Math 4400  
Week 5 - Tuesday  
Roots of polynomials + modular arithmetic  
gone off the rails.

Definition: Let $R$ be a ring and let $f(x) \in R[x]$ be a polynomial with coefficients in $R$. An element $r \in R$ is a root or zero of $f(x)$ if $f(r) = 0$.

Example: Let $f(x) = x^2 - 1$ (makes sense for any $R$). $x^2 - 1 = (x-1)(x+1)$ so $1, -1$ are always roots. If $R$ is a field, these are the only roots, but if $R = \mathbb{Z}/8\mathbb{Z}$ then:

- $f(0) = 0^2 - 1 = -1$  

- $f(1) = 1^2 - 1 = 0 \checkmark$  

- $f(2) = 2^2 - 1 = 3 \mod 8$ and $0$, are all roots  

- $f(3) = 3^2 - 1 = 8 = 0 \checkmark$  

of $x^2 - 1$ in
\[ f(4) = 11 - 1 = -1 \neq 0 \quad \overline{\mathbb{Z}}/\mathbb{Z} \cdot f(5) = 25 - 1 = 24 = 0 \checkmark \]
\[ f(6) = 3(-1 = 3 \neq 0, \\
 f(7) = 49 - 1 = 48 = 0 \checkmark \\
\overline{\mathbb{Z}} - 1 \]

**Theorem:** If \( K \) is a field and \( f(x) \in K[x] \), then for any \( a \in K \),
\[ f(a) = 0 \iff a \text{ is a root of } f \iff (x-a) \mid f(x). \]
\[ \text{this is the definition of a root.} \]
\[ \text{i.e. } f(x) = (x-a) q(x) \text{ for some } q(x) \in K[x]. \]

**Corollary:** If \( K \) is a field and \( f(x) \in K[x] \), then \( \# \text{ roots of } f(x) \leq \deg f(x) \text{ in } K \).

**Corollary:** If \( K \) is a field and \( f(x) \in K[x] \) is such that \( \deg f \leq 3 \), then \( f \) is irreducible/prime in \( K[x] \) if and only if \( f \) has no roots in \( K \).

**Recall:** If \( p \) is prime, \( \overline{\mathbb{Z}}/p\overline{\mathbb{Z}} \) is a field.
We will use the notation \( F_p := \overline{\mathbb{Z}}/p\overline{\mathbb{Z}} \), and call it "the field with \( p \) elements."
Example: Wilson's Theorem - if \( p \) is prime, then \((p-1)! \equiv -1 \mod p\).

\[ n! = \prod_{a=1}^{n-1} a \]

\("N \text{ Factorial.}"\)

E.g. \( p=2 \):
\[ (2-1)! = 1! = 1 \equiv -1 \mod 2 \, \checkmark \]

\( p=3 \):
\[ (3-1)! = 2! = 2 \cdot 1 = 2 \equiv -1 \mod 3 \, \checkmark \]

\( p=5 \):
\[ 4! = 24 \equiv -1 \mod 5 \, \checkmark \]

\( p=7 \):
\[ 6! = 720 \equiv -1 \mod 7 \, \checkmark \]

Proof for \( p>2 \):
\[ (p-1)! = (p-1)(p-2) \ldots (1) \]

Multiplying together all of \( \mathbb{F}_p^x \) \((\mathbb{Z}/p\mathbb{Z})^x\).

Pair them up as \( a, a^{-1} \)

E.g. \( p=7 \):
\[ 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \]
\[ = 6 \cdot (5 \cdot 3) (4 \cdot 2) \] in \( \mathbb{F}_7 \)
\[ = 6 \cdot 1 \cdot 6 \equiv -1 \mod 7 \]

Pairing up eliminates all terms not equal to their own inverse.

If \( x = x^{-1} \iff x^2 = 1 \iff x^2 - 1 = 0 \iff \exists \text{ a root of } x^2 - 1 \), we know by Theorem/Corollaries only roots are 0 and 1. So \( (p-1)(p-2) \ldots 1 = -1 \cdot 1 = -1 \) in \( \mathbb{Z}/p\mathbb{Z} \).

Modular arithmetic in general rings:

Definition:

- If \( R \) is a ring and \( r \in R \), \( a \equiv b \mod (r) \) means \( r \mid (b-a) \)
  (i.e. \( b-a = qr \) for some \( q \in R \)).
• $R/(r)$ is the set of congruence classes modulo $r$. It is a ring!

Example:
• $R = \mathbb{Z}$, $r = 5$
  
  $R/(r) = \mathbb{Z}/(5) = \mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$.

• $R = \mathbb{R}[x]/(x^2 + 1)$, $r = x^2 + 1$.
  
  $\mathbb{R}[x]/(x^2 + 1)$. All elements have unique representatives
  
  $a + bx$. (E.g. $x^3 = x(x^2 + 1) - x \equiv -x \mod (x^2 + 1)$).

  $a + bx + c + dx = (a + c) + (b + d)x$.
  
  $(a + bx)(c + dx) = ac + (bc + ad)x + bdx^2 \equiv x^2 \equiv -1$

  Compare $a + bx \mapsto a + bi \in \mathbb{C}$.

  You get same addition and multiplication laws.

  i.e., $\mathbb{R}[x]/(x^2 + 1) = \mathbb{C}$.

A field with 9 elements. $\mathbb{Z}/9\mathbb{Z}$ has 9 elements but it
is not a field.

Idea: repeat above, but use \( \mathbb{F}_3 \) instead of \( \mathbb{R} \).

\[ \mathbb{F}_3 \langle x \rangle / (x^2 + 1) \text{ is a field!} \]

Ring \( \checkmark \) Can check by hand everything is invertible.

Representative of the form
\[ a + b \cdot x \quad a, b \in \mathbb{F}_3, \]
3 choices for \( a \) & 3 choices for \( b \)
so 9 choices total, so 9 elements!

= 3 \cdot 3