Introduction

Let $a, b \in \mathbb{Z}$. We say that a **divides** b, written $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$.

Definition 1. A positive integer $p > 1$ is called **prime** if its only positive divisors are 1 and p itself.

Hello

Definition 2. For integers a and b, not both zero, the **greatest common divisor** $\gcd(a, b)$ is the largest positive integer that divides both a and b.

The Euclidean Algorithm

The Euclidean algorithm is an efficient method for computing the greatest common divisor of two integers.

Theorem 3 (Division Algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q and r such that*

$$a = bq + r \quad \text{with} \quad 0 \leq r < b.$$

*Here q is called the **quotient** and r is called the **remainder**.*

Theorem 4. *If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. Since $r = a - bq$, we have $d \mid r$. Thus d is a common divisor of b and r, so $d \leq \gcd(b, r)$.

Conversely, let $d' = \gcd(b, r)$. Then $d' \mid b$ and $d' \mid r$. Since $a = bq + r$, we have $d' \mid a$. Thus d' is a common divisor of a and b, so $d' \leq \gcd(a, b) = d$.

Therefore $d = \gcd(b, r)$. ⬜

The Algorithm

To compute $\gcd(a, b)$ where $a \geq b > 0$:

1. Apply the division algorithm repeatedly:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 \leq r_1 < b \\
b &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}$$

2. The last non-zero remainder r_n is $\gcd(a, b)$.

Theorem 5 (Bézout's Identity). *Let $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$. Then there exist integers x and y such that*

$$ax + by = d.$$

Proof. Consider the set $S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$. This set is non-empty (contains $|a|$ or $|b|$) and bounded below by 1, so by the well-ordering principle it has a smallest element, say $d' = ax_0 + by_0$.

We claim that $d' = \gcd(a, b)$. First we show that $d' \mid a$. By the division algorithm, write $a = d'q + r$ with $0 \leq r < d'$. Then

$$r = a - d'q = a - (ax_0 + by_0)q = a(1 - x_0 q) + b(-y_0 q).$$

If $r > 0$, then $r \in S$ and $r < d'$, contradicting the minimality of d'. Thus $r = 0$ and $d' \mid a$. Similarly, $d' \mid b$.

So d' is a common divisor of a and b, hence $d' \leq d = \gcd(a, b)$.

Conversely, since $d \mid a$ and $d \mid b$, we have $d \mid (ax_0 + by_0) = d'$. Thus $d \leq d'$.

Therefore $d = d'$, completing the proof. ⬜