Lecture 5

Uniqueness of factorization: $n = p_1 \cdots p_r = q_1 \cdots q_s$, p_i, q_j prime

Then we need to prove $r = s$, $p_i = q_i$ by permutation

Since $p_1 | n$, $p_1 | q_1 \cdots q_s$

prime divisibility property $\Rightarrow p_1 | q_j$ for some j, by permutation we can assume $j = 1$.

$p_1 | q_1$ since q_1 is a prime $p_1 = q_1$

Divide by p_1

$p_2 \cdots p_r = q_2 \cdots q_s$

Repeat this process

Then $r = s$, $p_1 = q_1, \cdots p_r = q_s$

Two problems:

① How can we tell if n is a prime?

② If n is not a prime, factor it into a product of primes

Chapter 8 Congruence

$a \equiv b \pmod{m}$

a is congruent to m if $m | a - b$

$a_1 \equiv b_1 \pmod{m}$

$a_2 \equiv b_2 \pmod{m}$

$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$

$a_1 a_2 \equiv b_1 b_2 \pmod{m}$

But $ac \equiv bc \pmod{m}$ doesn't imply $a \equiv b \pmod{m}$

$15 \cdot 2 \equiv 20 \cdot 2 \mod 10$, but $15 \not\equiv 20 \pmod{10}$

But if $\gcd(c, m) = 1$, then it is true, $m | ac - bc = c(a-b)$

$\Rightarrow m | a - b \Rightarrow a \equiv b \pmod{m}$

$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \equiv 0 \pmod{m}$ congruent equation

Try each value $0, 1, \cdots, m-1$

e.g. $x^2 + 2x - 1 \equiv 0 \pmod{7}$

try $0, 1, \cdots, 6$

so $x = 2, 3$ are solutions This works only when m is small

$x^2 \equiv 3 \mod 10$ has no solutions

If m is a prime, $x^n + a_1 x^{n-1} + \cdots + a_n \equiv 0 \pmod{m}$ has at most n solutions

This is no longer true if m is not a prime

e.g. $x^2 \equiv 1 \pmod{8}$

$x \equiv 1, 3, 5, 7 \pmod{8}$ are solutions

Linear Congruence

$ax \equiv b \pmod{m}$

$m | ax - c$

$ax - c = my$

$ax - my = c$

let $g = \gcd(a, m)$

$\{ax - my : x, y \in \mathbb{Z}\} = g\mathbb{Z}$

If $g \nmid c$, $ax - my = c$ has no solutions

i.e. $ax \equiv c \mod m$ has no solution

Suppose $g | c$, $au + mv = g$ has a solution by Euclidean ..

Linear Congruence Thm

Let a, c and m be ints with $m \geq 1$ and $g = \gcd(a, m)$

(a). If $g \nmid c$, then $ax \equiv c \pmod{m}$ has no solutions

(b). If $g | c$, then $ax \equiv c \pmod{m}$ has exactly g incongruent solutions. To find the solutions, first find a solution (u_0, v_0) to the linear equation

$au + mv = g$

Then $x_0 = \frac{c u_0}{g}$ is a solution to $ax \equiv c \mod m$ and a complete set of incongruent sol'ns is given by

$x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m}$ for $k = 0, 1, \cdots, g-1$

say $u=u_0, v=v_0$

Then $a(\frac{c}{g}u_0)+m(\frac{c}{g}v_0)=c$

so $x_0=\frac{c}{g}u_0 \pmod m$ is a sol to $ax\equiv c \pmod m$

Suppose x_1 is another solution

$ax_0\equiv c \bmod m$

$ax_1\equiv c \bmod m$

$ax_0\equiv ax_1 \bmod m$

$m \mid ax_1-ax_0$

$\frac{m}{g} \mid \frac{a}{g}(x_1-x_0)$

so $(\frac{m}{g},\frac{a}{g})=1$, $\frac{m}{g} \mid x_1-x_0$

So $x_1=x_0+\frac{m}{g}k$ for some k

Any two sets that differ by a multiple of m are considered to be the same.
So there are exactly g different sets $k=0,1,\cdots,g-1$

e.g. $18x\equiv 8 \bmod 14$ $\quad \gcd(18,14)=2$

solve $18u+14v=8$

$u=4$

$x_0=4\times 4=16\equiv 2 \bmod 14$

All other sol's are $x_1=2+\frac{14}{2}k$, $k=0,1$

$=2, 9$

e.g. $893x\equiv 266 \bmod 2432$

$\gcd(893,2432)=19$

$19 \mid 266$

First solve $893u+2432v=19$

$(u,v)=(-49,18)$

$x_0=-49\times\frac{266}{19}=-686\equiv 2432-686$

$x\equiv -686+\frac{2432}{19}k$, $k=0,\cdots,19$

Remark: (next class) "exactly one solution" case