1st problem set is due Tuesday, Jan 17
2nd problem set will be on web by next Monday

Notation: $\mathbb{Z}$ = all integers

Previously in Math 103a!

$\gcd(a,b)$ = largest positive integer dividing a & b

Thm If $a, b \in \mathbb{Z}$, $\exists\ s, t \in \mathbb{Z}$ s.t.

$$\gcd(a,b) = as + bt$$

(assuming $a \neq 0$ & $b \neq 0$)

We'll prove this today.

Pf of Thm. Let $S = \{am + bn \mid m, n \in \mathbb{Z},\ am + bn > 0\}$

$S \neq \emptyset$ (empty set), so it contains a smallest number (by well-ordering)

call it d. Need to show $d = \gcd(a, b)$.

Step 1. Show $d \mid a$ & $d \mid b$. By symmetry (a and b play same roles here) suffices to show $d \mid a$. Need to use the fact that d is the smallest positive integer in S.

By the division algorithm,

$$a = qd + r, \quad 0 \leq r < d$$

so that $(*)\ qd = a - r$

Let s, t satisfy

$$(**)\ as + bt = d$$

Trick: multiply $(**)$ by $-q$ to get

$$(-qs)a + (1-qb)t = -qd = r - a$$

↑ by $(*)$

so that

$$(1-qs)a + (-qt)b = r < d$$

$\therefore$ either $r \in S$ or $r = 0$ (r is a linear combination of a & b). Since $r < d$ & d is the smallest number in S, must have $r = 0$ i.e. $a = qd$ so that $d \mid a$.

Step 2. Need to show that d is the largest divisor of a and b i.e. if $d' \mid a$ & $d' \mid b$ then $d' \leq d$

We'll show $d' \mid d$ (so that $d' \leq d$).

$d' \mid a$ & $d' \mid b \Longrightarrow a = d'h$ & $b = d'k$ (***)

for some $h, k \in \mathbb{Z}$

Trick: Substitute (***) for a & b in (**)

$$d = d'hs + d'kt = d'(hs + kt)$$

so that $d' \mid d$. Since both are positive, $d' \leq d$. //Thm

---

Non uniqueness of s & t comes from

$$\begin{array}{r} ab - ba = 0 \\ + \quad as + bt = d \\ \hline a(b+s) + b(t-a) = d \end{array}$$

A corollary is

Euclid's Lemma. If p is prime & $p \mid ab$, $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$ (or both)

Pf. If $p \mid a$, then done. So assume $p \nmid a$. Then $\gcd(p, a) = 1$ (since only divisors of p are 1 & p, but $p \nmid a$.) By previous Thm $\exists\, s, t \in \mathbb{Z}$ with

$$as + pt = 1$$

$$\therefore \boxed{(ab)s + bpt = b}$$

$p \mid abs$ & $p \mid bpt$ so $p \mid b$ //

Prime factorization Thm. If $2 \leq n$, then $\exists\, p_1, p_2, \ldots p_k$ prime (not necessarily distinct) such that

$$(*) \quad \boxed{n = p_1 p_2 \cdots p_k}$$

Furthermore, factorization is unique, up to order of the p_j.

Pf: Use induction to prove existence.

Assume (*) holds for all $\ell \in \mathbb{Z}$ with $2 \leq \ell < n$.

(Note that it holds for $\ell = 2$, since 2 is prime.) We'll prove (*) for n.

If n is prime, we're done. So suppose n is not prime, i.e. $n = ab$, $a, b \geq 2$.

By the inductive hypothesis, both a & b may be factored into primes, giving a factorization of n.

Uniqueness of the primes in (*)

This is just a sketch of a proof.

First prove the generalized Euclid Lemma:

If $p \mid q_1 \cdots q_n$, where $p, q_1, \ldots, q_n$ are all prime

then $p = q_i$ for some i.

If $p_1 \cdots p_k = q_1 \cdots q_{k'}$, then $p_1 = q_i$, some i.

$\therefore$ $p_2 \cdots p_k = q_1 \cdots q_{i-1} q_{i+1} \cdots q_{k'}$

and you can prove the uniqueness by induction.

More notation: $\operatorname{lcm}(a,b)$ =

least common multiple of $a, b \neq 0$

= smallest positive number that is a multiple of both a & b

Equivalence relations: one of the most important notions in mathematics

Def. An equivalence relation on a set S is a set R of ordered pairs of elements of S s.t.

(1) $(a,a) \in R$ (every element is equiv. to itself) reflexive

(2) $(a,b) \in R \iff (b,a) \in R$ (if a is equivalent to b, then b is equivalent to a) symmetric

(3) $(a,b) \in R$ & $(b,c) \in R \Longrightarrow (a,c) \in R$ (if a is equiv to b & b is equiv to c, then a is equiv to c) transitive

Notation If $(a,b) \in R$, write $a \sim b$

(other common notation is $a \equiv b$)

Given S, R get a new set

For $a \in S$, put $[a] = \{x \in S : x \sim a\}$

$[a]$ is called an **equivalence class**

a is called a **representative** of $[a]$

We are often interested in the set of all equivalence classes, sometimes written S/R (S mod R)

Ex 1. $S = \mathbb{Z}$, fix $n > 1$

For $a, b \in \mathbb{Z}$, put

$$a \sim b \iff a \bmod n = b \bmod n$$

Then $[a] = \{a + kn : k \in \mathbb{Z}\}$

Set of all equivalence classes

$$= \{[0], [1], \ldots, [n-1]\}$$

So $x \in [j] \iff x \bmod n = j \bmod n$