453 Lecture 5

1. Greatest common divisor.

Suppose $a, b \in \mathbb{Z}$ not both 0. The greatest common divisor, $\gcd(a,b)$, is the largest positive integer that divides both a and b.

(Note that this equivalent to saying that the $\gcd(a,b)$ is a positive common divisor of a,b, with the property that for any integer d, $d \mid a,\ d \mid b \Rightarrow d \mid \gcd(a,b)$.).

Thm Let $a, b \in \mathbb{Z}$, a, b not both 0.
Let $S = \{ax + by \mid x, y \in \mathbb{Z},\ ax+by > 0\}$.
Then S is non-empty and $\gcd(a,b)$ is equal to the smallest element of S.
In particular, there exists $x, y \in \mathbb{Z}$ (not necessarily unique) such that

$$\gcd(a,b) = ax + by. \quad \text{(Bezout identity)}$$

Pf It is easy to check that S is non-empty.
Let d be the smallest element of S (which exists by the well ordering property).
Let $d = ax + by$ ...... (1) (cont)

We first prove that d is a common divisor of a, b.

Using Thm in Lecture 4, there exists q, r with

(2) .... $a = dq + r$, $0 \leq r < d$.

Substituting (1) in (2) we get

$$a = (ax+by)q + r$$

which gives

$$r = a(1-xq) + b(-yq).$$

If $r \neq 0$, then $r \in S$ and $r < d$, which is a contradiction!

So $r = 0$, which implies that $d \mid a$.

A similar argument proves that $d \mid b$.

Now suppose that $d' \mid a$, $d' \mid b$.

Then $d' \mid ax$, $d' \mid by$ and hence

$$d' \mid ax + by = d.$$

$\blacksquare$.