The Division Algorithm (Division Lemma).
Let $x$ and $y$ be non–zero integers with $y > 0$. Then, there exist unique integers $q$ and $r$ such that $x = qy + r$ where $0 \leq r < y$.

1. What are the main stages in the proof?

2. What is the main idea in proving existence of $q$ and $r$?

3. How are $q$ and $r$ defined?

4. How is uniqueness of $q$ and $r$ proved?

5. Why is there a need for a more general version of the Division Algorithm Theorem?

6. What is the statement of the more general Division Theorem?

7. What is the main idea in its proof?
**Theorem (The Euclidean Algorithm).** Let \( x \) and \( y \) be integers. Then there exist integers \( q_1, q_2, ..., q_k \) and a descending sequence of positive integers, \( r_1, ..., r_k, r_{k+1} = 0 \), such that:

\[
\begin{align*}
  x &= q_1y + r_1 \\
  y &= q_2r_1 + r_2 \\
  r_1 &= q_3r_2 + r_3 \\
  &\vdots \\
  r_{k-1} &= q_kr_k + 0
\end{align*}
\]

Furthermore, \( \gcd(x, y) = r_k \).

**Euclid’s Lemma.** Suppose \( n, a, \) and \( b \in \mathbb{N} \). If \( n \mid ab \) and \( \gcd(n, a) = 1 \), then \( n \mid b \).

*Proof:*

**Alternative version of Euclid’s Lemma.** If \( p \) is prime and \( p \) divides \( ab \), then \( p \) divides \( a \) or \( p \) divides \( b \).

*Proof:*
**Definition.** Two integers are called coprime or relatively prime if their greatest common divisor is 1.

**Corollary.** If \( n \in \mathbb{N} \) is not a square number, then \( \sqrt{n} \notin \mathbb{Q} \).

*Proof:*

---

**Definition.** A **Diophantine equation** is an equation of the form \( mx + ny = c \), where \( m, n, c \in \mathbb{N} \). We are interested in solutions \((x, y) \in \mathbb{Z}^2\).

**Theorem.**

1. For all \( m, n \in \mathbb{N} \) there are integer solutions \( x \) and \( y \) to the equation \( mx + ny = c \) if and only if \( \gcd(m, n) \mid c \).

2. Suppose \( x = X \) and \( y = Y \) is a solution to \( mx + ny = c \). Then, for all \( t \in \mathbb{Z} \),
   
   \[
   x = X + \frac{nt}{\gcd(m, n)} \quad \text{and} \quad y = Y - \frac{mt}{\gcd(m, n)}
   \]

   is also a solution. Furthermore, all solutions are of this form.

*Proof:*