Theorem 2.6 (Euclidean Algorithm). Let a and b be integers, with b positive. If b|a, then (a, b) = b. Otherwise, apply the division algorithm repeatedly. Let

$$a = bq_1 + r_1$$

$$b = r_1q_2 + r_2$$

$$r_1 = r_2q_3 + r_3$$

$$\vdots$$

$$r_{k-2} = r_{k-1}q_k + r_k$$

$$r_{k-1} = r_kq_{k+1} + 0,$$

where $q_i, r_i \in \mathbb{Z}$ for all i and $0 < r_k < r_{k-1} < \cdots < r_1 < b$. Then $(a, b) = r_k$.

Theorem 2.4 (Division Algorithm). Let $a, b \in \mathbb{Z}$ with b > 0. Then there exist unique integers q and r such that a = bq + r, with $0 \le r < b$.