Lecture 12: Euclid's Lemma, Euclidean Algorithm, Be'zout's Theorem

Summary:
We introduce the Euclidean algorithm for finding greatest common divisors and prove Be'zout's theorem, which establishes that the gcd of two integers can be expressed as a linear combination of those integers. We examine Euclid's lemma and its applications to prime numbers, proving that there are infinitely many primes.

Topics Covered: Be'zout's theorem, composite number, Euclidean algorithm, Euclid's lemma, greatest common divisor, prime number

Lemma:

Let $a, b, c \in \mathbb{Z}$. Note that

$$c \mid a \wedge c \mid b \implies c \mid xa + yb$$

In particular,

$$\gcd(a, b) \mid xa + yb$$

Lemma:

Let $a, b \in \mathbb{Z}$. Let $d = \gcd(a, b)$

$$\implies a' = \frac{a}{d},\ b' = \frac{b}{d}$$
$$\implies \gcd(a', b') = 1$$

Euclidean Algorithm:

The Euclidian algorithm is used for finding the gcd of integers $a, b \in \mathbb{Z}$.

1. Replace the largest of the two numbers by their difference, keep the smaller
2. Repeat until we get a 0 in one of the entires
3. The last nonzero integer is the gcd

Example:

- $(56, 20)$
- $(36, 20)$
- $(16, 20)$
- $(16, 4)$
- $(12, 4)$
- $(8, 4)$
- $(4, 4)$
- $(4, 0)$

Therefore,

$$\gcd(56, 20) = 4$$

Lemma:

Let $a, b \in \mathbb{Z}$. We have

$$\gcd(a, b) = \gcd(a - b, b)$$

Proof:

We will show that the common divisors of a, b are the same as the common divisors $a - b, b$.

If we have a common divisor c of a and b, we know that

1. $c \mid a$
2. $c \mid b$

By lemma 1, we know that

$$c \mid a - b$$

This is because $a - b$ is an integer linear combination of a and b.

In particular, c is a common divisor of $a - b$ and b.

$$d \mid a - b \ \land \ d \mid b \implies 1 \cdot (a - b) + 1 \cdot b = a, d \mid . b$$

$$\text{QED}$$

Theorem:

The Euclidean algorithm terminates and yields the gcd of the two integers we started with.

Proof:

Looking at the long form of the algorithm, in each step, we preserve the gcd of the numbers, so, as long as we terminate, we get the gcd.

It terminates because in short form the smaller number between the two is strictly decreasing at each step, so we must reach 0.

Theorem - Be'zout's Theorem:

Let $a, b \in \mathbb{Z}$ and let $d = \gcd(a, b)$ such that $\exists \alpha, \beta \in \mathbb{Z}$ such that $d = \alpha a + \beta b$.

There are infinitely many possible $\alpha, \beta \in \mathbb{Z}$ satisfying the above property.

Proof:

For $a \geq b$, we have

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a - b \\ b \end{pmatrix}$$

For $a \leq b$, we have

$$\begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b - a \end{pmatrix}$$

Thus, there exists a matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

such that

$$\begin{pmatrix} \gcd(a, b) \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\text{QED}$$

Corollary:

Let $a, b \in \mathbb{Z}$ with $c \mid a$ and $c\,b$. Then, we have

$$c \mid \ \gcd(a, b)$$

Corollary - Euclid's Lemma:

Let $a, b, c \in \mathbb{Z}$ with $\gcd(b, c) = 1$ and $c \mid ab \implies abc \mid a$

Proof:

By Be'zout's theorem, we know that

$$1 = \beta b + \gamma c, \beta, \gamma \in \mathbb{Z}$$

Hence, we have that

$$a = \beta ab + \gamma ac$$

- $c \mid ab$ (hypothesis)
- $c \mid ac \implies c$ divides any integer linear combination of ab and ac

$\implies$ by $a = \beta ab + \gamma ac$, we have that $c \mid a$.

$$\text{QED}$$

Our goal is to simultaneously with converging of the Euclidean Algorithm, also calculate (α, β).

Definition:

Let p be a positive integer. p is prime means:

1. $p \neq 1$
2. The only positive divisors of p are 1 and p

A positive integer n is composite if

1. $n \neq 1$
2. n has at least one divisor other than 1 and n

All positives (besides 1) are partitioned into primes and composites.

Lemma:

Let $n \in \mathbb{Z}^+$. Then, $\exists p$ prime such that $p \mid n$.

Proof:

We prove the lemma by induction on n.

Base case: $n = 2$. The statement holds with $p = 2$, since 2 is prime.

Inductive step: Consider $n \in \mathbb{Z}^+$.

- In the case that n is prime, it divides itself
- In the case that n is composite, $\exists k,\ 1 < k < n, k \mid n$. By the inductive hypothesis, we have $\exists p$ prime such that $p \mid k \implies p \mid n$.

Theorem (Euclid):

There exist infinitely many primes.

Proof:

Suppose otherwise. Let $p_1, \ldots., p_k$ be all of the primes.

$$n = \prod_{i=1}^{k} p_i \ + 1 > 1 \implies \exists p \text{ prime } .\ p \mid \prod_{i=1}^{k} p_i + 1 = n$$

Also, $p \mid \prod_{i=1}^{k} p_i + 1$, since all of them are primes.

Therefore,

$$p \mid 1 \cdot \left(\prod_{i=1}^{k} p_i + 1\right) + (-1) \cdot \left(\prod_{i=1}^{k} p_i\right) \implies p = 1 \text{ (contradiction)}$$

Therefore, there are infinitely many primes.

$$\text{QED}$$