The **greatest common divisor** of two integers \( a \) and \( b \) (not both zero) is the greatest integer which is a common factor of both \( a \) and \( b \). We denote this number by \( \text{gcd}(a, b) \), or simply \((a, b)\) when there is no confusion about the intent of the notation.

Example: \((13320, 22140) = ?\)

Solution #1: The divisors of 13320 are

\[ 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 37, 40, 45, 60, 72, 74, 90, 111, 120, 148, 180, 185, 222, 296, 333, 360, 370, 444, 555, 666, 740, 888, 1110, 1332, 1480, 1665, 2220, 2664, 3330, 4440, 6660, 13320; \]

the divisors of 22140 are

\[ 1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 27, 30, 36, 41, 45, 54, 60, 82, 90, 108, 123, 135, 164, 180, 205, 246, 270, 369, 410, 492, 540, 615, 738, 820, 1107, 1230, 1476, 1845, 2214, 2460, 3690, 4428, 5535, 7380, 11070, 22140 \]

The common divisors are highlighted; the largest number in both sets is 180.
Solution #2: The prime factorizations of these numbers are $13320 = 2^3 \cdot 3^2 \cdot 5 \cdot 37$ and $22140 = 2^2 \cdot 3^3 \cdot 5 \cdot 41$. The gcd can be inferred from the factorizations to be $2^2 \cdot 3^2 \cdot 5 = 180$.

**Proposition** Suppose that the integers $m$ and $n$ have prime factorizations $\prod_{i=1}^{k} p_i^{d_i}$ and $\prod_{i=1}^{k} p_i^{e_i}$, respectively, where the $d$’s and $e$’s are nonnegative exponents. (This allows us to use the same set of primes for both numbers.) Then $(m, n) = \prod_{i=1}^{k} p_i^\text{min}(d_i, e_i)$. //

**Corollary** Every common divisor of $m$ and $n$ is a divisor of $(m, n)$. //

**Porism** Suppose that the integers $m$ and $n$ have prime factorizations $\prod_{i=1}^{k} p_i^{d_i}$ and $\prod_{i=1}^{k} p_i^{e_i}$, respectively, where the $d$’s and $e$’s are nonnegative exponents. Then the least common multiple of $m$ and $n$ is given by the formula $[m,n] = \prod_{i=1}^{k} p_i^\text{max}(d_i, e_i)$. //

**Corollary** $(m, n)[m,n] = mn$. //
Solution #3: Using the division algorithm, we find that
\[ 22140 = 1 \cdot 13320 + 8820. \]
This relation implies that any common divisor of 13320 and 22140 — and in particular the gcd — must also be a divisor of 8820. Significantly, it also implies that any common divisor of 8820 and 13320 — and in particular their gcd — is a common divisor of of 13320 and 22140. It follows that \((8820, 13320) \leq (13320, 22140)\) and \((13320, 22140) \leq (8820, 13320)\). So \((13320, 22140) = (8820, 13320)\).

The same principle allows us to say that \((8820, 13320) = (4500, 8820)\), since 4500 is the remainder of the division of 13320 by 8820. This procedure has the benefit of reducing the size of the original numbers we are dealing with, despite the fact that we have not yet computed the gcd. Continuing:

\[
(13320, 22140) = (8820, 13320) = 22140 = 1 \cdot 13320 + 8820 \\
= (4500, 8820) = 13320 = 1 \cdot 8820 + 4500 \\
= (4320, 4500) = 8820 = 1 \cdot 4500 + 4320 \\
= (180, 4320) = 4500 = 1 \cdot 4320 + 180 \\
= 180 \quad 4320 = 24 \cdot 4320
\]

Note that at each stage, the previous divisor becomes the new dividend and the previous remainder becomes the new divisor, the divisions ending when the remainder reaches 0. The final nonzero remainder is the desired gcd.
This process is called the **Euclidean algorithm.** (It appears in a slightly different form Euclid’s *Elements.*) It can be much abbreviated by laying out the computations in a simple array:

\[
\begin{array}{ccc}
22140 \\
13320 & 1 \\
8820 & 1 \\
4500 & 1 \\
4320 & 1 \\
180 & 24 \\
0 & \\
\end{array}
\]

The second column holds the integer quotients \( q_i \) for the divisions obtained when we divide a number in the first column \( r_i \) into the number above it \( r_{i-1} \); the remainder of the division \( r_{i+1} \) becomes the subsequent number in the first column:

\[
\begin{align*}
r_{i-1} \\
\vdots \\
r_i & q_i \\
r_{i+1} & \vdots \\
\end{align*}
\]

Note how much less computation is required to find the gcd by the Euclidean algorithm than be the first two methods we considered!
**Theorem** The gcd of the (positive) integers $m$ and $n$ is representable as an **integer linear combination** of $m$ and $n$. That is, there exist integers $x$ and $y$ so that $(m,n) = xm + yn$. In fact, $(m, n)$ is the smallest positive integer linear combination of $m$ and $n$.

**Proof** We need only prove the final statement. Let $S$ be the set of all positive integers of the form $xm + yn$. Clearly, $S$ is non-empty (consider the cases $x = 1$, $y = 0$, and $x = 0$, $y = 1$), so it has a least element. Call this number $g = x_0m + y_0n$.

Now $g$ is divisible by every common factor of $m$ and $n$; in particular, $(m, n) | g$. So $(m, n) \leq g$. On the other hand, dividing $m$ by $g$ yields a quotient and remainder: $m = qg + r$, $0 \leq r < g$. Substituting for $g$ in this equation we obtain $m = q(x_0m + y_0n) + r$, or $r = (1 - qx_0)m + (qy_0)n$. But this means either that $r$ is in $S$ and is smaller than $g$, which is impossible, or that $r = 0$. Therefore, $g | m$. An entirely similar argument shows that $g | n$, too. So $g$ is a common divisor of $m$ and $n$, whence $g | (m, n)$, implying that $g \leq (m, n)$. We can then conclude that $g = (m, n)$. //

It is possible to extend the Euclidean algorithm slightly so as to compute the values of $x$ and $y$ so that $(m,n) = xm + yn$:
Find $x$ and $y$ so that $(22140, 13320) = 22140x + 13320y$.

Consider solutions to the equation

\[ r = 22140x + 13320y \]

<table>
<thead>
<tr>
<th>$r$</th>
<th>$x$</th>
<th>$y$</th>
<th>$q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>22140</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>13320</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8820</td>
<td>1</td>
<td>□1</td>
<td>1</td>
</tr>
<tr>
<td>4500</td>
<td>□1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4320</td>
<td>2</td>
<td>□3</td>
<td>1</td>
</tr>
<tr>
<td>180</td>
<td>□3</td>
<td>5</td>
<td>24</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We place the trivial solutions $x = 1, y = 0$, and $x = 0, y = 1$ in the first two rows of the array, then use the arithmetic of the integer division of each $r$ by the subsequent value of $r$ to determine the subsequent values of $x$ and $y$ as well: if the $(i-1)$st and $i$th rows of the array are determined by equations

\[
\begin{align*}
    r_{i\square} &= 22140x_{i\square} + 13320y_{i\square} \\
    r_i &= 22140x_i + 13320y_i
\end{align*}
\]

and $r_{i+1} = r_{i\square} \div q_i r_i$, then the $(i+1)$st row is determined by subtracting $q_i$ times the $i$th equation from the $(i-1)$st: $x_{i+1} = x_{i\square} \div q_i x_i, y_{i+1} = y_{i\square} \div q_i y_i$. 
When the array produces the gcd as the last nonzero remainder, the row of the array containing the gcd also contains the appropriate coefficients that represent it as a linear combination of 22140 and 13320: from the above array, we see that $180 = -3 \cdot 22140 + 5 \cdot 13320$.

If the numbers $a, b$ have gcd = 1, we see that they share no common factors besides 1. Such are numbers are said to be **relatively prime** to each other.