Division algorithm: For integers $a, d > 0$, there exist unique integers $q, r$ such that $a = dq + r$ for $0 \leq r < d$.

Definition: The greatest common divisor of integers $a, b$, denoted $\gcd(a, b)$, is the greatest integer $c$ such that $c \mid a$ and $c \mid b$.

Euclidean Algorithm: (finds the gcd of two inputs)
The inputs are integers $a$ and $d$. The algorithm proceeds in the following manner...

\[
\begin{align*}
a &= dq_0 + r_0 & 0 \leq r_0 < d \\
d &= r_0q_1 + r_1 & 0 \leq r_1 < r_0 \\
r_0 &= r_1q_2 + r_2 & 0 \leq r_2 < r_1 \\
r_1 &= r_2q_3 + r_3 & 0 \leq r_3 < r_2 \\
\vdots
\end{align*}
\]

...until we have a remainder $r_i = 0$.

Let $s$ be the smallest index such that $r_s = 0$.

- If $s = 0$, then $\gcd(d, a) = d$.
- If $s > 0$, then $\gcd(d, a) = r_{s-1}$.

Proposition: $(a, d)$ and $(d, r_0)$ as defined above have the same common divisors.

Definition: $a$ and $b$ are relatively prime if $\gcd(a, b) = 1$.

Proposition: For two positive integers $a, b$, there exist integers $u, v$ such that

\[\gcd(a, b) = ua + vb.\]