Theorem 16.1 (Quotient-Remainder). If $n, d \in \mathbb{Z}^+$, then there exist unique integers q and r such that $n = d \cdot q + r$ and $0 \leq r < d$.

Lemma 17.1. If $a \in \mathbb{Z}$, then $\gcd(a, 0) = a$.

Lemma 17.2. If $a, b \in \mathbb{Z}, q, r, \in \mathbb{Z}^{\text{nonneg}}$, and $a = b \cdot q + r$, then $\gcd(a, b) = \gcd(b, r)$.

Lemma 17.1-17.2. If $a, b \in \mathbb{Z}$, then

$$\gcd(a,b) = \begin{cases} a & \textit{if } b = 0 \\ \gcd(b, a \bmod b) & \textit{otherwise} \end{cases}$$