The Euclidean Algorithm

Math 31 - Topics in Algebra

This is a summary of the important definitions and results associated to the Euclidean algorithm, along with examples of the algorithm in action.

Theorem 1 (Division algorithm)**.** *Let n and m be integers, with $m > 0$. Then there exist integers q and r, with $0 \leq r \leq n-1$, such that*

$$n = qm + r.$$

Definition 1.

- *We say that an integer m **divides** an integer n if there exists $c \in \mathbb{Z}$ such that $n = cm$.*
- *The **greatest common divisor** of a and b, $\gcd(a, b)$, is the largest positive integer which divides both a and b.*
- *We say that a and b are **relatively prime** if $\gcd(a, b) = 1$.*

Euclidean algorithm: Given integers n and m (suppose that $m < n$), $\gcd(n, m)$ can be computed as follows:

1. Use the Division Algorithm to write
$$n = q_0 m + r_0.$$
2. Apply the Division Algorithm again to write
$$m = q_1 r_0 + r_1,$$
i.e., to obtain a new quotient and remainder.
3. Continue this process until you obtain a remainder of zero. The previous (nonzero) remainder is $\gcd(n, m)$.

Theorem 2. *Let $n, m \in \mathbb{Z}$. There exist integers x and y such that*

$$\gcd(n, m) = nx + my.$$

Example 2. Find $\gcd(105, 81)$.

Solution. We divide each remainder into the previous divisor:

$$\begin{aligned}
105 &= 1 \cdot 81 + 24 \\
81 &= 3 \cdot 24 + 9 \\
24 &= 2 \cdot 9 + 6 \\
9 &= 1 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0
\end{aligned}$$

We've reached a remainder of 0, so we stop. The last nonzero remainder is 3, so

$$\gcd(105, 81) = 3.$$

□

Example 3. Finding $\gcd(343, 210)$.

Solution. Run through the Euclidean algorithm until we hit 0:

$$\begin{aligned}
343 &= 1 \cdot 210 + 133 \\
210 &= 1 \cdot 133 + 77 \\
133 &= 1 \cdot 77 + 56 \\
77 &= 1 \cdot 56 + 21 \\
56 &= 2 \cdot 21 + 14 \\
21 &= 1 \cdot 14 + 7 \\
14 &= 2 \cdot 7 + 0
\end{aligned}$$

Then we see that $\gcd(343, 210) = 7$. □