Definition 1. If $a \mid b$ then $a$ is a divisor of $b$ and $b$ is a multiple of $a$.

Definition 2. $d = \gcd(a, b)$ or $d = (a, b)$ is a GCD (greatest common divisor) of $a$ and $b$ iff

1. $d > 0$,
2. $d \mid a$ and $d \mid b$,
3. if $e \mid a$ and $e \mid b$ this implies $e \mid d$.

Definition 3. $e = \lcm(a, b)$ or $e = [a, b]$ is a LCM (lowest common multiple) of $a$ and $b$ iff

1. $e > 0$,
2. $a \mid e$ and $b \mid e$,
3. if $a \mid f$ and $b \mid f$ this implies $e \mid f$.

Example 1. Evaluate and factor the following GCDs and LCMs.

1. $\gcd(540, 3750) = 30 = 2^1 \cdot 3 \cdot 5^2$.
2. $\lcm(540, 3750) = 67500 = 2^4 \cdot 3^3 \cdot 5^4$.
3. $\gcd(4725, 3234) = 21 = 3 \cdot 7$.
4. $\gcd(3718, 3234) = 22 = 2 \cdot 11$.
5. $\lcm(4725, 3234) = 727650 = 2 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11$.
6. $\lcm(3718, 3234) = 546546 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 13^2$.

Definition 4. Two integers $a$ and $b$ are coprime or relatively prime if $\gcd(a, b) = 1$.

Definition 5. A prime number is a positive integer, other than unity, which is divisible only by itself and unity. A composite number is a positive integer which is neither prime nor unity.

Example 2. Sieve of Erathostenes.

Theorem 1. Every integer greater than or equal to 2 is either prime or a product of primes.

Proof. By an induction argument. Consider $n = 2$ first. This is a prime number so the theorem is true in this case. Suppose the hypothesis is true for the integers $2, \ldots, k$. Now consider the case $n = k + 1$. If $k + 1$ is prime then the theorem is true. If $k + 1$ is not prime then $k + 1 = r \cdot s$ where $r, s < k$. But $r$ and $s$ must be primes or products of primes and therefore $r \cdot s$ is a product of primes, and consequently $k + 1$ is a product of primes. □
Theorem 2 (Euclid Book VII). For any integer \( a \) and any positive integer \( b \) there exists unique integers \( q \) and \( r \) with the property that

\[
a = bq + r \quad \text{with} \quad 0 \leq r < b.
\]

Corollary 1. Given any positive integer \( n > 1 \), then any integer can be expressed in the form

\[
nk, nk + 1, nk + 2, \ldots, nk + n - 1
\]

for some integer \( k \).

Remark 1. When \( n = 2 \) any integer can be expressed as \( 2k, 2k + 1 \) and this partitions the integers into even and odd integers.

Example 3. Example of the form \( ax + by \) for \( a = 56 \) and \( b = 35 \) with \( x \in \{0, 1, 2, 3, 4\} \) and \( y \in \{-4, -3, -2, -1, 0\} \). Here \( \text{GCD}(56, 35) = 7 \).

<table>
<thead>
<tr>
<th>( ax + by )</th>
<th>( x = 0 )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>( y = -4 )</td>
<td>-140</td>
<td>-84</td>
<td>-28</td>
<td>28</td>
<td>84</td>
</tr>
<tr>
<td>( -3 )</td>
<td>-105</td>
<td>-49</td>
<td>7</td>
<td>63</td>
<td>119</td>
</tr>
<tr>
<td>( -2 )</td>
<td>-70</td>
<td>-14</td>
<td>42</td>
<td>98</td>
<td>154</td>
</tr>
<tr>
<td>( -1 )</td>
<td>-35</td>
<td>21</td>
<td>77</td>
<td>133</td>
<td>189</td>
</tr>
<tr>
<td>( 0 )</td>
<td>0</td>
<td>56</td>
<td>112</td>
<td>168</td>
<td>224</td>
</tr>
</tbody>
</table>

Theorem 3. If \( a, b \neq 0 \) and \( d = \gcd(a, b) \) then \( d \) is the least element in the set of all positive linear combinations of \( a \) and \( b \).

Proof. Let

\[ T = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}. \]

Suppose \( a \neq 0 \). If \( a > 0 \) then \( a \cdot 1 + b \cdot 0 = a \in T \) while if \( a < 0 \) then \( a \cdot (-1) + b \cdot 0 = -a \in T \) so \( T \) is not an empty set. By the well ordering principle \( T \) contains a least element, \( e = au + bv \). Now it is immediate that \( d \mid a, d \mid b \) implies that \( d \mid e \) and therefore \( d \leq e \). By the division algorithm there exists \( q, r \) such that

\[
a = eq + r \quad \text{with} \quad 0 \leq r < e.
\]

Therefore

\[
r = a - eq = a - (au + bv)q = a(1 - qu) + b(-vq).
\]

If \( r \neq 0 \) we have a contradiction since \( r \in T \) and \( r < e \). This means that \( r = 0 \) and \( e \mid a \). By a similar argument \( e \mid b \) and \( e \) is a common divisor of \( a \) and \( b \). Hence \( e \leq d \). In conclusion \( e = d \). \( \square \)
Corollary 2. Two integers $a$ and $b$ are coprime iff there exists integers $x$ and $y$ such that

$$ax + by = 1.$$ 

Proof. Sufficiency states that $\gcd(a, b) = 1$ and by the theorem above there must exist integers $x$ and $y$ such that $ax + by = \gcd(a, b) = 1$. The necessity condition flows from the fact that the least positive integer is unity and that $T$ contains this integer so $\gcd(a, b) = 1$. □