Proof of Fundamental Theorem of Arithmetic:

Proof by Contradiction: Assume that \( \exists \) a positive integer \( > 1 \) which doesn't have this property. Let \( n \) be the smallest such integer, such an \( n \) exists by the well ordered property.

If \( n \) is prime, we get a contradiction and we are done. So suppose \( n \) is not prime. Then \( n = m_1 \cdot m_2 \), where \( m_1, m_2 < n \). But by the property that \( n \) is the smallest such integer, we can write \( m_1 \) and \( m_2 \) as a product of primes. Writing \( m_1 = \prod_{i=1}^{k} p_i^{n_i} \) and \( m_2 = \prod_{j=1}^{r} q_j^{t_j} \), we get

\[
    n = m_1 \cdot m_2 = \prod_{i=1}^{k} p_i^{n_i} \cdot \prod_{j=1}^{r} q_j^{t_j}
\]

This gives a contradiction, hence done.

Uniqueness: Suppose \( n = \prod_{i=1}^{k} p_i^{n_i} \), \( n = \prod_{j=1}^{r} q_j^{s_j} \).
Then must show that \( k = r \) and \( p_i = q_j \), for \( 1 \leq i \leq k \), \( 1 \leq j \leq r \).

Write \( n = p_1 \cdots p_k = q_1 \cdot q_2 \cdots q_r \), with \( p_i, q_j \) distinct.
Hence $p_i | n \Rightarrow p_i | q_1 \cdots q_k$.

But $p_i$, $q_j$'s are prime numbers

$\Rightarrow p_i | q_j \Rightarrow p_i = q_j$.

$n = p_1 \cdots p_c \cdots p_{c+1} \cdots p_k = q_1 \cdot q_2 \cdots q_j \cdots q_k$

From repeating this process conclude $k = 0$ and $p_i = q_j \Rightarrow$ Uniqueness of factorisation.

\[360 = 10 \times 36 = 2 \times 5 \times 4 \times 9\]

\[= 2 \times 5 \times 2 \times 2 \times 3 \times 3\]

\[= 2^3 \times 3^2 \times 5.\]
Def: The least common multiple (lcm) of two nonzero integers \( x \) and \( y \), denoted \([x, y]\) is the smallest positive integer divisible by both \( x \) and \( y \).

\[ [x, y] = e \Rightarrow x \mid e \text{ and } y \mid e. \]

Further, if \( x \mid f \) and \( y \mid f \), then \( e \leq f \).

**Ex.** \((36, 52) = 4 \) (gcd)

Suppose \( x = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \) \( \quad \text{Put } m_k = 0, \text{} \) \( y = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \)

\[ \begin{align*}
36 &= 4 \times 9 = 2^2 \times 3^2 = 2^2 \times 3^2 \\
52 &= 2 \times 26 = 2^2 \times 13 = 2^2 \times 3^0 \times 13^1 \\
(36, 52) &= 4; \quad [36, 52] = 2^2 \times 3^2 \\
&= \max(m_1, n_1) \quad \max(m_2, n_2) \quad \max(m_k, n_k) \\
&= \min(m_1, n_1) \quad \min(m_2, n_2) \quad \min(m_k, n_k).
\end{align*} \]

The
Lemma: If $x$ and $y$ are real numbers, then
$$\max(x,y) + \min(x,y) = x+y.$$ 

**Proof:** Suppose $x \geq y$, then $\max(x,y) = x$, $\min(x,y) = y$.
$$\Rightarrow \max(x,y) + \min(x,y) = x+y.$$

Theorem: If $a$, $b$ are positive integers, then
$$[a, b] = \frac{ab}{(a, b)}.$$ 

**Proof:** gcd $(a,b) = \text{Write } a = \prod p_i^{m_i} \ldots p_k^{m_k}$
$$b = \prod p_i^{n_i} \ldots p_k^{n_k}.$$ 

$$(a, b) = \prod p_i^{\min(m_i,n_i)} \ldots p_k^{\min(m_k,n_k)}.$$ 

$$[a, b] = \prod p_i^{\max(m_i,n_i)} \ldots p_k^{\max(m_k,n_k)}.$$ 

$$ab = \prod p_i^{m_i+n_i} \ldots p_k^{m_k+n_k}.$$ 

$$= \prod p_i^{\max(m_i,n_i)+\max(m_i,n_i)} \ldots p_k^{\max(m_k,n_k)+\min(m_k,n_k)}.$$ 

$$= \prod p_i^{\max(m_i,n_i)-\min(m_i,n_i)} \ldots p_k^{\max(m_k,n_k)-\min(m_k,n_k)}.$$ 

**Note:** $p_i^{\min(m_i,n_i)} = p_i^{\max(m_i,n_i)}$ 

$$\Rightarrow \frac{ab}{(a, b)} = [a, b].$$
\[ \text{Eqr : } 28, 52 \]
\[ 28 = 4 \times 7 = 2^2 \times 7 \quad \text{and} \quad 52 = 4 \times 13 = 2^2 \times 13 \]
\[ (a, b) = (28, 52) = 2^2 \times 7 \times 13 = 2^2 \times (1 \times 1) = 4 \]
\[ [a, b] = [28, 52] = 2^2 \times 7 \times 13 = 4 \times 7 \times 13 \]
\[ = 28 \times 13 = 364 \]
\[ \frac{a}{b} = \frac{28 \times 52}{4} = \frac{364}{4} \]

Expressing the \text{gcd} of \( a \) and \( b \) as a \( \text{l.c. of} \ a \) and \( b \):

\[ \text{Theorem: Let } a \text{ and } b \text{ be positive integers. Then } (a, b) = s_n a + t_n b, \]
where \( s_n \) and \( t_n \) are the \( n \) terms of the sequences defined recursively as follows:

\[ s_0 = 1, \quad t_0 = 0 \]
\[ s_1 = 0, \quad t_1 = 1 \]

and \( s_j = s_{j-2} - q_{j-1} \frac{s_{j-1}}{s_j}, \quad t_j = t_{j-2} - q_{j-1} \frac{t_{j-1}}{s_j} \) for \( j = 2, 3, \ldots, n \), where the \( q_j \) are the quotients in the division steps of the Euclidean algorithm used to compute \((a, b)\).
\( \text{Case: } (252, 198); \quad a = 6, \quad b = 6. \)

<table>
<thead>
<tr>
<th>( j )</th>
<th>( x_j )</th>
<th>( x_{j+1} )</th>
<th>( q_{j+1} )</th>
<th>( x_{j+2} )</th>
<th>( b_j )</th>
<th>( t_j )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>252</td>
<td>198</td>
<td>1</td>
<td>54</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>192</td>
<td>54</td>
<td>3</td>
<td>36</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>54</td>
<td>36</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>3</td>
<td>36</td>
<td>18</td>
<td>2</td>
<td>0</td>
<td>-3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ b_2 = x_0 - q_1 b_1 \quad (b_j = x_j - 2 - \frac{q_j}{b_{j-1}} b_{j-1}) \]

\[ = 1 - 1 \cdot 0 = 0 \]

\[ t_2 = t_0 - q_1 t_1 \quad (t_j = x_j - 2 - \frac{q_j}{b_{j-1}} b_{j-1}) \]

\[ = 0 - 1 = -1 \]

\[ b_3 = b_2 - q_2 b_2 = 0 - 3 \cdot 1 = -3 \]

\[ t_3 = t_2 - q_2 t_2 = 1 - 3(-1) = 4 \]

\[ b_4 = b_3 - q_3 b_3 = 1 - (1)(-3) = 4 \]

\[ t_4 = t_2 - q_3 t_3 = -1 - (1)(4) = -5 \]

\[ n = 4; \quad b_4 \cdot 252 + t_4 \cdot 198 = b_4 \cdot a + t_4 \cdot b \]

\[ = 4 \cdot (252) - 5 \cdot (198) = 1008 - 990 \]

\[ = 18 \]
The greatest common divisor (gcd) $d = (a, b)$ can be written as a linear combination:

$$d = sa + tb$$

in infinitely many ways. For all integers $k$, if $d = sa + tb$, then

$$d = \left( s + (k, \frac{b}{d}) \right) a + \left( t - (k, \frac{a}{d}) \right) b$$

for any integer $k$.

Given $b/d = 19.8/18 = 1.1$ and $a/d = 2.52/18 = 0.14$,

$$s = s_4 = 4, \quad t = t_4 = -5. \quad \text{Take } k = 1.$$

Thus, $d = (4 + 11k) \cdot a + (-5 - 14k) \cdot b$, $a = 252$, $b = 192$.

At $k = 0$, $d = 981$, $a = 1234$.

---

<table>
<thead>
<tr>
<th>$i$</th>
<th>$x_i$</th>
<th>$x_{i+1}$</th>
<th>$q_{i+1}$</th>
<th>$y_{i+1}$</th>
<th>$t_{i+2}$</th>
<th>$x_{i+2}$</th>
<th>$t_i$</th>
<th>$t_j$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1234</td>
<td>981</td>
<td>1</td>
<td>253</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>981</td>
<td>253</td>
<td>3</td>
<td>222</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>253</td>
<td>222</td>
<td>1</td>
<td>31</td>
<td>1</td>
<td>-1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>222</td>
<td>31</td>
<td>7</td>
<td>5</td>
<td>-1</td>
<td>4</td>
<td>-5</td>
<td>39</td>
</tr>
<tr>
<td>4</td>
<td>31</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td>-31</td>
<td>39</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$$t_i = 1 = (190) \left( \frac{1234}{981} \right) - 239 \left( \frac{981}{981} \right)$$

$$= 234460 - 234459 = 1$$
\[ (981, 1234) = 1. \]

\[ 86 = 190 + 239 = t_6; \quad 86a + t_6b = 1 \]

\[
(190) (1234) - (239)(981) = 234460 - 234459 = 1.
\]

For any integer \( k \),
\[
(86 + kb)a + (t_6 - ka)b = 1 \]
\[
86a + bat k + t_6b - kab = 1.
\]

**Lemma:** Let \( m \) and \( n \) be relative prime positive integers. Then, if \( d \) is a positive integer which is a divisor of \( m \) and \( n \), then there is a unique pair of positive divisors \( d_1 \) of \( m \) and \( d_2 \) of \( n \) such that \( d = d_1d_2 \). Conversely, if \( d_1 \) and \( d_2 \) are positive divisors of \( m \) and \( n \) respectively, then \( d = d_1d_2 \) is a positive divisor of \( mn \).

**Proof:** Write \( m = p_1^{m_1}p_2^{m_2}...p_k^{m_k} \), \( n = q_1^{n_1}q_2^{n_2}...q_l^{n_l} \).

Since \((m, n) = 1\), the sets \( \{p_i, \ldots, p_k\} \) and \( \{q_1, \ldots, q_l\} \) have no common element. If \( d \) is a positive divisor of \( mn \), then
\[
d = p_1^{e_1}p_2^{e_2}...p_k^{e_k}q_1^{f_1}...q_l^{f_l}, \quad 0 \leq e_i \leq m_i, \quad 0 \leq f_j \leq n_j.
\]
Let \( d_1 = (d, m) \), and \( d_2 = (d, n) \).
Hence $d_1 | m$ and $d_2 | n$. Then $d = d_1 d_2$.

$d_1 = p_1^{a_1} \cdots p_k^{a_k}$, $d_2 = q_1^{b_1} \cdots q_j^{b_j}$.

By FTA, these decompositions are unique.
Also every prime power in the factorisation of $d$ must occur in either $d_1$ or $d_2$. Prime powers of the form $p_i^{d_i}$ occur as divisors of $d_1$ and those of the form $p_j^{b_j}$ occur as divisors of $d_2$.

Hence $d_1 = (d, m)$, and $d_2 = (d, n)$.

Converse: $d_1 | m$ \(\iff\) $d_1 = \prod p_i^{d_i}$, $d_2 | n$ \(\iff\) $d_2 = \prod q_j^{b_j}$

\[0 \leq d_i \leq m_i; \quad 0 \leq b_j \leq n_j\]

Hence $d = d_1 d_2 | mn$.

---

Eg: \((15, 28): m = 15, n = 28.$

\[15 = 3 \times 5, \quad 28 = 2^2 \times 7\]

\[15 \times 28 = 420, \quad 60 \mid 420,\]

\[60 = 15 \times 4, \quad 15 \mid 15, \quad 4 \mid 28,\]

\[15 \times 28 = 2^2 \times 3 \times 5 \times 7\]

\[3 \mid 15, \quad 4 \mid 28, \quad \text{hence } 3 \times 7 = 21 \mid 420.\]
8.  A Diophantine Equation is an equation (or a set of equations) with integer coefficients. (Diophantus: Ancient Greek Mathematician)

\[ 4x + 5y = 83 \]
\[ 3x - 2y + 4z = 11 \]

Q: Can we find integral (i.e., integer) solutions for such an equation?

Brahmagupta – 7th Cent. CE

Theorem: Let \( a \) and \( b \) be integers with \( d = (a, b) \).

Then the equation \( ax + by = c \) has no integral solution if \( d \nmid c \). If \( d \mid c \), then there are infinitely many integral solutions. Moreover, if \( x = x_0 \) and \( y = y_0 \) is a particular solution so that \( ax_0 + by_0 = c \), then all other solutions \( (x, y) \), \( x, y \in \mathbb{Z} \) are given by \( x = x_0 + \left( \frac{b}{d} \right)n \), \( y = y_0 + \left( \frac{a}{d} \right)n \), where \( n \) is an integer.

pf. Suppose \( x_0, y_0 \in \mathbb{Z} \) such that \( ax_0 + by_0 = c \).

Let \( d = (a, b) \), then clearly \( d \mid c \). Hence if \( d \nmid c \), then \( ax + by \) has no integral solution.
Conversely, suppose $d|c$. Since $d=(a,b)$, we know that $d$ is a linear combination of $a$ and $b$, hence there exist integers $s,t \in \mathbb{Z}$ such that

$$d = sa + tb.$$  

Now $d|c \Rightarrow c = de$, $e \in \mathbb{Z}$. Hence, we get

$$c = de = ase + bte.$$  

Put $x_0 = ae$, $y_0 = te$, then we get an integral solution $(x_0, y_0)$.

Suppose $x = x_0 + \left(\frac{b}{d}\right)n$, $y = y_0 - \left(\frac{a}{d}\right)n$.

Substituting in $ax + by = c$, we get

$$a(x_0 + \left(\frac{b}{d}\right)n) + b(y_0 - \left(\frac{a}{d}\right)n) = ax_0 + by_0 = C.$$  

Hence $(x,y)$ is also an integral solution.

Conversely, suppose $x, y \in \mathbb{Z}$ s.t. $ax + by = c$.

We must show that $x = x_0 + \left(\frac{b}{d}\right)n$, $y = y_0 - \left(\frac{a}{d}\right)n$,

where $ax_0 + by_0 = C$ and $(x_0, y_0)$ is a given solution.

Have: $ax_0 + by_0 = C$; $ax + by = c$; hence

$$(ax + by) - (ax_0 + by_0) = C - C = 0.$$  

$\Rightarrow a(x-x_0) + b(y-y_0) = 0$. Now divide by $d=(a,b)$.

Get: $a\left(\frac{x-x_0}{d}\right) + b\left(\frac{y-y_0}{d}\right) = \frac{b}{d}(y_0-y)$.

Since $d=(a,b)$, we have $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.  

Hence \( \exists n \in \mathbb{Z} \) s.t. \( \left( \frac{a}{d} \right) n = y_0 - y \), since \( \frac{a}{d} \mid y_0 - y \). But this implies
\[
\left( \frac{a}{d} \right) n = y_0 - y \Rightarrow y = y_0 - \left( \frac{a}{d} \right)n.
\]

Hence any solution \((x, y)\) is of the form
\[
\left( \left( x_0 + \left( \frac{b}{d} \right)n \right), \ y_0 - \left( \frac{a}{d} \right)n \right).
\]

Example: \(21x + 16y = 36\); \((21, 16) = 1\), \(1 \mid 36\).

Hence has a solution (integral).

\(15x - 48y = 10\); \((15, 48) = 3\), \(3 \nmid 10\).

Hence has no integral solutions.

\(21x + 16y = 36\). To find solutions:
Express 1 as a l.c. of 21 and 16.

\(21(-3) + 16(4) = -63 + 64 = 1\). Hence

\(21(-3 \times 36) + 16(4 \times 36) = 1 \times 36 = 36\)

\((x_0, y_0) = (-108, 144)\) is an integral soln.

Any other solution is of the form:
\[
\left( x, y \right) = \left( -108 + 16n, 144 - 21n \right), \quad \left( \frac{b}{d} = 16, \frac{a}{d} = 21 \right)
\]