Lecture 11

Solving Diophantine linear equations Continued.

Euclid's algorithm is an efficient method for finding the gcd of two natural numbers.

Example EA applied to compute gcd(19,7).

$19 = 7 \cdot 2 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$ ← last non-zero remainder = gcd

$2 = 1 \cdot 2 + 0$

Thus $\gcd(19,7) = 1$.

Bézout's Theorem The Diophantine equation $ax+by=\gcd(a,b)$ always has a solution.

We can prove this using a procedure called the extended Euclidean algorithm that takes the calculations obtained in the course of EA and "runs them in reverse".

Example Extended Euclidean algorithm.

Goal Given a and b find x and y integers s.t. $ax + by = \gcd(a,b)$. Here $a = 19$, $b = 7$

Here calculations in EA.

$$19 = 7 \cdot 2 + 5 \quad (2)$$
$$7 = 5 \cdot 1 + 2 \quad (1)$$
$$5 = 2 \cdot 2 + 1 \leftarrow \gcd(19,7)$$

remainders

Idea: Rewrite remainders starting with the last non-zero remainder.

$$\underbrace{1}_{\gcd(19,7)} = 5 - 2 \cdot 2 \quad (1)$$
$$= 5 - (7 - 5 \cdot 1) \cdot 2$$
$$= 5 - \cancel{14}\ 2 \cdot 7 + 2 \cdot 5$$
$$= 3 \cdot 5 - 2 \cdot 7 \quad \text{\& check}$$

$$= 3 \cdot (19 - 7 \cdot 2) - 2 \cdot 7 \quad (2)$$
$$= 3 \cdot 19 - 6 \cdot 7 - 2 \cdot 7$$
$$= 3 \cdot 19 - 8 \cdot 7 \quad \text{STOP}$$

Thus

$$\underline{1} = 19(\underset{x}{3}) + 7(\underset{y}{-8})$$

It follows that $(3,-8)$ is an integer solution to $19x + 7y = 1$

A better method for solving this problem will be described once we have dealt with matrices

---

The above gives us a necessary and sufficient condition for a Diophantine linear equation to have a solution.

<u>Lemma</u> A Diophantine linear equation $ax + by = c$ has a solution if and only if $\gcd(a,b) \mid c$.

<u>Proof</u>

Proof 'If and only if' means that there are two things to prove.

S'pose that $ax+by=c$ has a solution. Then we can find $(x_0^*, y_0^*) \in \mathbb{Z}^2$ such that

$$a x_0^* + b y_0^* = c.$$

The LHS is divisible by $\gcd(a,b)$ and so the RHS is divisible by $\gcd(a,b)$.

S'pose that $\gcd(a,b) \mid c$. Let

$$c = \gcd(a,b)\, d \quad \text{for some } d \in \mathbb{N}.$$

By Bézout's theorem the equation $ax+by=\gcd(a,b)$ has a solution computed using the EEA. Let

$$ax' + by' = \gcd(a,b).$$

Multiply both sides by d to get

$$a(x'd) + b(y'd) = \gcd(a,b)d = c$$

Thus $(x'd, y'd)$ is a solution to $ax+by=c$ $\blacksquare$

Any one solution to $ax+by=c$ is called a <u>particular solution</u>.

<u>Example</u> Show that the Diophantine linear equation $4x+6y=10$ has a solution and find a particular solution.

<u>Solution</u> $\gcd(4,6)=2$ and $2 \mid 10$

Thus this Diophantine equation has at least one solution. Observe that

$$6-4=2$$

Thus

$$4(-1)+6(1)=2.$$

It follows that $(-1,1)$ is a solution to

$$4x+6y=2$$

Thus $(-5,5)$ is a <u>particular solution</u> to

$$4x+6y=10.$$

Given that a Diophantine linear equation $ax+by=c$ has a particular solution, we shall now show how to find all solutions.

We need some theory.

Let $a,b \in \mathbb{N}$. They are called coprime if $\gcd(a,b)=1$.

Gauss's Lemma Let $a \mid bc$ where $\gcd(a,b)=1$ then $a \mid c$.

Proof By Bézout's Theorem, $1 = ax'+by'$ for some $(x',y') \in \mathbb{Z}^2$. Multiplying both sides by c we get $c = acx' + bcy'$. RHS is divisible by a so $a \mid c$ as required ∎

Lemma $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$

This is the basis of writing a fraction in its lowest terms.

<u>Lemma</u> Let $\frac{a}{b}$ be a fraction in its lowest terms so $\gcd(a,b) = 1$. Suppose that $\frac{a}{b} = \frac{c}{d}$. Then $c = at$ and $d = bt$ for some $t \in \mathbb{Z}$.

<u>Proof</u> $ad = bc$. $a \mid ad$ so $a \mid bc$.
But a and b are coprime so by Gauss's lemma $a \mid c$. It follows that $c = at$ for some $t \in \mathbb{Z}$.

Thus $\cancel{a}d = bc = b\cancel{a}t$

Hence $d = bt$. $\blacksquare$

We are now ready to find <u>all</u> solutions to $ax + by = c$ given one particular solution (x_0, y_0).