then $k = 2$.
Since 2 is even, then 2 is not odd.
Since $k = 2$ and 2 is not odd, then k is not odd, as desired.

We next prove: if $2^k - 1$ is prime and $k \neq 2$, then k is odd.
Let $p = 2^k - 1$.
Then p is prime.
Since $k \in \mathbb{Z}^+$, then $k \geq 1$.

Suppose $k = 1$.
Then $p = 2^1 - 1 = 1$, so $p = 1$ is prime.
But, 1 is not prime.
Therefore, $k \neq 1$.

Since $k \geq 1$ and $k \neq 1$, then $k > 1$.
Since $k \in \mathbb{Z}^+$ and $k > 1$ and $k \neq 2$, then $k > 2$.

We must prove k is odd.
Suppose for the sake of contradiction k is not odd.
Then k is even, so $k = 2n$ for some integer n.
Thus, $p = 2^k - 1 = 2^{2n} - 1 = (2^n)^2 - 1 = (2^n - 1)(2^n + 1)$.
Since $2n = k$ and $k > 2$, then $2n > 2$, so $n > 1$.
Since $n > 1$ and $1 > 0$, then $n > 0$.
Since $n \in \mathbb{Z}$ and $n > 0$, then $n \in \mathbb{Z}^+$.
Since $n \in \mathbb{Z}^+$, then $2^n \in \mathbb{Z}$, so $2^n - 1 \in \mathbb{Z}$ and $2^n + 1 \in \mathbb{Z}$.

Since $n > 0$ and $1 < 2$, then $n < 2n$, so $2^n < 2^{2n}$.
Hence, $2^n - 1 < 2^{2n} - 1$.

Since $n > 1$, then $2^n > 2$, so $2^n - 1 > 1$.
Since $1 < 2^n - 1$ and $2^n - 1 < 2^{2n} - 1$, then $1 < 2^n - 1 < 2^{2n} - 1$.
Therefore, $1 < 2^n - 1 < p$.

Since $2^n > 2$, then $2^n + 2^n > 2^n + 2$.
Hence, $2(2^n) = 2^{n+1} > 2^n + 2$.
Since $2^n > 2$ and $2^n > 0$, then $2^n \cdot 2^n > 2 \cdot 2^n = 2^{n+1} > 2^n + 2$.
Thus, $(2^n)^2 > 2^n + 2$, so $2^{2n} > 2^n + 2$.
Consequently, $2^{2n} - 1 > 2^n + 1$.

Since $n > 0$, then $2^n > 0$, so $2^n + 1 > 1$.
Since $1 < 2^n + 1$ and $2^n + 1 < 2^{2n} - 1$, then $1 < 2^n + 1 < 2^{2n} - 1$.
Therefore, $1 < 2^n + 1 < p$.

Since $2^n - 1 \in \mathbb{Z}$ and $2^n + 1 \in \mathbb{Z}$ and $1 < 2^n - 1 < p$ and $1 < 2^n + 1 < p$ and $p = (2^n - 1)(2^n + 1)$, then p is composite.
But, this contradicts p is prime.
Therefore, k is odd. $\square$

Exercise 150. Compute the prime factorization of the integers:

a. 1234
b. 10140
c. 36000

Solution. For part a, observe that $1234 = 2 \cdot 617$.

For part b, observe that $10140 = 2^2 \cdot 3 \cdot 5 \cdot 13^2$.

For part c, observe that $36000 = 2^5 \cdot 3^2 \cdot 5^3$. $\square$

Exercise 151. Let $S = \{3k + 1 : k \in \mathbb{Z}^+ \vee k = 0\}$.

Let $a \in S$.

Define $a > 1$ to be prime iff a cannot be factored into two smaller integers in S.

Example is 10 and 25 are prime, but $16 = 4 * 4$ and $28 = 4 * 7$ are not prime.

a. Prove any member of S greater than 1 is either prime or a product or primes.

b. Give an example to show that it is possible for an integer in S to be factored into primes in more than one way.

Solution. Since $1 \in S$, but $1 \not> 1$, then 1 does not satisfy the definition of prime in S.

Therefore we exclude consideration of $1 \in S$ being prime or not prime in S.

Primes in S include:

$4 = 1 \cdot 4$, since $1 \in S$ and $4 \in S$ and $1 < 4$, but $4 \not< 4$.
$7 = 1 \cdot 7$
$10 = 1 \cdot 10$
$13 = 1 \cdot 13$
$19 = 1 \cdot 19$
$22 = 1 \cdot 22$
$25 = 1 \cdot 25$
$31 = 1 \cdot 31$
$34 = 1 \cdot 34$
$37 = 1 \cdot 37$
$43 = 1 \cdot 43$
$46 = 1 \cdot 46$
$55 = 1 \cdot 55$
$58 = 1 \cdot 58$
$61 = 1 \cdot 61$
$67 = 1 \cdot 67$

Composites in S include:

$16 = 4 \cdot 4$, since $4 \in S$ and $4 < 16$.
$28 = 4 \cdot 7$, since $4 \in S$ and $7 \in S$ and $4 < 28$ and $7 < 28$.
$40 = 4 \cdot 10$, since $4 \in S$ and $10 \in S$ and $4 < 40$ and $10 < 40$.
$49 = 7 \cdot 7$

$52 = 4 \cdot 13$
$64 = 4 \cdot 16$
$70 = 7 \cdot 10$ ☐

Proof. We prove : any member of S greater than 1 is either prime or a product of primes.

Let a be an arbitrary element of S greater than 1.
Then $a \in S$ and $a > 1$.
To prove a is either prime or a product of primes, we prove the equivalent statement : if a is not prime, then a is a product of primes.
Suppose a is not prime.
Since $a \in S$, then $a = 3k + 1$ for some integer k with $k \geq 0$.

Suppose $k = 0$.
Then $a = 3 \cdot 0 + 1 = 1$, so $a = 1$.
But, $a > 1$, so $a \neq 1$.
Therefore, $k \neq 0$.

Since $k \geq 0$ and $k \neq 0$, then $k > 0$.
Since $a > 1$ and a is not prime in S, then a can be factored into smaller integers in S.
Thus, there exist integers $x \in S$ and $y \in S$ such that $a = xy$ and $x < a$ and $y < a$.
Since $x \in S$, then $x = 3m + 1$ for some integer m with $m \geq 0$.
Since $y \in S$, then $y = 3n + 1$ for some integer n with $n \geq 0$.
We can show that $m > 0$ and $n > 0$.
Since $x \in \mathbb{Z}^+$ and $y \in \mathbb{Z}^+$, then either $x < y$ or $x = y$ or $x > y$.
Without loss of generality, assume either $x < y$ or $x = y$.
We consider these cases separately.
Case 1: Suppose $x = y$.
Then $3m + 1 = x = y = 3n + 1$, so $3m + 1 = 3n + 1$.
Hence, $3m = 3n$, so $m = n$.
Either $m \in S$ or $m \notin S$.
TODO: Finish proof.
Can x be factored into smaller factors in S?
Should we divide x by 3 using the division algorithm? ☐

Solution. For part b.
NO
TODO: Fix this!
This example does not work.
Let $s = 280 = 3 \cdot 93 + 1$.
Then $s \in S$.
Observe that $s = 280 = 4 \cdot 70 = 10 \cdot 28$.
Since $4 = 3 \cdot 1 + 1$, then $4 \in S$
Since $70 = 3 \cdot 23 + 1$, then $70 \in S$.

Since $10 = 3 \cdot 3 + 1$, then $10 \in S$.
Since $28 = 3 \cdot 9 + 1$, then $28 \in S$.

$\square$

Exercise 152. It is conjectured that every even integer can be written as the difference of two consecutive primes in infinitely many ways.

For example, $6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \ldots$.

Express the integer 10 as the difference of two consecutive primes in fifteen ways.

Solution. Observe that

$$\begin{aligned}
10 &= 13 - 3 \\
&= 17 - 7 \\
&= 23 - 13 \\
&= 29 - 19 \\
&= 41 - 31 \\
&= 47 - 37 \\
&= 53 - 43 \\
&= 71 - 61 \\
&= 83 - 73 \\
&= 89 - 79 \\
&= 107 - 97 \\
&= 113 - 103 \\
&= 137 - 127 \\
&= 149 - 139 \\
&= 167 - 157.
\end{aligned}$$

$\square$

Exercise 153. Let $a \in \mathbb{Z}^+$.

Then $a > 1$ is a perfect square iff in the canonical form of a all the exponents of the primes are even integers.

Proof. TODO We've already done this. So find the proof in one of the exercises and copy it here and clean up the proof to make it coherent, clear. $\square$

Lemma 154. ***Each prime factor of a square number greater than one has even exponent.***

Let $n \in \mathbb{Z}^+$ and $n > 1$.

Then each prime factor of n^2 has even exponent.

Proof. Since $n > 1$, then by the Fundamental Theorem of Arithmetic., n has a unique canonical prime decomposition $n = p_1^{e_1} * p_2^{e_2} * * * p_k^{e_k}$ for primes $p_1, p_2, ..., p_k$ and positive integers $e_1, e_2, ..., e_k$ such that $p_1 < p_2 < ... < p_k$.

Observe that $n^2 = (p_1^{e_1} * p_2^{e_2} * * * p_k^{e_k})^2 = p_1^{2e_1} * p_2^{2e_2} * * * p_k^{2e_k}$.

Therefore, each of the exponents $2e_i$ is even. □

Exercise 155. An integer is said to be square-free if it is not divisible by the square of any integer greater than 1.

a. Any integer $n > 1$ is square-free iff n can be factored into a product of distinct primes.

b. Every integer $n > 1$ is the product of a square-free integer and a perfect square.

Proof. TODO □

Exercise 156. Any integer n can be expressed as $n = 2^k m$, where $k \geq 0$ and m is an odd integer.

Proof. TODO □

Exercise 157. It is conjectured that there are infinitely many primes p such that $p + 50$ is also prime.

Find 15 of these primes.

Solution. We use SageMath to write a simple function to compute primes p and $p + 50$.

Below is a list of some primes.

$$
\begin{aligned}
&\text{prime } p | p + 50 \\
&(3, 53) \\
&(11, 61) \\
&(17, 67) \\
&(23, 73) \\
&(29, 79) \\
&(47, 97) \\
&(53, 103) \\
&(59, 109) \\
&(89, 139) \\
&(101, 151) \\
&(107, 157) \\
&(113, 163) \\
&(131, 181) \\
&(149, 199) \\
&(173, 223).
\end{aligned}
$$

□

Chapter 3.2 The Sieve of Eratosthenes

Chapter 3.2 Problems

TODO