Lecture 14: Solutions to Linear Diophantine Equations, Modular Congruence

Summary:
We examine solutions to linear Diophantine equations, establishing conditions for their existence and methods for finding them. We introduce modular congruence and prove that the integers modulo m form a group under addition and a monoid under multiplication.

Topics Covered: Be'zout's theorem, Euclidean algorithm, greatest common divisor, group, integers modulo m, linear equation, linear equation solution lemma, modular congruence, monoid

Let

$$ax + by = e$$

with $a, b, e \in \mathbb{Z}$ be a linear equation.

We are looking for integral solutions $x, y \in \mathbb{Z}$.

Example:

$$2x + 4y = 3$$

Note that this doesn't have any integral solutions because the LHS is always even and the RHS is always odd.

Lemma:

Let $ax + by = e$ be a linear equation with $a, b, e \in \mathbb{Z}$, and $x, y \in \mathbb{Z}$ are variables.

Let $d = \gcd(a, b)$.

1. If $d \not| e$ then $ax + by = e$ has no integer solutions
2. If $d \mid e$ then $ax + by = e$ has infinitely many solutions

Proof of 1:

Suppose that $d \not| e$. We want to show that $ax + by = e$ has no integer solutions.

Suppose, for contradiction, that $ax + by = e$ has an integer solution (x, y).

We proved that any common divisor of a and b (in particular, $d = \gcd(a, b)$) divides any integral linear combination of a and b. In particular, $ax + by$ is a linear combination of a and b.

Therefore, we have that

$$d \mid ax + by$$

Recall that $ax + by = e$, so, we have that

$$d \mid e$$

which contradicts our initial assumption that $d \not| e$.

Therefore, we conclude that $ax + by = e$ has no integer solutions.

$$\text{QED}$$

Proof of 2:

Suppose that $d \mid e$. Then, Be'zout's theorem tells us that

$$d = \alpha a + \beta b$$

for some $\alpha, \beta \in \mathbb{Z}$.

Since $d \mid e$, we know that $e = qd$ for some $q \in \mathbb{Z}$.

Multiply by q. Then, we have

$$e = qd = (q\alpha)a + (q\beta)b$$

$$\implies x_0 = q\alpha, \;\; y_0 = q\beta$$

are integral solutions of $ax + by = e$

Recall that the associated homogeneous linear equation $ax + by = 0$ has infinitely many solutions

$$S_{\text{homogenous}} = \{(x', y') \in \mathbb{Z}^2 \;:\; ax' + by' = 0\}$$

$$|S_{\text{homogenous}}| = \infty$$

Then, we have infinitely many solutions to the non-homogeneous equation

$$S_{\text{non-homogenous}} = \{(x_0 + x', y_0 + y') \;:\; (x', y') \in S_{\text{homogenous}}\}$$

$$|S_{\text{non-homogenous}}| = \infty$$

$$\text{QED}$$

Summary of results:

- If $d \nmid e$ then there are no integral solutions
- If $d \mid e$, then there are infinitely many integral solutions. We find **all of them** as follows:
  - Find all solutions (x', y') to the homogeneous equation $ax + by = 0$
  - Find one solution (x_0, y_0) to the non-homogeneous equation $ax + by = e$
  - Then, the solutions are parameterized by $x = x' + x_0, \;\; y = y' + y_0$

We also proved that there are no solutions other than the ones described above.

Example:

Find all integer solutions of

$$56x + 20y = 8$$

Note that $\gcd(56, 20) = 4$ which divides 8. So, by the lemma we proved above, we know that this equation has infinitely many solutions.

First, we find a particular solution

$$-2 \cdot 56 + 6 \cdot 20 = 8$$

$$(x_0, y_0) = (-2, 6)$$

Then, we find all solutions to the homogeneous equation as follows:

$$56x + 20y = 0$$

$$a' = \frac{56}{\gcd(56, 20)} = 14$$

$$b' = \frac{20}{\gcd(56, 20)} = 5$$

Then, the solutions to the homogeneous equation are.

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

Translating the solutions to the homogeneous equation by the particular solution, we get

$$(5k + 2, -14k + 6) \;\; \forall k \in \mathbb{Z}$$

which is all solutions to $ax + by = e$.

$$\text{QED}$$

Definition - modulus:

$$a \equiv b \pmod m \iff m \mid a - b \iff \exists q \in \mathbb{Z}.\ a - b = qm$$

$$\iff \text{residue of a - b upon division by m is 0}$$

$$\iff \text{the residues of a and b upon fivision by m are equal}$$

Recall:

$\equiv$ is an equivalence relation on $\mathbb{Z}$, which means it is

1. Reflexive
2. Symmetric
3. Transitive

Proposition:

Let $a, b \in \mathbb{Z}$ and suppose that

$$a \equiv b \pmod m$$

$$a' \equiv b' \pmod m$$

Then, it follows that

1. $a + a' \equiv b + b' \pmod m$
2. $aa' \equiv bb' \pmod m$

Proof of 1:

We know that

$$m \mid (a - b)$$

$$m \mid (a' - b')$$

Therefore, there exist $k, k' \in \mathbb{Z}$ such that

$$a - b = km$$

$$a' - b' = k'm$$

This implies that

$$(a - b) + (a' - b') = m(k + k')$$

$$\implies (a + a') - (b + b') = m(k + k')$$

$$\implies a + a' \equiv b + b' \pmod m$$

$$\text{QED}$$

Proof of 2:

We know that

$$m \mid (a - b)$$

$$m \mid (a' - b')$$

So, there exist $k, k' \in \mathbb{Z}$ such that

$$a = b + km$$

$$a' = b' + k'm$$

Now, consider the product aa':

$$aa' = (b + km)(b' + k'm)$$

Expanding this expression, we get

$$aa' = bb' + b(k'm) + b'(km) + (km)(k'm)$$

$$aa' = bb' + m(k'b) + m(kb') + m^2(kk')$$

Factor out m:

$$aa' = bb' + m\left(k'b + kb' + mkk'\right)$$

This shows that

$$aa' - bb' = m\left(k'b + kb' + mkk'\right)$$

which means

$$m \mid (aa' - bb')$$

Thus,

$$aa' \equiv bb' \pmod{m}$$

$$\text{QED}$$

Congruence classes in $\mathbb{Z}$:

Define the congruence class notation:

$$[a]_m = \{b \in \mathbb{Z} \ : \ a \equiv b \ (\text{mod } m)\}$$

This is the set of integers that yield the remainder a when divided by m.

Then, define the $+$ and $\cdot$ operations on congruence classes:

$$[a]_m + [b]_m = [a + b]_m$$

$$[a]_m \cdot [b]_m = [ab]_m$$

Note that $+$ and $\cdot$ are well-defined operations.

Proof that $+$ is well-defined:

Assume that

$$[a]_m = [a']_m$$

$$[b]_m = [b']_m$$

This means

$$a \equiv a' \pmod{m}$$

$$b \equiv b' \pmod{m}$$

This implies that

$$m \mid (a - a')$$

$$m \mid (b - b')$$

Consider

$$(a + b) - (a' - b') = (a - a') + (b - b')$$

Since m divides both $(a - a')$ and $(b - b')$, m divides their sum too. We write:

$$m \mid (a + b - a' - b')$$

Therefore,

$$a + b \equiv a' + b' \pmod{m}$$
$$\implies [a+b]_m = [a' + b']_m$$

Therefore, $+$ is well-defined.

$$\text{QED}$$

Proof that $\cdot$ is well-defined:

$$\text{Proof omitted}$$

Congruence classes:

Denote $\mathbb{Z}_m$ to be the set of congruence classes modulo m

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Then, we have the following structures:

- $(\mathbb{Z}_m, +)$ is a group
- $(\mathbb{Z}, \cdot)$ is a monoid
    - It isn't necessarily a group because elements won't always be invertible!

Proof that $(\mathbb{Z}_m, +)$ is a group:

Note that $\mathbb{Z}_m$ is closed under $+$, by definition of $+$.

The associativity of $+$, as defined above, follows from the associativity of addition on integers.

Note that $[0]_m \in \mathbb{Z}_m$ is the identity element in $\mathbb{Z}_m$ with respect to $+$.

Finally, we have that for any $[a]_m \in \mathbb{Z}_m$, it holds that

$$[a]_m + [-a]_m = [a-a]_m = [0]_m = e_{\mathbb{Z}_m}$$
$$[-a]_m + [a]_m = [-a+a]_m = [0]_m = e_{\mathbb{Z}_m}$$

Therefore, every element in $\mathbb{Z}_m$ is invertible under $+$.

So, $(\mathbb{Z}_m, +)$ is a group.

$$\text{QED}$$

**Proof that $(\mathbb{Z}_m, \cdot)$ is a monoid:

By definition, $\mathbb{Z}_m$ is closed under $\cdot$. Note that $\mathbb{Z}_m$ has an identity element $[1]_m \in \mathbb{Z}_m$. Since multiplication of integers is associative, it follows that $\cdot$ is associative. So, $(\mathbb{Z}_m, \cdot)$ is a monoid.

$$\text{QED}$$