Greatest Common Divisor and Bézout's Identity

Greatest Common Divisor (GCD):

The GCD of two integers a and b not both zero, as the name says, is the largest of all the divisors they have in common. If the only divisor a and b have in common is 1 ($\gcd(a,b)=1$), a and b are said to be **relatively prime**.

Finding GCD using Euclidean Algorithm:

To find $\gcd(a,b)$, assuming $a > b$, we use the Euclidean Algorithm as follows:

1. Divide a by b with remainder: $a = b \times q_1 + r_1$
2. Divide the previous divisor (b) by the previous remainder (r_1) with remainder: $b = r_1 \times q_2 + r_2$
3. Repeat step 2 until the remainder in the division is 0:

$$\begin{aligned} b &= r_1 \cdot q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n \\ r_{n-1} &= r_n \cdot q_n + 0 \end{aligned}$$

4. The most recent non-zero remainder is the GCD: $\gcd(a,b) = r_n$

Useful Fact: For all integers a, b, k:

$$\gcd(a,b) = \gcd(a-kb, b) = \gcd(a, b-ka).$$

In words, subtracting a multiple of the second number from the first, or subtracting a multiple of the first number from the second does not change the GCD.

This can be used to simplify GCD calculations.

Example. If a and b are relatively prime, find $\gcd(a+7b, 3a+22b)$.

Solution.
We can simplify the GCD by applying the above useful fact repeatedly. We can start by using the single a on the left side to cancel out the $3a$ on the right.

$$\begin{aligned}\gcd(a+7b, 3a+22b) &= \gcd(a+7b, 3a+22b-3(a+7b)) \\ &= \gcd(a+7b, b)\end{aligned}$$

Then, we can remove the $7b$ on the left with the b on the right.

$$\begin{aligned}\gcd(a+7b, b) &= \gcd(a+7b-7(b), b) \\ &= \gcd(a,b) = 1\end{aligned}$$

Thus, $\gcd(a+7b, 3a+22b) = 1$ and they are also relatively prime. ◆

Example. Calculate $\gcd(105, 24)$.

Solution.
We follow the steps outlined above:

1. Divide 105 by 24 with remainder:
$$105 = 24 \times 4 + 9$$
2. Divide 24 by 9 with remainder:
$$24 = 9 \times 2 + 6$$
3. Keep dividing with remainder until we find a remainder of 0:
$$9 = 6 \times 1 + 3$$
$$6 = 3 \times 2 + 0$$
4. The remainder before we found a 0 was 3, so we have that $\gcd(105, 24) = 3$. ◆

Bézout's Identity:

Bézout's identity says that for two integers a and b not both zero we can find $m, n \in \mathbb{Z}$ so that $am + bn = \gcd(a,b)$. To find these integers m and n we perform the extended Euclidean Algorithm outlined as follows:

1. Find $\gcd(a,b)$ by using the Euclidean Algorithm.
2. In the divisions from the Euclidean Algorithm, solve each of the equations for the remainder:
$$\begin{aligned} a = bq_1 + r_1 &\Leftrightarrow r_1 = a - bq_1 \\ b = r_1 q_2 + r_2 &\Leftrightarrow r_2 = b - r_1 q_2 \\ &\vdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n &\Leftrightarrow r_n = r_{n-2} - r_{n-1} q_{n-1} \end{aligned}$$
3. Starting from the last remainder, substitute the remainders backwards into the equation until you have an equation with a and b. When substituting, do not multiply numbers immediately. Instead, collect like-terms (this step will become clearer in the example). This process is called extended Euclidean Algorithm.

Example. Find $m, n \in \mathbb{Z}$ so that $105m + 24n = \gcd(105, 24)$.

Solution.
To do this we must follow the extended Euclidean Algorithm:

1. From the previous example we know $\gcd(105,24)=3$, we also have the equations we will need for step 2.
2. Solve the division equations for the remainder:

$$105 = 24\cdot 4 + 9 \Leftrightarrow 9 = 105 - 24\cdot 4$$
$$24 = 9\cdot 2 + 6 \Leftrightarrow 6 = 24 - 9\cdot 2$$
$$9 = 6\cdot 1 + 3 \Leftrightarrow 3 = 9 - 6\cdot 1$$

3. Start at the end and substitute all the remainders backwards:

$$\begin{aligned}
3 &= 9 - 6\times 1\\
3 &= 9 - (24 - 9\times 2)\times 1\\
3 &= 9 - 24 + 9\times 2\\
3 &= 9\times 3 - 24\\
3 &= (105 - 24\times 4)\times 3 - 24\\
3 &= 105\times 3 - 24\times 12 - 24\\
3 &= 105\times 3 + 24\times(-13)
\end{aligned}$$

Thus, $105\times 3 + 24\times(-13) = \gcd(105,24)$, i.e., $m = 3$ and $n = -13$. ◆