Polynomial congruences.

- Finding solutions (if they exist) to problems like.

$$f(x) \equiv 0 \pmod{m}$$

where f is a polynomial with integer coefficients.

Compare with the situation for poly. equations

$$f(x) = 0.$$

Theorem "Fundamental Theorem of Algebra"

If f is a poly. of degree n with complex coefficients.

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$a_i \in \mathbb{C}$$

then $f(x) = 0$ will have n solutions in $\mathbb{C}$ (counted with multiplicities)

Q?, Might something like this be true for our congruences.

Well, it can't be as simple as F.T.A.

Ex 6.1 Consider

$$2x - 3 \equiv 0 \pmod 4$$

$$\iff \quad 2x \equiv 3 \pmod 4$$

Has <u>no</u> solutions. Check all possible x

$$\left.\begin{array}{l} x \equiv 0,\ 2x \equiv 0 \\ x \equiv 1,\ 2x \equiv 2 \\ x \equiv 2,\ 2x \equiv 0 \\ x \equiv 3,\ 2x \equiv 2 \end{array}\right\} \pmod 4$$

<u>Ex 6.2</u> Consider $x^2 - 1 \equiv 0 \pmod 8$

This has four solutions. Since for $x \equiv 1, 3, 5, 7 \pmod 8$ then $x^2 \equiv 1 \pmod 8$

<u>Also solved by</u> $x = \underset{[1]}{9}, \underset{[1]}{17}, \underset{[3]}{11}, \underset{[5]}{13}, \ldots$

A reminder, when solving

$$f(x) \equiv 0 \pmod m$$

we're talking about congruence classes of solutions.

Remember: $a \equiv b \pmod m$ then

$$f(a) \equiv f(b) \pmod m$$

for any poly. f with integer coefficients.

First, a simple case

Linear congruences (polys of degree 1)

$$ax \equiv b \pmod{n}$$

Tempted to say there is a solution namely $x \equiv a^{-1} b \pmod{n}$.

Valid, provided a^{-1} exists, ie provided $\gcd(a, n) = 1$

Thus theorem 6.1 If $\gcd(a, n) = 1$, i.e. $a^{-1} \pmod{n}$ exists then

$$ax \equiv b \pmod{n}$$

has a unique solution

$$x \equiv a^{-1} b \pmod{n}$$

Eg.

$$5x \equiv 3 \pmod{11}$$

$\equiv 5^{-1} \bmod 11$

Note $\gcd(5, 11) = 1$ E.A. $5x + 11y = 1$

This is uniquely solved by

$$\boxed{x \equiv 5^{-1} \cdot 3} \pmod{11}$$

$$\equiv 9 \cdot 3$$

$$\equiv 27$$

$\equiv 5$] $\pmod{11}$.

But what if $\gcd(a,n) > 1$?
Can solutions exist? Not always,
see Ex 6.1.

Let's suppose a solution $x \in \mathbb{Z}$.
exists for $ax \equiv b \pmod{n}$

$$\iff n \mid ax - b$$

$$\iff \exists q \in \mathbb{Z}. \quad ax - b = qn.$$

$$\iff \exists q \in \mathbb{Z} \quad b = ax - qn.$$

Therefore a solution exists for $ax \equiv b \pmod{n}$
iff. $\exists \underline{q, x} \in \mathbb{Z}$ $\underline{b = ax - qn}$

i.e. iff b is a linear combination
of a and n

i.e. $d \mid b$, where $d = \gcd(a, n)$.

<u>This is Th. 6.2</u>

Solutions to $ax \equiv b \pmod{n}$
exist iff $d \mid b$, where $d = \gcd(a, n)$.

So if $d|b$, then how many solutions exist, and what are they?

This story for linear congruences is finished with theorem 6.3

<u>Theorem 6.3</u> $\quad ax \equiv b \pmod{n}$

Proof of this is along similar lines to theorems 6.1, 6.2.

<u>Sketch</u> If $d = \gcd(a,n)$ & $d|b$.

then

$$ax \equiv b \pmod{n} \ \& \ \frac{a}{d}x \equiv \frac{b}{d} \pmod{n/d}$$

have the same integer solutions since.

$$ax - b = qn \iff \frac{a}{d}x - \frac{b}{d} = q\frac{n}{d}$$

and these

$$x_i \equiv t + i\frac{n}{d}, \quad i = 0, \ldots, d-1$$

are all solutions to the reduced congruence, since.

$$x_i \equiv t \pmod{\frac{n}{d}}$$

and so are solutions to original congruence. Then we show the x_i

are all distinct modulo n.

Ex 6.3

Q1. $5x \equiv 3 \pmod{24}$

$\gcd(5,24)=1$, so there's a unique solution

$d=1$

$$x \equiv 5^{-1} \cdot 3 \pmod{24}$$
$$\equiv 5 \cdot 3 \quad " \quad "$$
$$\equiv 15 \pmod{24}$$

Q2. $25x \equiv 15 \pmod{120}$ $(*)$

Apply Th. 6.3.

$\gcd(25,120) = 5 = d.$

and $5 \mid 15$ So there are five solutions modulo 120, given by

$\boxed{x_i \equiv t + i\,24}$ for $i=0,\ldots,4$

where t is the unique solution to the reduced congruence.

$$5x \equiv 3 \mod 24$$

$\Longleftrightarrow$ $x \equiv \underbrace{15}_{t} \pmod{24}$, from above.

So solutions to $(*)$ are

$x_0 \equiv 15$, $x_1 \equiv 39$, $x_2 \equiv 63$, $x_3 \equiv 87$,
$x_4 \equiv 111$ $\pmod{120}$

- polys of higher degree will be discussed tomorrow.
- In general, to solve a poly congruence

$$f(x) \equiv 0 \pmod{m}$$

we will proceed by solving the set of congruences (individually)

$$m = \prod_{i=1}^{r} p_i^{a_i}$$ ⟵ prime factorization of m. p_i distinct primes

$$f(x) \equiv 0 \pmod{p_i^{a_i}}, \quad i = 1, \dots, r$$

then by taking a combination of solutions to this set

$$x \equiv b_i \pmod{p_i^{a_i}}$$

we will generate a solution x

of $f(x) \equiv 0 \pmod{m}$ that uniquely corresponds to this set of solutions.

Chinese Remainder Theorem

Let $m_1, \ldots, m_k$ be pairwise coprime moduli

i.e. for $i \neq j$ $\gcd(m_i, m_j) = 1$.

(eg. the $p_i^{a_i}$ from the discussion above).

Note the 4-tuple $(2, 4, 3, 9)$ is a coprime 4-tuple. i.e. $\gcd(2,4,3,9) = 1$, but not pairwise-coprime since $\gcd(2,4) = 2$, $\gcd(3,9) = 3$.

Then the system of simultaneous congruences.

$$x \equiv b_i \pmod{m_i}$$
$$i = 1, \dots, k.$$

is equivalent to a unique congruence class modulo

$$M = m_1 \cdots m_k = \prod_{i=1}^{k} m_i$$

<u>Proof</u> (Very constructive, i.e. we're going to fully specify the solution modulo M).

Define some ingredients.

$$M = \prod_{i=1}^{k} m_i$$

$$M_i = \frac{M}{m_i} = \prod_{\substack{j=1 \\ j \neq i}}^{k} m_j, \quad i = 1, \dots, k$$

$$M_i' \equiv M_i^{-1} \pmod{m_i}$$

note this inverse exists since

$$\gcd(M_i, m_i) = 1,$$ since

m_i are pairwise-coprime.

Then the solutions x to the simultaneous system

$$x \equiv b_i \pmod{m_i} \quad i = 1, \dots, k.$$

is the unique congruence class

$$x \equiv \sum_{i=1}^{k} b_i M_i M_i' \pmod{M}$$

$$\equiv b_1 M_1 M_1' + b_2 M_2 M_2' + \cdots \quad (\text{" "})$$
$$+ b_k M_k M_k'$$

What happens when we look at such an integer x modulo

m_j for some j from $\{1, \ldots, k\}$

$$x \equiv b_j M_j M_j' \pmod{m_j}$$

since $m_j \mid M_i$ for all $i \neq j$

i.e. $M_i \equiv 0 \pmod{m_j}$

for all $i \neq j$.

but recall $M_j' \equiv M_j^{-1} \pmod{m_j}$

So $x \equiv b_j \pmod{m_j}$

as required for $j = 1, \ldots, k$.

Then we argue that this is the unique solution.

Example 6.4 bi $\quad$ m i

Q1.
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7.$$

C.R.T. says there is a unique solution to these simultaneous modulo $M = 105$.

$M_1 = 35$, $M_2 = 21$, $M_3 = 15$.

Their inverses are:

$$\boxed{M_1'} \equiv M_1^{-1} \bmod 3$$
$$\equiv 35^{-1} \bmod 3$$
$$\equiv 2^{-1} \bmod 3$$
$$\equiv \boxed{2}$$

$$\boxed{M_2'} \equiv 21^{-1} \pmod 5$$
$$\equiv 1^{-1} \pmod 5$$
$$\equiv \boxed{1} \pmod 5$$

$$\boxed{M_3'} \equiv 15^{-1} \bmod 7.$$
$$\equiv 1^{-1} \quad " \quad "$$
$$\equiv \boxed{1} \pmod 7$$

So the solution is

$$\boxed{x \equiv \sum_{i=1}^{3} b_i M_i M_i'} \pmod M$$

$$\equiv \boxed{2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}}$$

$$\equiv 140 + 63 + 30$$

$$\equiv 233 \pmod{105}$$

$$\equiv \boxed{23 \pmod{105}}$$

$\boxed{Q2}$

$$\begin{array}{ll} & \underline{b_i} \qquad \underline{m_i} \\ x \equiv & 0 \pmod{3} \\ x \equiv & 1 \pmod{4} \\ x \equiv & 10 \pmod{23} \end{array}$$

$x \equiv \, ? \pmod{276}$.

$M = 276$, $M_1 = 92$,

$M_2 = 69$, $M_3 = 12$

$M_1' \equiv 92^{-1} \equiv 2^{-1} \equiv 2 \pmod{3}$

$M_2' \equiv 69^{-1} \equiv 1^{-1} \equiv 1 \pmod{4}$

$M_3' \equiv 12^{-1} \equiv 2 \pmod{23}$.

So by the C.R.T. sol is

$$\boxed{x \equiv 0 \cdot 92 \cdot 2 + 1 \cdot 69 \cdot 1 + 10 \cdot 12 \cdot 2} \pmod{276}$$

$$\equiv 69 + 240 \equiv 309 \mod (276)$$

$$\boxed{\equiv 33 \pmod{276}}$$