Lecture 13: Linear Diophantine Equations

Summary:
We study linear Diophantine equations and their solutions. We examine Euclid's lemma and its role in understanding divisibility properties.

Topics Covered: fundamental theorem of arithmetic, greatest common divisor, linear diophantine equation

Lemma:

Let p be prime and let $b, c \in \mathbb{Z}$. If $p \mid bc$ then $p \mid b$ or $p \mid c$.

> Is a prime number necessarily positive?

Example:

$$5 \mid 100 = 4 \cdot 25$$
$$\implies 5 \mid 4 \,\vee\, 5 \mid 25$$

Euclid's lemma:

Let $a, b, c \in \mathbb{Z}$ with $\gcd(b, c) = 1$. Then

$$c \mid ab \implies c \mid a$$

Example:

Proof:

$$d = \gcd(p, b) \implies d \mid p \,\wedge\, d \mid b$$

Case 1:

$$d = p \implies p \mid b$$

Case 2:

$$d = 1$$

Apply Euclid's lemma to $b, c, p \implies p \mid c$

Theorem - Fundamental theorem of arithmetic:

Let $n \in \mathbb{Z}$ with $n > 1$.

1. There exists primes $p_1, \ldots, p_r$ such that $n = p_1 \cdot \ldots \cdot p_r$.
2. If $q_1, \ldots, q_s$ are primes such that $n = q_1 \cdot \ldots \cdot q_s$, then $p_1, \ldots, p_r$ is a rearrangement of $q_1, \ldots, q_s$.

Proof:

By strong induction on n.

Base case:

$n = 2, r = 1, p_1 = 2$.

Inductive hypothesis:

$\forall k \in \mathbb{Z}$, k has a prime factorization.

Inductive step: We have to prove that n has a prime factorization.

Case 1: If n is prime, $r = 1$ and $p_1 = n$.

Case 2: If n is composite, then $\exists$ prime p such that

$$n = pq$$

$$1 < pq < n$$

By the inductive hypothesis, we know that both p and q have prime factorizations.

Proof that prime factorizations are unique:

Suppose that

$$n = p_1 \cdot \ldots \cdot p_r. = q_1 \cdot \ldots \cdot q_s$$

Take arbitrary prime p. If $p \notin \{p_1, \ldots, p_r, q_1, \ldots, q_s\}$, do nothing, If $p \in \{p_1, \ldots, p_r, q_1, \ldots, q_s\}$, then assume WLOG that $p = p_i$ with $i \in [r]$.

$$p \mid n = q_1 \cdot \ldots \cdot q_s$$

$$p \mid q_1 \cdot \ldots \cdot q_s = q \cdot (q_2 \cdot \ldots \cdot q_s)$$

$$\implies p \mid q_1 \ \vee \ p \mid q_2 \cdot \ldots \cdot q_s$$

$$\implies \ldots \implies p \mid q_j$$

for some $j \in [s] \implies q_j = p$.

Now, cross out on both sides

$$p_1 p_2 \ldots p_{i-1} p_{i+1} \ldots p_r = q_1 \ldots q_{j-1} q_{j+1} q_s$$

and repeat.

$$\text{QED}$$

Proposition:

Let $a, b \in \mathbb{Z}{>}\ 0$. By the fundamental theorem of arithmetic, we have

$$a = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$

$$b = p_1^{\beta_1} \ldots p_r^{\beta_r}$$

1. $a = b \iff \alpha_i = \beta_i \ \forall i \in [r]$
2. $a \mid b \iff \alpha_I \leq \beta_i \ \forall i \in [r]$
3. $\gcd(a, b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$

Lemma:

$\sqrt{2}$ is irrational.

Proof:

Suppose otherwise. Suppose that $\exists a, b \in \mathbb{Z}$ such that

$$\sqrt{2} = \frac{a}{b}$$

$$\implies 2b^2 = a^2$$

$$a = 2^{\alpha_1} 3^{\alpha_2} \ldots$$

$$b = 2^{\beta_1} 3^{\beta_2} \ldots$$

$$\implies 2^{\beta_1 + 1} = 2^{\alpha_1}$$

This is a contradiction.

$$\text{QED}$$

Linear equations:

$$ax + by = e$$

$$a, b, c \in \mathbb{Z}$$

We start with $e = 0$.

$$(a, b) \cdot (x, y) = 0$$

Proposition

The integer solutions of $ax + by = 0$ for $a, b \in \mathbb{Z}$ are

$$x = b'k$$

$$y = a'k$$

where $k \in \mathbb{Z}$ is arbitrary,

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

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

We must show that this is a solution for all $k \in \mathbb{Z}$, and, conversely, all solutions are of this form. Denote

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

To see that this is a solution, note that

$$a\frac{b}{d}k + b\left(-\frac{a}{d}\right)k = \frac{abk}{d} - \frac{abk}{d} = 0$$

Now, we prove that all integer solutions of $ax + by = 0$ are of the form above.

$$ax + by = 0$$

Divide LHS and RHS by d.

$$a'x + b'y = 0$$

$$a'x = b'(-y)$$

$$b' \mid a'x$$

Recall that $\gcd(a', b') = 1$. Therefore,

$$b' \mid x \implies x = b'k$$

for some $k \in \mathbb{Z}$.

$$\implies ab'k + b'y = 0$$

$$\implies y = -a'k$$

$$\text{QED}$$

Example:

Using this method, we want to find all integer solutions of

$$56x + 20y = 0$$

First, we compute $\gcd(56, 20)$. In this case, we have

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

$$a' = \frac{56}{4} = 14$$

$$a' = \frac{56}{4} = 14$$

$$b' = \frac{20}{4} = 5$$

$$x = 5k,\ y = -14k\ \ \forall k \in \mathbb{Z}$$