Lecture 10

Any equation we wish to solve using only integers is said to be Diophantine (named after Diophantos, a Greek mathematician). We shall describe how to solve the Diophantine equation

$$ax + by = c \qquad (*)$$

where $a, b, c \in \mathbb{N}$ and $a, b, c \neq 0$.

Observation If $(*)$ has an integer solution then any number that divides both a and b must also divide c.

A number that divides both a and b ($a, b \in \mathbb{N}$, a, b not both zero) is called a common divisor of a and b. 1 is always a common divisor of a and b. There may be others. The largest common divisor of a and b is called the greatest common divisor denoted $\gcd(a, b)$.

We can refine our observation above.

If $ax + by = c$ has an integer solution then $\gcd(a,b) \mid c$.

This turns out to be the key to solving Diophantine linear equations in two unknowns.

Example We calculate $\gcd(6, 9)$

let $A = \{n : n \mid 6\}$, $B = \{n : n \mid 9\}$

$A = \{1, 2, 3, 6\}$, $B = \{1, 3, 9\}$

Set of common divisors $= A \cap B = \{1, 3\}$

Thus $\gcd(6, 9) = 3$.

The above example illustrates the obvious way of computing $\gcd(a,b)$. It is very inefficient. I shall now describe a very efficient way of computing gcd.

We need the following which we shall treat as an axiom.

Remainder theorem Given $a, b \in \mathbb{N}$, $b \neq 0$

We can write $a = bq + r$

(q: quotient, r: remainder)

where $0 \leq r < b$. In addition, q and r are unique.

The above theorem is the main tool for all calculations in $\mathbb{N}$ or $\mathbb{Z}$.

Euclid's algorithm This is an efficient way of computing $\gcd(a, b)$.

Remark $\gcd(a, 0) = a$ if $a \neq 0$.

Let $a \geq b > 0$. Then

$$a = bq + r \qquad 0 \leq r < b$$

Claim $\gcd(a,b) = \gcd(b,r)$

Proof. Let $d|a$ and $d|b$.

Then $r = a - bq$ and so $d|r$.

Let $d|b$ and $d|r$. Then since $a = bq + r$ it follows that the set of common divisors of a and b = the set of common divisors of b and r. Thus

$$\gcd(a,b) = \gcd(b,r).$$

Two points.

(i) (b,r) is smaller than (a,b).

(ii) The above process can be repeated with b and r.

Here is an example of how this idea can be turned into a method for computing gcd.

Example We compute gcd(19,7)

using Euclid's algorithm.

$$19 = 7 \cdot 2 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$\gcd(19,7) = \gcd(7,5) = \gcd(5,2) = \gcd(2,1) = \gcd(1,0) = 1$$

The last non-zero remainder = gcd(19,7)

What isn't so obvious is that we can use Euclid's algorithm to extract more information. In particular, we can find one solution to a special kind of Diophantine equation.

Bézout's theorem Let $a, b \in \mathbb{N}$ not both zero. The equation

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

can always be solved.

We shall use our calculation of Euclid's algorithm to solve the above equation in a process called the

extended Euclidean algorithm

Example We find one solution to

$$19x + 7y = 1 \quad (= \gcd(19,7))$$

using the extended Euclidean algorithm.

$19 = 7 \cdot 2 + \underline{5}$ ← remainders

$7 = 5 \cdot 1 + \underline{\underline{2}}$ ←

$5 = 2 \cdot 2 + \underline{\underline{1}}$ ← gcd(19,7)

$1 = 5 - \underline{\underline{2}} \cdot 2$ Rewrite remainders

$= 5 - (7 - 5 \cdot 1) \cdot 2$

$= 5 - 7 \times 2 + 2 \times 5$

$= 3 \times \underline{5} - 7 \times 2$ & check.

$= 3 \times (19 - 7 \cdot 2) - 7 \times 2$

$= 3 \times 19 - 6 \times 7 - 7 \times 2$

$= 3 \times (19) - 8 \times (7)$ Stop